Dévai Dóra:

A KIBERKÉPESSÉGEK SZERVEZETI INTEGRÁCIÓJA AZ AMERIKAI EGYESÜLT ÁLLAMOK HADEREJÉBEN – ADAPTÁCIÓS LEHETŐSÉGEK A MAGYAR HONVÉDSÉG SZÁMÁRA

DOI: 10.35926/HSZ.2022.1.2

ÖSSZEFOGLALÓ: *A Magyar Honvédségben 2019. január 1-jén kezdték meg működésüket a haderőnemi szemlélőségek (köztük a kibervédelmi), és ezzel elkezdődött a Magyar Honvédségben a kiberműveletek szervezeti hátterének stratégiai szintű kialakítása és fejlesztése. Az Amerikai Egyesült Államokban a katonai kiberképességek[1] kialakítása valamivel korábban, a kétezres évek elején kezdett kibontakozni. Ez a fejlődési ív egy újabb meghatározó szakaszhatárhoz ért 2018. május 4-én, amikor is a Kiberparancsnokság (U.S. Cyber Command – USCYBERCOM) tizedik egyesített műveleti parancsnoksággá való átszervezése megtörtént, tehát kialakult a kiberképesség stratégiai szintű szervezetének alapvető struktúrája. Ezt követően a figyelem a hadműveleti és a harcászati szintű kiberképességek kialakítása és integrálása felé fordult. Az Amerikai Egyesült Államok vizsgálata egyrészt katonai, diplomáciai és technológiai vezető szerepénél fogva, másrészt az ezen a téren felhalmozott tapasztalat okán értékes mintákkal, tanulságokkal szolgálhat a magyar kiberképességek szervezeti kialakításához, valamint a hazai hadtudományi szakirodalom bővüléséhez.*

KULCSSZAVAK: *Magyar Honvédség Parancsnoksága Haderőnemi Szemlélőség (kibervédelmi), Kiberparancsnokság, harcászati szintű kiberképességek, többdimenziós műveletek*

[1] Az Amerikai Egyesült Államok haderejében a katonai kiberműveletek (cyberspace operations – CO) jelenlegi fogalmi rendszerét lefektető 2018-as összhaderőnemi szakdoktrína a Joint Publication 3-12 Cyberspace Operations, I-4. a következőképpen határozza meg a kiberképességet (cyberspace capability): „olyan eszköz vagy számítógépes program, beleértve a software, firmware vagy hardware bármilyen kombinációját, amelynek a célja, hogy valamilyen hatást érjen el a kibertérben vagy a kibertéren keresztül." Ez tehát a kiberképességek szűk, kizárólag technológiai értelmezése. A kutatás azonban, ahogy a fentiekben megfogalmaztuk, a kiberműveletekkel kapcsolatos átfogó haderőfejlesztést vizsgálja. Ezért az amerikai hadseregben általánosan elterjedt doktrína, szervezet, kiképzés, hadfelszerelés, vezetés, állomány, infrastruktúra, szakpolitika (Doctrine, Organization, Training, Material, Leadership, Personnel, Facility – Policy – DOTMLPF-P) modellen keresztül értelmezem a képességeket. A doktrína szerint a kiberműveletek definíciója: „A kiberképességek alkalmazása olyan esetekben, ahol az elsődleges cél valamilyen feladat megvalósítása a kibertérben vagy azon keresztül." Joint Publication 3-12 – Cyberspace Operations. vii. US Joint Chiefs of Staff, 08. 06. 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (Letöltés időpontja: 2021. 03. 12.)

