Kassai Károly

A honvédelmi célú elektronikus információs rendszerek fejlesztéséhez szükséges, továbblépést megalapozó vizsgálat – egy zöld könyv kialakításának támogatása

Military and Intelligence CyberSecurity Research Paper
2022/5.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

A tanulmány a honvédelmi célú elektronikus információs szolgáltatások és rendszerek fejlődését, illetve az egyre komplexebb kapcsolódó védelmi kérdéseket vizsgálja. Áttekinti röviden a honvédelmi ágazat szakpolitikai, stratégiai szabályozási környezetét és a kapcsolódó szakirodalmi diskurzust az elektronikus információbiztonság kapcsán. Kitekint az EU és NATO fejlesztési törekvésekre és azok főbb hazai hatásaira, majd gyakorlati szempontokra koncentrálva keresi a biztonsági szint megerősítéséhez és emeléséhez szükséges, stratégiai aspesktusból kulcsfontosságú lépéseket.

Kulcsszavak: honvédelem, információbiztonság, információs szolgáltatások, kiberbiztonság, stratégia

The study examines the evolution of the defence digital services and systems parallel with the increasingly complex defence issues. It gives a short introduction in the policy and strategic level regulation of the defence sector and a short insight in the professional discourse on digital information security. It also reviews the development efforts of the EU and NATO and their effect on national progress, then by concentrating on practical aspects looks for strategic key steps towards strengthening and raising the level of security.

Keywords: defence, information security, information servicec, cyber security, strategy

BEVEZETÉS

Hazánkban a nemzetközi folyamatoknak megfelelően lépten-nyomon tapasztalható a kommunikációs szolgáltatások robbanásszerű fejlődése, a digitalizáció különböző szolgáltatásokban történő megjelenése, ami egyértelműen azonosítható tendencia honvédelmi területen is.

A honvédelmi célú elektronikus információs szolgáltatások (vagy rendszerek) fejlődése, illetve a kapcsolódó védelmi kérdések nem tekinthetők új hadtudományi témának. A feszített ütemű szervezeti átalakulások, technikai fejlesztések kapcsán joggal felmerülhet a kérdés, hogy az elektronikus információs rendszerek üzemeltetését, elektronikus információbiztonságát, elektronikus információvédelmét,[1] illetve kibervédelmét biztosító keretrendszer pontosan illeszkedik-e a helyzethez? A jövőbeli várható változások, szervezeti és technikai korszerűsítési lépések igényelnek-e stratégiai szinten komolyabb korrekciós lépéseket? Felmerülhet-e hiányzó honvédelmi követelményeket, eljárásokat

[1] A két kifejezés alkalmazása nem csak a nyomatékosítást szolgálja: a hazai jogszabályi környezet a nem minősített adatkezelésre az „elektronikus információbiztonság”, míg minősített adatkezelés területén az „elektronikus információvédelem” kifejezést alkalmazza, melyek mellett a kapcsolatrendszer és a tartalom részletes azonosítása nélkül – a nemzetközi trendnek megfelelően – megjelent a „kibervédelem” kifejezés is.

megfogalmazó stratégiai szintű – vagy alacsonyabb szintű – szabályozó hiánya?

E vizsgálat tehát nem napjaink egyik legnépszerűbb témájának – a kibervédelemnek – határait feszegeti, inkább gyakorlati szempontokra koncentrálva keresi a biztonsági szint megerősítéséhez és emeléséhez szükséges, stratégiai szempontból kulcsfontosságú lépéseket…

A vizsgálat terjedelmi okok miatt nem tekinthető teljes körű feldolgozásnak, illetve tudatosan csak nyílt, publikusan megjeleníthető információkra támaszkodik, a következtetések során is csak ilyen információkat jelenít meg.

A HAZAI ELŐZMÉNYEK NAGYBANI ÁTTEKINTÉSE

Magyarországon 2011-2012-ben már azonosítható a kibertérrel kapcsolatos kérdések nemzeti szintű kezelése. A nemzeti kibervédelmi feladatokról 2012-ben a Nemzeti Biztonsági Stratégia a 31. pontban rendelkezik.[2] Erre építve a Nemzeti Katonai Stratégia a Magyar Honvédség egyik céljaként jeleníti meg a hálózatalapú hadviselés feltételeinek megteremtését, és ennek részeként a Magyar Honvédség kibervédelmének megerősítését. A kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmak átfogó felülvizsgálatát és adott esetben módosítását.[3]

A Nemzeti Kiberbiztonsági Stratégia 2013-ban meghatározza a kiberbiztonsági környezetet, kijelöli a nemzeti célokat és feladatokat, valamint megállapítja az eszközrendszert. A Stratégia a nemzetközi együttműködés vonatkozásában kiemeli, hogy Magyarország az atlanti együttműködést a kiberbiztonság terén kiemelten fontosnak tartja; az időközben kiadott NATO nyilatkozatok[4] alapján ez azt is jelenti, hogy a kiberbiztonság kérdése a NATO Alapító Okmányának 5. cikkelye alá tartozó kollektív védelem körébe tartozik.[5]

A Stratégia mellett megjelent az állami és önkormányzati elektronikus információs rendszerekre vonatkozó elektronikus információbiztonsági követelményeket meghatározó törvény és annak végrehajtási rendeletei.[6] A 2009-ben és 2010-ben csak minősített adatkezelésre koncentráló követelmények (törvény és végrehajtási rendeletek) így kiegészültek a nem minősített adatok védelmi kötelezettségeivel - az állami és önkormányzati elektronikus adatkezelésre szűkített hatállyal. Szentgáli Gergely 2013-as munkája részletesebben ábrázolja az

[2] *Magyarország Nemzeti Biztonsági Stratégiájáról* szóló 1035/2012. (II.21.) Korm. határozat, 31. p.

[3] *Magyarország Nemzeti Katonai Stratégiájának elfogadásáról* szóló 1656/2012. (XII. 20.) Korm. határozat 82, 33. pontok.

[4] *NATO Walesi Nyilatkozat*, 2014. szeptember 05. (72. pont). NATO Varsói Nyilatkozat 2016. július 09. (71-72. pont).

[5] *Magyarország Nemzeti Kiberbiztonsági Stratégiájáról* szóló 1139/2013. (III. 21.) Korm. határozat 8. pont és 10. pont e) alpont.

[6] 2013. évi L. törvény *az állami és önkormányzati szervek elektronikus információbiztonságáról* (Ibtv.) és a végrehajtására vonatkozó kormányrendeletek. Szakmai érdekesség, hogy a kidolgozás során folyamatosan a jogszabály kialakításán volt a hangsúly, a stratégiai megalapozás szükségessége gyakorlatilag a kiadás előtt, hirtelen jelent meg.

akkori helyzetképet, melyből *említésre érdemes elem az offenzív kibertér műveleti képesség fontossága*.[7]

2015-ben a szabályozási rend felülvizsgálaton esett át és megjelent a manapság ismert szabályozási keret – azóta további változásokkal frissítve.