BEVEZETŐ

2020-ra Magyarországon is létrejöttek a kiberműveleti képességek alkalmazásához szükséges nemzeti stratégiai, jogszabályi és szervezeti struktúra alapjai.[2] A magyar haderőben a katonai kiberképességek letéteményese a Magyar Honvédség Parancsnokságán (MHP) belül létrehozott Haderőnemi Szemlélőség (kibervédelmi). Ez a szervezet a Magyar Honvédség kibervédelmének és kiberműveleti képességeinek stratégiai szintű képességkialakító, a Magyar Honvédség (MH) kibervédelmi szakterülete fejlesztését irányító és felügyeletét ellátó szervezeti egysége. A haderőnemi szemlélő irányítja az MHP, valamint az MH hadrendjébe tartozó katonai szervezetek kibervédelmi tevékenységét, meghatározza a szakterülete vezetéséhez szükséges szervezeti kialakítás alappilléreit, struktúráját. Koordinálja a kibervédelmi képességfejlesztést, valamint harmonizálja e képességek kialakítását.[3]

Az új hazai fegyvernem képessége kialakításának e korai szakaszában értékes tapasztalatokkal szolgálhat más szövetséges államok struktúráinak a vizsgálata. Az Amerikai Egyesült Államok a katonai kiberképességekkel egyik legrégebben rendelkező szövetséges nagyhatalom, ezért nagy szerepe van a kiberképességekkel kapcsolatos alapelvek kialakításában. Célom tehát elsősorban az amerikai haderőn belül a három vezetési szinten kialakított szervezet, illetve az ezek közötti feladatmegosztás és együttműködés bemutatása. A 2010 és 2017 közötti időszakban a haderőfejlesztés főként a stratégiai szintre koncentrált, ezt követően a figyelem viszont egyre inkább a harcászati szintű egységek összetétele és működése felé fordult.

Az Amerikai Egyesült Államokban a szervezeti struktúra kialakításával párhuzamosan az új képességek hatása tükröződik a hadviselés koncepcionális és doktrinális átalakulásában is, mint például az információs műveletek újraértelmezése és a többdimenziós műveletek (Multidomain Operations – MDO) bevezetése is. Másik célom tehát a szervezeti változások elméleti, hadtudományi hátterének rövid bemutatása.

Tanulmányomban rámutatok azokra az alapvető megoldásokra, tanulságokra is, amelyek véleményem szerint a Magyar Honvédség számára is átültethetők és megfontolandók.

A KIBERKÉPESSÉGEK KIALAKÍTÁSA A MAGYAR HONVÉDSÉGBEN

Az MH feladatait a kibertérben az 2020-ban kiadott Nemzeti Biztonsági Stratégia[4] (NBS) és a honvédelmi törvény (Hvt.) szintén 2020-ban hatályba lépő változtatása szabja meg:[5]

- a katonai műveletek kibertámogatása;
- ki kell alakítani a kiberműveletekben alkalmazható offenzív képességeket;
- fejleszteni kell az MH kibervédelmi és kiberműveleti erőit;

---

[2] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új nemzeti biztonsági stratégiájában. Honvédségi Szemle, 2020/5., 3–18. https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/120 (Letöltés időpontja: 2021. 08. 04.)

[3] A Magyar Honvédség Parancsnoksága. https://honvedelem.hu/a-magyar-honvedseg-parancsnoksaga.html (Letöltés időpontja: 2021. 03. 12.)

[4] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020/81., 2101–2119. https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/ (Letöltés időpontja: 2020. 09. 04.)

[5] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről. https://net.jogtar.hu/jogszabaly?docid=a1100113.tv (Letöltés időpontja: 2020. 09. 03.)

- a kiberműveleti tevékenységek vezetése és végrehajtása különböző szinteken;[6]
- a kibervédelemhez szükséges hazai bázisú kutatás-fejlesztés erősítése;
- aktív nemzetközi együttműködés, szövetségesi feladatok ellátása;
- a Magyarország biztonságát, honvédelmi érdekeit sértő, veszélyeztető, katonai jellegű kibertérműveletek, kibertérre ható cselekmények vagy kibertámadások elleni fellépés;[7]
- az MH-nak folyamatosan biztosítania kell a honvédelmi szervezetek, gyakorlatok és műveletek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét;[8]
- a védelem mellett a honvédelmi szervezeteket érő kibertámadások esetén az esetleges támadást az MH kibertérműveleti erőinek meg kell szakítaniuk;[9]
- amennyiben a kibertámadások olyan súlyosak, hogy azok Magyarország biztonságát fenyegetik, akkor külön döntés szerint a támadó rendszerekkel szemben katonai kibertéri műveletekkel kell fellépnie;[10]
- a szövetségesi kötelezettségeit sértő vagy fenyegető rendszerekkel szembeni katonai kibertérműveleti fellépés.[11]