Ebben az időszakban a honvédelmi ágazatnál több vonalon történtek a honvédelmi elektronikus információs rendszerek biztonságát erősítő lépések. Technikai területen kicsit az előbb említett jogszabályok előtt 2012-ben megjelent *a honvédelmi elektronikus információbiztonság általános követelményeit meghatározó miniszteri utasítás*,[8] kiegészítve a korábbi, szervezeti és szabályozási kereteket rögzítő Információbiztonsági Politikát.[9] Az akkor még jogszabályi követelmények nélkül megfogalmazott honvédelmi kontrollkészlet szabvány alapú megközelítéssel, életciklus szemléletet követve határozta meg a rendszerekre vonatkozóan az alapvető biztonsági szempontokat.

Az általános követelmények rendszer specifikumaként 2013-ban az MH központi elektronikus információs rendszerének biztonsági követelményeinek meghatározása érdekében a szakmai irányításért felelős szerv szakutasítást adott ki,[10] melynek legfontosabb feladata a hálózati struktúrához igazodva a felelősségi körök lehatárolása, illetve a helyi területi és központi szakfeladatok összehangolása, természetesen biztonsági szempontból.

Minősített elektronikus adatkezelés területén NATO kompatibilis módon 2012-2014-ben megtörtént a rendszerek rendszer-specifikus biztonsági követelményekre,[11] a szabályozásra,[12] az ellenőrzésre [13] és az akkreditálási eljárásra[14] vonatkozó korszerű szempontrendszer meghatározása.

A kibertér védelmével kapcsolatos katonai érdekek azonosítása és szervezeti válaszok keresése a kormányzati stratégiák megjelenése előtt, 2011-ben kezdődött. Az

[7] Az említett elem a 2021-es Nemzeti Katonai Stratégiában azonosítható. SZENTGÁLI Gergely: *A magyar kibervédelem anatómiai képe*. Felderítő Szemle 2013. december, pp. 74-89, p. 85-86.

[8] 3/2012. (01. 13.) HM utasítás *a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról*

[9] 94/2009. (XI. 27.) HM utasítás *a honvédelmi tárca információbiztonság politikájáról*. A politikáról részletesebb információk a következő publikációban olvashatók: KASSAI Károly: *A honvédelmi tárca biztonságpolitikájában meghatározott követelmények, feladatok és azok fontosabb hatásai*. Hadmérnök, IV. Évfolyam 4. szám - 2009. december, pp. 183-190.

[10] 20/2013. (HK 12.) HVK HIICSF szakutasítás *a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszer-specifikus elektronikus biztonsági követelményeinek meghatározásáról*

[11] 18/2016. HVK HIICSF szakutasítás *a Minősített Elektronikus Adatkezelő Rendszerek Rendszer Biztonsági Követelményeire vonatkozó szabályokról*

[12] 9/2012. HVK HIICSF szakutasítás *a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről*

[13] 10/2012. HVK HIICSF szakutasítás *a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről*

[14] 13/2016. (HK 7.) HVK HIICSF szakutasítás *a Minősített Elektronikus Adatkezelő Rendszerek biztonsági akkreditációs eljárásrendjéről*

alap- és teljes képesség kialakításának rendjére vonatkozó elrendelés honvédelmi miniszteri utasításban történt meg.[15] A szükséges szakfeladatokat 2013-ban miniszteri utasítás foglalta össze a Magyar Honvédség Kibervédelmi Szakmai Koncepció formájában,[16] *központi követelményként meghatározva a kibervédelmi fejlesztések keretét és a képességfejlesztési feladatokat*.

2013-ban a törvényi feladatszabás alapján a honvédelmi ágazati feladatok meghatározása érdekében honvédelmi miniszteri rendelet jelent meg,[17] kétéves időtartamra meghatározva a honvédelmi ágazati eseménykezelési és hatósági struktúrát. Erre alapozva 2014-ben az akkori szervezeti struktúrára alapozva megjelent a honvédelmi eseménykezelést szabályozó szakutasítás, az eljárások biztosítása, működési rend kialakítása érdekében.[18] Folytatást jelentett az MH Kormányzati Célú Elkülönült Hírközlő Hálózat (a továbbiakban: MH KCEHH) hálózati szintű elektronikus eseménykezelési feladatokat ellátó szervezeti elem kialakításának elrendelése HM utasítás formájában, 2015-ben.[19]

2015-ben a Honvédelmi Szakpolitikai Program elektronikus információvédelmi/elektronikus információbiztonsági területen az MH és KNBSZ kibervédelmi képességek erősítését, a katonai szervezetek elektronikus minősített adatkezelésének fejlesztését, a katonai szervezetek elektronikus minősített adatkezelésének fejlesztését, kapcsolódó feladatként a védelemigazgatási minősített adatkezelés és a tábori híradás fejlesztését tűzte ki célul.[20]

Következő honvédelmi szakterületű változást jelentett 2016-ban kormányrendelettel elrendelt új követelmény,[21] mely szerint az ágazati elektronikus információbiztonsági hatósági felügyeleti feladatok a KNBSZ főigazgató hatáskörébe kerültek. Ugyanebben az évben megújult az először 2010-ben megkötött NATO – magyar kibervédelmi együttműködési megállapodás.[22]

Technikai síkon az akkori terminológia szerint híradó és informatikai (napjainkban

---

[15] 81/2011. (VII. 29.) HM utasítás *a honvédelmi tárca Kibernetikai Védelmi Koncepció kialakításához szükséges feladatok meghatározásáról*, 3. §. (5-6) p.

[16] 60/2013. (IX. 30.) HM utasítás *a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról.*

[17] 16/2013. (VIII. 30.) HM rendelet *a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről* (hatályon kívül).

[18] 5/2014. HVK HIICSF szakutasítás *a honvédelmi tárca elektronikus adatkezelő rendszerek incidenskezelési eljárásrendről*

[19] 10/2015. (III. 26.) HM utasítás *a Magyar Honvédség egyes szervezetei feladatrendszerének módosításával és vezetési rendszerét érintő átalakításokkal kapcsolatos egyes feladatokról*, 3. § (1-2) p. (hatályon kívül).

[20] *Honvédelmi Szakpolitikai Program* 7.1, 7.2, 6.3 és 3.3 pontok.

[21] 22/2016. (II. 17.) Korm. rendelet *az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet módosításáról*, 1. §.

[22] *Hungary signs new MoU on cyber defence cooperation*; https://nicp.nato.int/hungary-signs-new-mou-on-cyber-defence-cooperation/index.html

infokommunikációs) fejlesztések gyorsítása érdekében 2015-ben kormányhatározat jelent meg,[23] ami jelzi, hogy az infrastruktúrafejlesztés keretén belül már vezetői szinten is érzékelt a biztonsági feladatok, funkciók fontossága.

AZ EU ÉS NATO SZINTŰ HATÁSOK FOKOZÓDÓ ADAPTÁCIÓJA

Az EU-ban 2017-ben a szorosabb védelmi együttműködés egyik zálogaként megkezdődött az Állandó Strukturált Együttműködés,[24] ami kibervédelmi programokat is tartalmaz. Molnár Anna – Szabolcs Laura beszámolója szerint[25] a programok között szerepel a kiberfenyegetés és eseménykezelő információmegosztási platform, magyar részvétellel.[26] A több körösen indított projektek következő csatlakozási pontja Kovács László 2020-as tájékoztatása szerint[27] hazánk csatlakozása a német kezdeményezésű Kiber és Információs Műveleti Központ kialakítását célzó kezdeményezéshez.[28]

Az eljárások és technikai körülmények fejlődése 2017-2018 idején már többszörösen is érintette a honvédelmi ágazat különböző szakterületeit a nemzetközi kibervédelmi gyakorlatok illetve a nemzetközi válságkezelési gyakorlatok kibervédelmi feladatainak megoldásában. A NATO Cyber Coalition és a NATO Kibervédelmi Kiválósági Központ[29] Locked Shield kibervédelmi gyakorlatsorozat, illetve a NATO és nemzeti erőket is alkalmazó válságkezelési gyakorlatsorozat kibervédelmi forgatókönyvei[30] évről-évre újabb, technikai és jogi, hadműveleti szempontból bonyolultabb feladatokat szabnak a végrehajtó üzemeltető, kibervédelmi egyéb szakterületű állománynak. A Locked Shield gyakorlatsorozat evolúciója jól mutatja a kibertér kezeléséhez szükséges eszközök és megoldások számának növekedését. A kezdetben tudatosan technikai orientációjú gyakorlat napjainkban már csak részeiben ismerhető fel. A különböző forgatókönyvek megoldásához továbbra is magas szintű technikai megoldó képesség és külső-belső együttműködési lépés szükséges, melyet napjainkban már védelemigazgatási és válságkezelési, hadműveleti szakértőkből

[23] 1500/2015. (VII. 23.) Korm. határozat *a Magyar Honvédség kibervédelem szempontjából kiemelt jelentőségű komplex informatikai fejlesztéseihez kapcsolódó beszerzéseknek a védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról* szóló 228/2004. (VII. 30.) Korm. rendelet 2. § (3) bekezdés d) pontja szerinti minősítéséről, 1. p.

[24] Permanent Structured Cooperation (PESCO).

[25] MOLNÁR Anna– SZABOLCS Laura: *Megerősített együttműködés, változó geometria, PESCO*. Hadtudomány 2020/4. pp. 87-88.

[26] A kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform.

[27] Magyarország élen jár az európai katonai kibervédelemben; https://honvedelem.hu/hirek/magyarorszag-elen-jar-az-europai-katonai-kibervedelemben.html

[28] CIDC: Cyber and Information Domain Centre.

[29] NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE.

[30] NATO Crysis Management Exercise – NATO CMX.

álló stratégiai csoporttal, jogi tanácsadó csoporttal, média és stratégiai kommunikációs támogatással megerősítve lehet csak sikeresen végrehajtani.

Az említett NATO alapú tevékenységek mellett említést érdemel a Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet által szervezett első nemzeti kibervédelmi gyakorlat lebonyolítása 2019. decemberben.[31]

Az EU katonai ambíciószint emelkedését jelzi a 2021. februárban[32] és júniusban[33] lezajlott első kétfokozatú, katonai eseménykezelő központoknak rendezett kibervédelmi gyakorlat.

A 2021. októberben lebonyolított hibrid műveleti fókuszú Létfontosságú Bástya nemzeti válságkezelési gyakorlat is tartalmazott kibervédelmi feladatsort.[34]
Ezek a történések tanúsítják, hogy nagyobb publicitás nélkül megkezdődött a polgári és a honvédelmi, katonai nemzetbiztonsági feladatokon belül a kibervédelmi kérdések gyakorlati szintű kezelése.

A napi életben és a gyakorlatokon megoldandó technikai feladatok elsajátítása hosszú és rögös utat jelent az érintett állománynak, ahol egy lehetséges megoldás a NATO Kibervédelmi Központ által biztosított tanfolyami képzési lehetőség, melyet esetenként kihelyezett tanfolyammal is lehet biztosítani, mint 2016-ban ez megtörtént a Nemzeti Közszolgálati Egyetem biztosításában.[35]

2017-ben a jogszabályok szerinti eseménykezelésre, sérülékenységvizsgálatra és hatósági feladatokra vonatkozó ágazati követelmények részletes meghatározása érdekében HM utasítás jelent meg.[36]

A 2016-os NATO követelményekkel összhangban a magyar honvédelmi szabályozás jogszabályi változásokkal korszerűsödött. A Hvt. 2018-as módosításában megjelent a Honvédség feladatai között a kibertér védelme, illetve ezzel kapcsolatban a szövetségesi, nemzetközi együttműködési kötelezettség. Meghatározott esetekben a Honvédség

[31] Sikeresen lezajlott a magyar kiberbiztonsági gyakorlat (HunEx2019) https://nki.gov.hu/intezet/kozlemenyek/sikeresen-lezajlott-a-magyar-kiberbiztonsagi-gyakorlat/

[32] Cyber defence exercise brings together military CERTs https://eda.europa.eu/news-and-events/news/2021/02/19/cyber-defence-exercise-brings-together-military-certs

[33] EDA MilCERT Interoperability Conference talks strategy https://eda.europa.eu/news-and-events/news/2021/06/08/milcert-interoperability-conference-talks-strategy

[34] A gyakorlat során cél volt a katonai, rendvédelmi és civil képességek összehangolt tevékenységének gyakoroltatása a létfontosságú létesítményeket veszélyeztető hibrid fenyegetések és támadások elleni fellépés időszakában. 30/2021. (VII. 23.) HM utasítás *a „Létfontosságú Védőbástya 2021" nemzeti létfontosságú rendszerelemeket érintő válságkezelési gyakorlat honvédelmi ágazatot érintő feladatainak előkészítéséről és végrehajtásáról*, 2 §. (3)

[35] Átfogó képet kaptak a kibertér védelméhez szükséges módszerekről és eszközökről; https://honvedelem.hu/hirek/hazai-hirek/atfogo-kepet-kaptak-a-kiberter-vedelmehez-szukseges-modszerekrol-es-eszkozokrol.html

[36] 15/2017. (IV. 28.) HM utasítás *a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól*. 2020-ban megtörtént a bekövetkezett változások követése, így ez a szabályozás pontosítottnak tekinthető.

felhasználható a kibertérből érkező és egyéb elektronikai fenyegetések elhárításában, illetve a NATO, EU megoldásnak megfelelően a törvény is leszögezte, hogy a kibertér műveleti területként kezelendő. Új feladatként jelent meg a „honvédelmi veszélyhelyzet" fogalom, amikor a Kormány elrendelheti a KNBSZ és a honvédségi szervezetek felderítő, elhárító, valamint kibertér műveleti erők tevékenységeinek fokozását.[37]