A fenti feladatok végrehajtása érdekében megkezdődött a szakdoktrinális keretek és a szervezeti struktúra kiépítése. 2020 augusztusában nemzeti elfogadásra került az Allied Joint Doctrine For Cyberspace Operations – AJP-3.20 (Edition 1) / Szövetségi összhaderőnemi kibertérműveleti doktrína.[12]

2019 júniusában kezdte meg működését az MH Kiber Képzési Központja, amely képzési, oktatási és kiképzési feladatokat lát el. Megkezdődött a kiberműveleti erők szervezése,[13] valamint a Kiberműveleti Központ felállítása. Tevékenysége – a jelenleg ismert koncepció alapján – a következő tevékenységeket és képességeket foglalja magában:

- információgyűjtés, -elemzés, -értékelés;
- kibervédelmi és kibertéri műveletek tervezése, szervezése, integrációja és vezetése (beleértve a támadó műveleteket is);
- kutatás-fejlesztés;
- oktatás, képzés, speciális kibertérműveleti kiképzés, gyakorlatok;
- nemzetközi együttműködés.[14]

KIBERKÉPESSÉGEK A KÜLÖNBÖZŐ VEZETÉSI SZINTEKEN – ELMÉLETI ALAPVETÉSEK

A legutóbbi szakdoktrinális felosztás a kiberműveleteket az Amerikai Egyesült Államokban és a NATO-ban is az adott művelet által elérendő cél vagy hatás szerint határozza meg. Eszerint védelmi kibertéri műveletekről (*defensive cyberspace operations* – DCO) és támadó

[6] Kovács: i. m. 16.
[7] Hvt. 36. § (2) g) pont.
[8] Kovács: i. m. 13.
[9] Hvt. 62/A. § * (1) bek.
[10] Kovács: i. m. 13.
[11] Hvt.: i. m.
[12] A honvédelmi miniszter 42/2020. (VIII. 14.) HM utasítása egyes NATO egységesítési egyezmények nemzeti elfogadásáról. 5. §. Magyar Közlöny, 2020/46., 4296.
[13] Kovács: i. m. 16.
[14] Szakértői közlés. NKE Nemzetbiztonsági Szakkollégium Workshop, 2021. 04. 28.

kibertéri műveletekről (*offensive cyberspace operations* – OCO) beszélünk.[15] A nemzetközi szakirodalomban széles körben elfogadott elv, hogy a védelmi kiberműveletek szükségszerűen magukban foglalják a támadóképességeket is annak érdekében, hogy a saját és a szövetséges erők számítógép-hálózatait *(blue networks)* hatásosan megvédhessék. Így tehát a DCO támadó tevékenységet és támadó technikákat is integrálhat védelmi céllal.[16] Ezzel szemben a támadó kiberműveletek célja a kibertérben vagy azon keresztül történő erőkivetítés a műveleti parancsnokság által kitűzött célok megvalósítása érdekében.

Mivel a katonai kiberképesség mint új fegyvernem kialakítása világszerte még korai szakaszban van, ezért az elméleti hadtudományi szakirodalom is még igen csekély számú. A kinetikus háborúból kiindulva a hadtudomány három klasszikus szintet különböztet meg: stratégiai, hadműveleti és harcászati. Ehhez igazodik a kiberképességek tervezése és alkalmazása is.