2019-ben folytatódtak a változások. A Hvt. megalapozta, hogy a Honvédség műveleteinek támogatása érdekében nyújtott kibertér műveleti támogatáshoz a Honvédség eszközei szabályozottan átengedhető KNBSZ számára. Megjelentek a katonai kibertér műveletekre vonatkozó különös szabályok (eljárásrend, a kibervédelmi ügyeletes parancsnok feladatkör). [38]

2019-ben változott továbbá a nemzetbiztonságról szóló törvény (Nbtv.), ahol a KNBSZ eddigi, a kibertevékenységekről történő információgyűjtési feladat bővült a honvédelmi ágazati elektronikus információbiztonsági feladatok ellátásával, illetve a minisztérium és a Magyar Honvédség parancsnoksága információvédelmi tervező munkához szükséges információk biztosításával. A KNBSZ kibertér műveleti képességeivel ellátja honvédelmi érdekek nemzetbiztonsági jellegű védelmét és támogatja a MH kibervédelmét és műveleteit.[39]

2019-ben stratégiai szintű, lényegi szervezeti változás a Honvédelmi Minisztérium és Magyar Honvédség Parancsnoksága szervezetek elkülönülése (dezintegráció). Ennek a lépésnek szakmai vonzata a korábban is vezérkari csoportfőnökség által végzett híradó, informatikai és információvédelmi szakmai irányítói hatáskör megjelenése mellett a kibervédelmi területű haderőnemi szemlélőség megjelenése, a stratégiai szintű szakfeladatok (tanácsadás, fejlesztési feladatok irányítása, kommunikációs feladatok) biztosítása érdekében.

2019-ben Szentendrén megtörtént a Kiberakadémia megnyitója, újabb támogatási lehetőséget nyitva a képzési lehetőségek között.[40] 2021 szeptemberében már folytak a Kiberműveleti Központ Előkészítő Osztály tanfolyamai, a hivatkozott forrás szerint – más tanfolyamok mellett – egynapos kibervédelmi tudatossági tanfolyamok is zajlottak.[41]

A katonai elektronikus információbiztonságra fókuszáló képzés keretei korábban, 2005-2006 környékén alakultak a Nemzeti Közszolgálati Egyetem

[37] 2011. évi CXIII. törvény *a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről*, 36. § (2) g. pont, 80. §. 5 és 22. pont, 21. § A (1) d. pont. (Módosítás: a 2018. évi CX. törvény szerint.)

[38] Hvt. 37. §. (5) d. pont, 62/A (1-8).

[39] 1995. évi CXXV. törvény *a nemzetbiztonsági szolgálatokról* (módosítás- 2019. évi CV. Törvény) 6. §. f, g. pontok

[40] Átadták a Magyar Honvédség Kiber Képzési Központját; https://honvedelem.hu/media/aktualis-videok/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat.html

[41] Fókuszban a kiberbiztonság (2021. 09. 17), https://honvedelem.hu/hirek/fokuszban-a-kiberbiztonsag.html

jogelődjénél, egy korábbi cikk beszámolója szerint. Ekkor alakult ki a rendszerbiztonsági felelős (később felügyelő) és a rendszeradminisztrátori biztonsági képzési tematika, az elektronikus információvédelmi kockázatelemző és a kompromittáló kisugárzás elleni védelmi szaktanfolyamok, valamint a rejtjelző alaptanfolyamok, eszközkezelő tanfolyamok rendje.[42]

SZABÁLYOZÁSI ÉS DOKTRINÁLIS KÉRDÉSEK

2020-ban új NATO követelményként azonosítható a NATO Kibertér Műveleti Doktrína megjelenése,[43] melynek ratifikálása miniszteri utasítás formájában hazánkban is megtörtént.[44]

A NATO doktrína ratifikálása mellett saját nemzeti követelményként miniszteri feladatszabásban szereplő feladat[45] a nemzeti kibervédelmi doktrína kiadása.[46] A szervezetkialakításra vonatkozó folyamat felgyorsulását (a gondolkodás irányának változását) jelzi, hogy a műveleti alapokat meghatározó doktrína kiadása előtt megjelent a Kiber és Információs Műveleti Központ 2022-es megalakítását elrendelő miniszteri szervezési utasítás, ami tartalmi eltérést mutat a korábbi, kibervédelmet célzó feladatkörhöz képest.[47]

A kibertérre vonatkozó doktrinális kérdéseket nem lehet önállóan, az összhaderőnemi és a többi funkcionális doktrína figyelembe vétele nélkül megoldani. Így figyelmet igényel a kibertér kérdések összhangjának megteremtése:

- A 2018-ban kiadott MH Összhaderőnemi Doktrínával,[48] amihez kapcsolódó feladatot jelenthet a korábban említett jogszabályi változások és a 2020-es új Nemzeti Katonai Stratégiában megjelenő kibertér feladatok.
- A 2014-ben kiadott MH Információs Műveleti Doktrínával, ahol az elmúlt időszak változásainak megfelelően pontosan ki kell dolgozni az információs műveletek folyamatainak és

[42] KASSAI Károly: *Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005 – 2015 közötti időszakban*; Hadmérnök X. Évfolyam 3. szám - 2015. szeptember, pp. 279 – 291, p. 282.

[43] NATO Cyber Operations Doctrine – AJP 3.20. (2020)

[44] 42/2020 HM utasítás *egyes NATO egységesítési jelzések elfogadásáról*, 5. §.

[45] 14/2021. (III. 19.) HM utasítás *a honvédelmi szervezet 2021. évi kiemelt feladatainak, valamint a 2022–2023. évi fő célkitűzéseinek meghatározásáról* Az éves fő feladatokat meghatározó miniszteri feladatszabás részletes szakmai követelményeket egy szakterületen sem határoz meg, így a nemzeti doktrínára vonatkozó elvárások itt nem azonosíthatók. Az úttörő jellegű doktrína kidolgozási folyamat mellett megemlítendő, hogy a korábbi kiadású Összhaderőnemi Doktrína, a Hadműveleti Doktrína, az Információs Műveletek Doktrína, a HÍD terminológiában, a műveleti folyamatokban nem követi az új gondolatokat, mely helyzet sürgős összehangolási feladatok szükségességét jelezi.

46 A Doktrína kiadása 2022. 05.02-én megtörtént: 175/2022. (HK 4.) MH PK *intézkedés a Magyar Honvédség Kibertér műveleti doktrína (1. kiadás) című szolgálati könyv kiadásáról*

[47] 32/2021. (VII. 23.) HM utasítás *a Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról*

[48] Hatályba léptette: 462/2017. (HK 12.) HVKF szakutasítás.

eljárásainak lényegi elemeit, a korábban említett, megalakítás előtt álló szervezeti elem működésének biztosítása érdekében; biztosítani kell a katonai műveletek sikeréhez szükséges információs műveletek integrálását a műveleti tervezés és végrehajtás folyamataiba.

– A 2013-ban kiadott MH Összhaderőnemi Híradó és Informatikai Doktrínával, tekintettel arra, hogy a kibertér műveletek tervezése és végrehajtása során a híradó és informatikai infrastruktúra megkerülhetetlen.[49] Ennél a kérdésnél még meg kell oldani a korábban említett MH Informatikai Szabályzattal és az MH Informatikai Stratégiával történő összehangolási feladatokat is.