A *stratégiai szinten* ez – leegyszerűsítve – a háború megnyerésére és nemzetszintű célpontokra vagy célokra irányul. A kialakulóban lévő szakirodalom szerint a stratégiai kibertámadások akár önállóan is alkalmasak az ellenfél megtörésére. Békeidőben ezek a támadások az alapvető struktúrák, például a kritikus infrastruktúrák ellen irányulnak, de magukban foglalják az amerikai stratégiai koncepcióból ismert „előretolt védelmet” *(defend forward)*, a harctér felderítő-előkészítését, az elrettentést és a kényszerítő *(coercion)* diplomáciai intézkedéseket is.[17]

A *hadműveleti szinten* az egyes katonai műveletek tervezését és vezetését végzik, tehát a csapatok különböző hadszíntereken történő alkalmazásának kérdéseivel foglalkoznak. Ezen a szinten a katonai műveletek elsősorban katonai célpontok ellen irányulnak. Itt a kibertér és a kiberműveletek jellemzően kiegészítő, támogató funkciót töltenek be a hadműveleti célok elérésében. Ilyen lehet például a fegyveres konfliktus korai szakaszában a figyelem elterelésére és a hadrend megbontására irányuló kiberművelet, mialatt a kinetikus haderő bevonul a harctérre. Esettanulmányként említhető az izraeli haderő által Szíria ellen végrehajtott Gyümölcsöskert hadművelet 2007-ben, a Grúzia ellen 2008-ban végrehajtott orosz támadás során alkalmazott kiberműveletek és a 2014 óta tartó Ukrajna elleni orosz műveletek.[18]

Végül *harcászati szinten* működnek az alacsonyabb szintű alakulatok (dandár, zászlóalj, század stb.),[19] illetve a legtöbb hagyományos fegyverrendszer. A harcászati szintű kiberművelet célja lehet például egy „okosvárosban” a videókamerák meghekkelése a harctér felderítő-előkészítése érdekében. De hasonló harcászati feladat lehet a digitális katona informatikai

[15] Joint Publication JP 3-12., II-3; AJP 3.20 – Allied Joint Doctrine for Cyberspace Operations. Edition A, Version 1. 01. 2020., 16–17. NATO Standardization Office (NSO). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (Letöltés időpontja: 2021. 08. 04.) A korábbi, a számítógép-hálózati műveletek hármas felosztása alapján megkülönböztették a számítógép-hálózati felderítést is. Jelen tanulmányban a hírszerzés, megfigyelés és felderítés (Intelligence, Surveillance, Reconnaissance – ISR) terminológiát használjuk az AAP-06 (NATO Glossary of Terms and Definitions. NSO, 2017) alapján.

[16] Piret Pernik: Preparing for Cyber Conflict: Case Studies of Cyber Command. International Center for Defence and Security, Tallinn, 12. 2018., 2. https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf (Letöltés időpontja: 2021. 02. 23.)

[17] Matthias Schulze: Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. In: Taťana Jančárková et al. (eds.): 2020 – 12th International Conference on Cyber Conflict – 20/20 Vision: The Next Decade. NATO CCDCOE, Tallinn, 185. https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (Letöltés időpontja: 2021. 08. 04.)

[18] Uo. 189.

[19] Az Amerikai Egyesült Államok szárazföldi haderejénél a hadtest a legnagyobb harcászati szintű alakulat.

rendszerei, vagy egy-egy drón vagy a GPS elleni kiberművelet. Az eddigi tapasztalatok alapján a harcászati kiberműveletek két nagy csoportba oszthatók: a harcászati alakulatokba integrált és azokkal együtt mozgó kiberműveleti szakértő, illetve a „távvezérlésű" *(reachback)* kibertámogatás egy biztosított helyszínről vagy vezetési pontról.[20]

A kiberműveletek vezetési rendszerének szervesen kapcsolódnia kell a többi törzs hasonló felépítésű rendszereihez, hogy ezek az adott szintű parancsnokság vonatkozásában egységes összfegyvernemi (összhaderőnemi) vezetési rendszert alkossanak. A kiberműveletek – és különösen a támadó műveletek – harcászati szintű alkalmazása azonban jelentős szakpolitikai vita tárgyát képezik az Amerikai Egyesült Államokban. A kibertér sajátos technikai meghatározói jelentős mértékben behatárolják a művelettervezés, a vezetés és a végrehajtás szintjét. A 2010-es évek óta a haderőnemek parancsnokai folyamatosan érveltek a kiberképességek teljes spektrumának a hadműveleti és a harcászati szintű alakulatokba történő állandó integrációja, de legalább az e képességekhez való közvetlen hozzáférés, valamint a hadműveleti és a harcászati vezetés minél szélesebb döntéshozatali jogköre mellett.[21]