A doktrinális kérdésekkel foglalkozó Mező Andrástól markáns megfogalmazásban olvasható 2018-ban, hogy „… a szabványos NATO-doktrínákon nyugvó magyar katonai gondolkodás Magyarország biztonságának egyik alapvető pillére.”,[50] ami jelzi, hogy a doktrínák kialakítása és pontosítása, valamint tartalmi összehangolásuk fontos eleme kell, hogy legyen a katonai kultúrának.

A katonai műveletek tervezése és végrehajtása nem csak az irányelveket jelző doktrínák, hanem részletesebb követelményeket meghatározó szabályozók kérdése is. A NATO átfogó művelet tervezési irányelveire[51] építve 2013-ban megjelent az MH Törzsszolgálati Utasítás, melynek feladata a katonai műveletek tervezéséhez és végrehajtásához, irányításához szükséges összes folyamat, feladat, felelősség és kapcsolódási pontok meghatározása, ami biztosítja a Honvédség – mint gépezet – működését önállóan vagy szövetségi keretekbe ágyazva. A NATO követelmények változtak 2021-ben, az új tervezési irányelvek megjelenésével számos ponton kibertér műveleti szempontok jelentek meg. Emiatt kifejezetten kibertér műveleti síkra egyszerűsítve is igényként jelentkezik az Utasítás modernizálásának kérdése.

A szabályozottsággal kapcsolatos részletes értékelést ez a tanulmány nem vállalhat, egyrészt a téma érzékenysége-, másrészt a teljes körű, részletes vizsgálat hiánya miatt. A működéshez szükséges folyamatokra, feladatokra és felelősségekre vonatkozó szabályozási kérdések fontosságának megítélése, a stratégiai súly érzékeltetése Farkas Ádám 2021-es írásában szemléletesen olvasható. E szerint „Minden jól strukturált és felkészült

[49] A nyilvánvaló összefüggést jelzi a NATO doktrína értelmezése, mely szerint a híradó és informatikai infrastruktúra műveletek kibertér műveletnek minősülnek a védelmi, offenzív és felderítő műveletek mellett.

50 A gondolat folytatása: „A doktrinális gondolkodás elhanyagolása megfosztaná a hadsereget a módszeres gondolkodástól, a szövetségi együttműködés lehetőségétől, a haderő konzisztens fejlesztésétől.” Mező András: *A Magyar Honvédség doktrínafejlesztése – 2. rész*, Hadtudomány, 2018/1. pp. 48-57. p. 55.

[51]Allied Command Operations: Comprehensive Operations Planning Directive (COPD INTERIM V2.0), 2013 (hatálytalan). Jelenleg az irányelv 2021-ben kiadott harmadik változata van érvényben.

védelmi szervezet számára alapvető fontosságú a szabályozottság, hiszen előre meghatározott protokollok nélkül nincs hierarchia, (…)". további veszélyre figyelmeztető gondolat, hogy „ha a védelmi és biztonsági funkciók szabályozása nem kellően korszerű, nem kellően konzisztens, nem kellően stabil és kiszámítható, akkor az az állammal szembeni bizalom erózióját eredményezheti."[52] Ezek a gondolatok megvilágítják, hogy *a folyamatok (vagy katonai műveletek) szabályozása nem rosszul értelmezett bürokratikus útvesztő, hanem nélkülözhetetlen, mással nem pótolható vezetéssel szemben támasztott követelmény.*

Esetenként felbukkanó, markánsan fogalmazó, a katonai képességfejlesztés fontosságát tükröző vélekedések szerint nem jogszabályokra, szabályozásra van szükség, hanem cselekvésre! Ez a populáris megközelítés a köznapi életben szimpatikus, haladáspártinak könyvelhető, ugyanakkor elfedi az előbbi gondolatot a honvédelmi területen a szabályozottság fontosságáról. Ugyanilyen népszerű, gyakran bemutatott nézet a kibertérben történő helyzetek villanásnyi idő alatt történő bekövetkezése („nincs idő jogértelmezésre, azonnal kell cselekedni"), illetve visszatérő jellegű még a kibertér „határtalansága" (az adatok és szolgáltatások „nem az országhatárok szerint működnek") és a történések megítélésének nehézsége. A hasonló, kibertéri feladatokat népszerűsítő, bár kevésbé szakszerű gondolatok ellenszere csak a tanulás lehet! Szükség van annak megértésére, hogy *a villámlásszerűen történő események a valóságban hosszú előkészítés eredményei* (ahol meg kell találni a detektálási lehetőségeket), illetve *a „légiesnek" tűnő adatmozgások hardver és szoftver elemekhez köthetők, ami egyben földrajzi kötődést is kell, hogy jelentsen* (még akkor is, ha egy világűrben keringő objektumról vagy nyílt óceánon tartózkodó hajóról van szó).

Vasvári Géza 2018-as szakmai szintet célzó írásában erre vonatkozóan összefoglalóan megjegyezte, hogy hazánk NATO csatlakozása óta a jogszabályi környezet jelentősen átalakult fejlődött. A digitalizáció (és az egyéb technikai fejlődés) újabb kihívásokat eredményez, „ami megköveteli a szabályozási környezetnek az elért eredmények és az információbiztonsági trendek elemzésén alapuló folyamatos felülvizsgálatát".[53]

Gerőfi Szilárd 2017-es, az utolsó évtizedre fókuszáló írása szerint a híradó szolgálat fejlődése lehetővé tette a katonai informatikai rendszerek látványos bővülését. A két szolgálat (szakterület) a vizsgált időszakban jelentősen közelített egymáshoz, szorosan együttműködik, melyhez csatlakozik az elektronikus információvédelem is. Más helyen megállapítja, hogy az informatika területén is időről-időre változott az irányításra vonatkozó elképzelés (centralizálás vagy decentralizálás), illetve az elektronikus információvédelem is „sokáig kereste helyét a struktúrában", ami jelzi, hogy a

[52] FARKAS Ádám: *A kortárs technikai-fejlődés és innováció viszonya a honvédelmi szabályozással*, MTA Law Working Papers, ISSN 2064-4515, 2021/4, p. 3, 5.

[53] VASVÁRI Géza: *A katonai szervezetek elektronikus információvédelmi képességeinek fejlesztésével kapcsolatos feladatok*, Hadtudományi Szemle, 2018/5. pp. 73-89. p. 87.

fejlődés nem minden esetben zökkenőmentes lépésekből állt e szakterületeknél. E mellett további idézésre érdemes a szakállomány biztosításával és megtartásával kapcsolatos nehézség, a polgári szféra elszívó ereje miatt.[54]

Ez az inkább szervezeti oldalú vizsgálat érdemi magyarázattal szolgálhat a rendszerek (szolgáltatások) irányításával és szabályozásával kapcsolatos összetett helyzetre.[55]

Új nemzetközi jelenség az elrettentés (deterrence) összetett feladatrendszerének a kibertérben történő kiemelése és a „kiber (kibertér) elrettentés" gondolatkör kialakítása, fejlesztése. A kérdés helyes megoldása nem lehet e vizsgálat tárgya, így csak annyit célszerű rögzíteni, hogy az elrettentés komplex logikájának megértése nagy segítséget nyújthat az új, stratégiai szintű gondolatok formálásához. Ennek része kell, hogy legyen annak megítélése, hogy *milyen meglévő, reális képesség, folyamat, feladatrendszer tekinthető hitelesnek, működőképesnek, ezáltal mások által is elrettentőnek*. Hasonló kategória kell, hogy legyen a NATO és EU követelményekből lebontandó *ellenálló képesség (resilience),*[56] *ahol nem csak alrendszer, rendszer szintű, hanem nemzeti, ágazatokon átívelő, illetve nemzetközi szektorok közötti civil - katonai képességek összehangolását kell célul kitűzni*, beleértve természetesen a digitalizációs megoldásokat, kibertér műveleti kérdéseket.

Az eddigiekben bemutatott szervezeti, technikai és eljárási lépések mellett *nem elhanyagolható a humán faktorban rejlő kockázatok tudatos ellensúlyozása.* A honvédelmi ágazatnál a biztonságtudatosítás keretén belül több lépéssel, fokozatosan kialakult a felhasználók támogatása érdekében kialakított, elektronikus közlemények formájában megvalósított – a kibervédelmi kockázatok csökkentését célzó tájékoztatási rendszer –, melyet a 2020-as COVID-19 veszélyhelyzet a gyakorlatban tesztelt Knapp Gábor tájékoztatása szerint.[57] A tudatosítás formavilága változatos, mint azt egy korábbi beszámoló is mutatja. 2010-ban az akkori Zrínyi Miklós Nemzetvédelmi Egyetem, Híradó Tanszék és a HM Honvéd Vezérkar Híradó és Informatikai Csoportfőnökség, Elektronikus Információvédelmi Osztály közösen megszervezte az első Katonai Elektronikus Információvédelmi Konferenciát. Az éves ismétlődésű – mai napig zajló – rendezvény sorozat célja szakmai konzultáció és tapasztalatcsere.[58] A 2022 májusi

[54] GERŐFI Szilárd: *A Magyar Honvédség vezetéstámogató rendszere alkalmazásának lehetőségei a XXI. századi kihívások tükrében*; Hadtudomány, 2017/3-4. pp. 96-105, p. 97, 103.

[55] Megjegyzendő, hogy más minisztériumokban a Gerőfi által szemléltetett folyamat helyett szervezeti elkülönítésen alapuló kultúrák alakultak ki és az elektronikus információvédelem (benne: rejtjelzés) és elektronikus információbiztonság a távközléstől (vagy infokommunikációtól) független szervezeti elemként dolgozik (pl. Biztonsági Főosztály).

[56] Akár az elrettentés gondolatához is köthetően.

[57] KNAPP Gábor: *Az elektronikus információbiztonság-tudatosítás feladatrendszerének honvédelmi ágazati szempontú vizsgálata és kihívásai*; Szakmai Szemle XVIII. évfolyam 3. szám, p. 150, 154.

[58] KASSAI Károly: *Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005 – 2015 közötti időszakban*; Hadmérnök X. Évfolyam 3. szám - 2015. szeptember, p. 282.

konferencián a közönség meghallgathatta Magyarország kiberkoordinátorának bevezető előadását a készülő nemzeti kiberbiztosági stratégiáról, információk hangzottak el a kiberműveleti doktrína legfontosabb kérdéseiről, illetve a Kibervédelmi Akadémia által is biztosított képzési lehetőségekről. [59]

Remélhetően ehhez hasonló gyakorlat alakul ki az EU Kibervédelmi Hónap rendezvény naptárában megjelenő, a Katonai Nemzetbiztonsági Szolgálat által szervezett 2021-es szakmai konferencia nyomvonalán. A konferencián Knapp Gábor az eseménykezelés vonalán – korábbi cikkével összhangban – a minősített adatkezelésre jogosított rendszerek, illetve a rejtjeltevékenység sajátosságait vizsgálta és rámutatott, hogy ezekben a speciális üzemeltetési környezetben sem kizárható incidensek bekövetkezése és az azok kezelésére vonatkozó megoldások kialakítása és fenntartása. Farkas Ádám jelezte, hogy az állami funkciókat összehangoltan, hibrid környezetthez igazodó szemlélettel kell kialakítani. Marsi Tamás az államigazgatásban bevezetett korai előrejelző rendszer kapcsán az incidenskezelés támogatására és a reagálási idő csökkentésére mutatva jelezte ennek a védelmi vonalnak a fontosságát. Király Ágnes a kibertér fenyegetettség elemzés (Cyber Threat Intelligence – CTI) lényegi ismertetésénél a strukturált megközelítés fontosságára hívta fel a figyelmet (stratégiai, hadműveleti és harcászati (taktikai), illetve rámutatott, hogy az általánosan ismert életciklus modellt (szemléletet) – a fennálló nehézségek mellett – ezen a területen is alkalmazni kell.[60] A szakmai konferenciák vonalától eltérő, de hasonlóan fontos terület a szakértői szintű együttműködés. Ennek szükségességére mutat rá a V4 országok katonai kibervédelmi szervezeteinek 2021 szeptemberében lebonyolított találkozója a Magyar Honvédség Parancsnokságának kibervédelmi haderőnemi szemlélőjének szervezésében. A már említett német vezetésű CIDCC PESCO projekt magas szintű képviselője is részt vett a rendezvényen, bemutatva a projekt legfontosabb jellemzőit.[61]

A fontosabb történések lezárásaként említendő a Nemzeti Katonai Stratégia 2021-es kiadása,[62] miben már a kibertérben zajló honvédelmi érdekérvényesítés több eleme is olvasható.

2021-es további változás a nemzeti felügyeleti rendben, hogy a megújuló Nemzeti Kiberbiztonsági Koordinációs Tanács munkájában állandó tagként részt vesz a KNBSZ főigazgatója is.[63]

Honvédelmi területen irányadónak kell tekinteni az éves miniszteri feladatszabást. Ennek értelmében 2022-

[59] Nemzetközi Katonai Információbiztonsági Konferencia (2022. 05. 03.); https://honvedelem.hu/hirek/nemzetkozi-katonai-informaciobiztonsagi-konferencia.html

[60] MAGYAR Sándor: *Katonai kibertér 2021. Konferencia beszámoló*; Szakmai Szemle XIX. évfolyam 4. szám, p. 138, p. 146. és p. 147.

[61] A visegrádi országok katonai kibervezetői tanácskoztak Budapesten (2021. 11. 15.), https://honvedelem.hu/hirek/a-visegradi-orszagok-katonai-kibervezetoi-tanacskoztak-budapesten.html

[62] 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

[63] 259/2021. (V. 20.) Korm. rendelet a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról, 26. §. (3)

ben kiemelt szakfeladat a honvédelmi ágazati elektronikus eseménykezelés, sérülékenységvizsgálat és hatósági felügyeleti funkciók területén a képességfejlesztés folytatása, valamint a Magyar Honvédség Kiber- és Információs Műveleti Központ megalakítása, majd kezdeti műveleti képességének elérése 2024 végére.[64]

Utolsó gondolatként célszerű utalni a már látható, érzékelhető kibertér kihívásokra melyek kezelése már a közeljövőben is megoldandó feladatokat jelenthet.

A nemzeti szuverenitás biztosítása, a szükséges önvédelmi lépések megtétele nem képzelhető el a betudás (attribúció) témakörének feldolgozása-, az eszkalációs folyamatok kialakítása vagy a szükséges feladatok gyakoroltatása nélkül. Páll-Orosz Piroska 2021-es írása szerint *szükség van – más nemzetekhez hasonló módon – a betudásra vonatkozó nemzeti álláspont megfogalmazására és kinyílvánítására, illetve ezzel párhuzamosan a sikeres azonosításhoz szükséges összes szereplő feladatainak azonosítására és tevékenységük összehangolására*.[65]
A korábbi megállapítások mutatják, hogy jogszabályokban, nemzeti stratégiákban már megjelennek a kibertér műveleti offenzív lehetőségek. Kovács László 2021-es írásában ezt a feladatot kezdte tanulmányozni, több helyen is aláhúzva *a terminológiai feszültséget, az eltérő megközelítések ütköztetésének szükségességét, illetve elkezdte a hibrid műveleteken belül értelmezendő offenzív műveletek fontosabb elemeinek azonosítását,* mint a szélesen értelmezett felderítés és adatgyűjtés, a támadás és a hatáselemzés.[66]

ZÁRÓ GONDOLATOK

Az egész világon tapasztalható digitalizáció hazánkban is rengeteg eljárási, technikai változást hozott ebben az évezredben.

A honvédelmi területű működési keretrendszer ebben az időszakban nagyságrendekkel bonyolultabbá vált. Ráadásul az is kockázat nélkül jósolható, hogy a digitális fejlődés nem tekinthető lezártnak…

A honvédelmi célú elektronikus információs rendszerek szükséges mértékű védelme érdekében az elektronikus információbiztonsági/információvédelmi, az üzemeltetői és a kibervédelmi szakterület szoros együttműködési kényszere mellett *az egyéb szakmai területek felé irányuló fokozottabb szakterületi támogatási igény is jól tapintható* (a teljesség igénye nélkül említve pl. a védelemigazgatási, jogi, védelempolitikai, művelettervezési, haderőfejlesztési és humán területeket).

Honvédelmi területen jól érzékelhető, hogy *az elektronikus információs rendszerek üzemeltetésére,*

[64] 3/2022. (I. 27.) HM utasítás *a honvédelmi szervezet 2022. évi kiemelt feladatainak, valamint a 2023–2024. évi fő célkitűzéseinek meghatározásáról*; 2. §. 47, 56. p. és 3. §. 31. p.

[65] PÁLL-OROSZ Piroska: *Attribúció (betudás) a kibertérben*, Nemzetbiztonsági Tanulmányok II. ISBN 978-615-6128-04-01, 2021; p. 81.

[66] KOVÁCS László: *Offenzív kiberműveletek 1: Az offenzív kiberműveletek természete*, Hadmérnök, 16. évfolyam (2021) 2. szám p. 195 – 198.

használatára illetve biztonságára vonatkozó eljárások, folyamatok több szabályozói szinten és több területen fejtik ki hatásukat – időben is széttagoltan.

Ebben a helyzetben „kristálygömbje" válogatja, hogy milyen vezetői, szakmapolitikai és szakmai lépések tekintendők egyedüli, kizárólagosan jó megoldásnak, gyógyírnak a honvédelmi célú elektronikus információs rendszerek biztonsága növelése érdekében.

A cselekvési alternatívák feltárását, a helyes fontossági sorrend kialakítását meg kell alapozni egy olyan felülvizsgálattal, ahol az előnyök, hátrányok azonosítása mellett megtörténik a folyamatok (és szervezetek, feladatok) közötti függőségek pontos feltárása, melyet egy legalább stratégiai szintű kockázatelemzéssel és értékeléssel kell megerősíteni. Az így kialakult reális helyzetkép alapot biztosít felelős vezetői döntések megalapozásához, a szükséges szakmai cselekvési lépések megfogalmazásához. Megtörténhet az üzemeltetési, biztonsági és kibervédelmi folyamatok megerősítése (pl. folyamatok pontosítása, képzési és gyakorlási célok kitűzése), a katonai vezetési és irányítási rendszerben szükséges módosítások megtétele, illetve a kibervédelmi (tágabban: kibertér műveleti) „gondolkodás" stratégiai, hadműveleti és harcászati szintű beágyazása a kor követelményeinek megfelelően.

A fenti lépések megtétele ellen számtalan, a napi életben folyamatosan – gyakran figyelmeztető jelek nélkül – jelentkező hatás (igény, követelmény) léphet fel. A nyilvánosság is jól követheti a haderőfejlesztés fontosabb történéseit és a korábban nem tapasztalható ütemben történő légi, légvédelmi, szárazföldi haditechnikai rendszerek, eszközök megjelenését és alkalmazásba vételi igényét, melyeket számtalan, „láthatatlan" üzembe helyezési, fenntartási és képzési feladathalmaz kísér, nehezít. Ezek a tényezők a rendelkezésre álló erőforrásokat gyakran a napi legsürgősebb ügyek megoldására rendelik, a jelenleg is sokszínű elektronikus adatkezelés palettájának további színesítésével – és az összkép még bonyolultabbá tételével.

Az előbbiek megalapozzák a következtetést, hogy a jelenlegi helyzetben a honvédelmi célú elektronikus információs rendszerek biztonságának növelése rengeteg új folyamat megjelenését és fenntartását igényli, ami a rengeteg kérdőjel mellett az ismeretlen függőségi kapcsolatok, a támogatói lánc kockázatok, a tudásban vagy telepítésben (beüzemelésben) lévő esetleges hiányosságok felkiáltójeleit is magukkal hordozzák.

Ezek mellett *kiemelt fontosságúnak kell tekinteni a meglévő működési keretrendszer felülvizsgálatát, pontosítását* és a stratégiai szintű kockázatok azonosítására, értékelésére alapozott kockázatkezelési lépések megtételét.

Egyszerűen kifejezve kijelenthető, hogy *megbízható, szilárd alapok nélkül kockázatos az építkezés!*

FELHASZNÁLT FORRÁSOK

[1] 3/2022. (I. 27.) HM utasítás a honvédelmi szervezet 2022. évi kiemelt feladatainak, valamint a 2023–2024. évi fő célkitűzéseinek meghatározásáról

[2] 10/2012. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről

[3] 10/2015. (III. 26.) HM utasítás a Magyar Honvédség egyes szervezetei feladatrendszerének módosításával és vezetési rendszerét érintő átalakításokkal kapcsolatos egyes feladatokról (hatályon kívül).

[4] 1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[5] 13/2016. (HK 7.) HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszerek biztonsági akkreditációs eljárásrendjéről

[6] 15/2017. (IV. 28.) HM utasítás a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól

[7] 1500/2015. (VII. 23.) Korm. határozat a Magyar Honvédség kibervédelem szempontjából kiemelt jelentőségű komplex informatikai fejlesztéseihez kapcsolódó beszerzéseknek a védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról szóló 228/2004. (VII. 30.) Korm. rendelet 2. § (3) bekezdés d) pontja szerinti minősítéséről

[8] 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről (hatályon kívül)

[9] 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájának elfogadásáról

[10] 175/2022. (HK 4.) MH PK intézkedés a Magyar Honvédség Kibertér műveleti doktrína (1. kiadás) című szolgálati könyv kiadásáról

[11] 18/2016. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszerek Rendszer Biztonsági Követelményeire vonatkozó szabályokról

[12] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (módosítás- 2019. évi CV. Törvény)

[13] 20/2013. (HK 12.) HVK HIICSF szakutasítás a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszer-specifikus elektronikus biztonsági

követelményeinek meghatározásáról

[14] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

[15] 22/2016. (II. 17.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet módosításáról

[16] 259/2021. (V. 20.) Korm. rendelet a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról

[17] 3/2012. (01. 13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról

[18] 30/2021. (VII. 23.) HM utasítás a „Létfontosságú Védőbástya 2021" nemzeti létfontosságú rendszerelemeket érintő válságkezelési gyakorlat honvédelmi ágazatot érintő feladatainak előkészítéséről és végrehajtásáról, 2 §. (3)

[19] 32/2021. (VII. 23.) HM utasítás a Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról

[20] 42/2020. HM utasítás egyes NATO egységesítési jelzések elfogadásáról

[21] 5/2014. HVK HIICSF szakutasítás a honvédelmi tárca elektronikus adatkezelő rendszerek incidenskezelési eljárásrendről

[22] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

[23] 81/2011. (VII. 29.) HM utasítás a honvédelmi tárca Kibernetikai Védelmi Koncepció kialakításához szükséges feladatok meghatározásáról

[24] 9/2012. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről

[25] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról

[26] Allied Command Operations: Comprehensive Operations Planning Directive (COPD INTERIM V2.0), 2013

[27] A visegrádi országok katonai kibervezetői tanácskoztak Budapesten (2021. 11. 15.), https://honvedelem.hu/hirek/a-visegradi-orszagok-katonai-kibervezetoi-tanacskoztak-budapesten.html

[28] Átadták a Magyar Honvédség Kiber Képzési Központját; https://honvedelem.hu/media/aktualis-videok/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat.html

[29] Átfogó képet kaptak a kibertér védelméhez szükséges módszerekről és eszközökről; https://honvedelem.hu/hirek/hazai-hirek/atfogo-kepet-kaptak-a-kiberter-vedelmehez-szukseges-modszerekrol-es-eszkozokrol.html

[30] Cyber defence exercise brings together military CERTs https://eda.europa.eu/news-and-events/news/2021/02/19/cyber-defence-exercise-brings-together-military-certs

[31] Cyber PESCO Projects Conference (2022. 05. 23.) https://www.defesa.gov.pt/pt/pdefesa/CAIH/en/eucaih

[32] EDA MilCERT Interoperability Conference talks strategy https://eda.europa.eu/news-and-events/news/2021/06/08/milcert-interoperability-conference-talks-strategy

[33] EU cyber resilience challange (2022. 05. 25.); https://www.ucm.es/file/save-the-date-cyber-pesco-conference/?ver

[34] Farkas Ádám: *A kortárs technikai-fejlődés és innováció viszonya a honvédelmi szabályozással*, MTA Law Working Papers, ISSN 2064-4515, 2021/4

[35] Fókuszban a kiberbiztonság (2021. 09. 17), https://honvedelem.hu/hirek/fokuszban-a-kiberbiztonsag.html

[36] Gerőfi Szilárd: *A Magyar Honvédség vezetéstámogató rendszere alkalmazásának lehetőségei a XXI. századi kihívások tükrében*; Hadtudomány

[37] Honvédelmi Szakpolitikai Program

[38] Hungary signs new MoU on cyber defence cooperation; https://nicp.nato.int/hungary-signs-new-mou-on-cyber-defence-cooperation/index.html

[39] Knapp Gábor: *Az elektronikus információbiztonság- tudatosítás feladatrendszerének honvédelmi ágazati szempontú vizsgálata és kihívásai*; Szakmai Szemle XVIII. évfolyam 3. szám

[40] Kovács László: *Offenzív kiberműveletek 1: Az offenzív kiberműveletek természete*, Hadmérnök, 16. évfolyam (2021) 2. szám

[41] Magyarország élen jár az európai katonai kibervédelemben; https://honvedelem.hu/hirek/magyarorszag-elen-jar-az-europai-katonai-kibervedelemben.html

[42] Magyar Sándor: *Katonai kibertér 2021. Konferencia beszámoló*; Szakmai Szemle XIX. évfolyam 4. szám

[43] Mező András: *A Magyar Honvédség doktrínafejlesztése – 2. rész*, Hadtudomány, 2018/1.

[44] MOLNÁR Anna – SZABOLCS Laura: *Megerősített együttműködés, változó geometria, PESCO*; Hadtudomány 2020/4

[45] NATO Cyber Operations Doctrine – AJP 3.20. (2020)

[46] NATO Varsói Nyilatkozat, 2016. július 09.

[47] NATO Walesi Nyilatkozat, 2014. szeptember 05.

[48] Nemzetközi Katonai Információbiztonsági Konferencia (2022. 05. 03.); https://honvedelem.hu/hirek/nemzetkozi-katonai-informaciobiztonsagi-konferencia.html

[49] Nemzeti Mesterséges Intelligencia Stratégia 2020

[50] PÁLL-OROSZ Piroska: *Attribúció (betudás) a kibertérben*, Nemzetbiztonsági Tanulmányok II. ISBN 978-615-6128-04-01, 2021

[51] Sikeresen lezajlott a magyar kiberbiztonsági gyakorlat (HunEx2019) https://nki.gov.hu/intezet/kozlemenyek/sikeresen-lezajlott-a-magyar-kiberbiztonsagi-gyakorlat/

[52] SZENTGÁLI Gergely: *A magyar kibervédelem anatómiai képe*, Felderítő Szemle 2013. december, HU ISSN 1588-242X

[53] VASVÁRI Géza: *A katonai szervezetek elektronikus információvédelmi képességeinek fejlesztésével kapcsolatos feladatok*, Hadtudományi Szemle, 2018/5.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2022/5.

Szerző(k) / Author(s):
Dr. Kassai Károly PhD

Kézirat lezárásának ideje / Manuscript closing time:
2022.06.26.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Prof. Dr. Resperger István PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.