A saját rendszerek informatikai biztonsága, a hadműveleti biztonság a parancsnokok felelőssége, ezek rutinszerű kiberműveleti feladatok. Emellett a kiberfölény kivívása, a valós idejű és széles körű felderítési információk megszerzése, a saját erők hatékony kibervédelme, az egyes fegyvernemek specifikus fegyverrendszereinek, valamint a légi és a földi robotjárművek irányításának folyamatos biztosítása, az információk nagy távolságú továbbítása és az ellenfél komputerhálózatos rendszereinek informatikai támadása mind a kiberműveletek részét képezik.[22] A kibertéri műveletek esetében rendkívül nagy a valós idejű felderítési információ iránti igény, hiszen a környezet másodpercek alatt megváltozhat, ezért a folyamatos jelenlét, a gyors reagálóképesség és a rugalmasság alapelvek. Ezek a tényezők a küldetésalapú vezetés igényeit támasztják alá.[23]

Ugyanakkor a harcászati szinten végrehajtott kiberműveleteknek lehetnek akár stratégiai következményei is. A kiberteret alkotó hálózatos informatikai rendszerek nem mindig esnek egybe a műveleti terület földrajzi határaival, valamint a kibertérben zajló párhuzamos tevékenységekből adódó hatásköri konfliktusok és az összekapcsolódó rendszerekből adódó esetleges járulékos károk elkerülése miatti állandó koordináció, a kiberműveletekhez kapcso-

[20] Schulze: i. m. 189.

[21] Isaac R. Porche III et al.: Tactical Cyber. Building a Strategy for Cyber Support to Corps and Below. RAND Corporation, Santa Monica, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf (Letöltés időpontja: 2021. 08. 05.); Mark Pomerleau: Authorities Complicate Use of Cyber Capabilities. Part 1. Fifth Domain, 09. 01. 2017. https://www.fifthdomain.com/home/2017/01/09/authorities-complicate-the-use-of-cyber-capabilities/ (Letöltés időpontja: 2020. 02. 19.); Cyberspace Operations Concept Capability Plan 2016–2028. TRADOC Pamphlet 525-7-8. 22. 02. 2010. https://fas.org/irp/doddir/army/pam525-7-8.pdf (Letöltés időpontja: 2021. 08. 05.)

[22] Haig Zsolt: Információs műveletek a kibertérben. Dialóg Campus, 2018, 234–242. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12651/web_PDF_Informacios_muveletek_a_kiberterben.pdf;jsessionid=3C9322D937E5956BBE25D745755A8DFD?sequence=1 (Letöltés időpontja: 2021. 08. 05.); Draveczki-Uri Ádám: Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül. Interjú dr. Kovács László dandártábornokkal. Honvédelem.hu, 2020. 07. 03. https://honvedelem.hu/hirek/hazai-hirek/egy-korszeru-harckocsi-is-szamitogep-halozat-csak-70-tonna-vas-veszi-korul.html = (Letöltés időpontja: 2021. 01. 23.); Hegedűs Ernő – Hennel Sándor: Többdimenziós (multidomain) hadműveletek. Hadtudomány, 2020/2., 3–28. https://www.mhtt.eu/hadtudomany/2020/2020_2szam/HT-2020-2_Egyben_col_PDF-A_WEB.pdf (Letöltés időpontja: 2021. 01. 23.)

[23] Porche: i. m. 3.

lódó jelentős mértékű összadatforrású ISR-igény,[24] az attribúciós probléma, a kiberműveletek rendezetlen nemzetközi háttere mind sokszor magasabb szintű katonai és/vagy politikai stratégiai döntéshozatalt és koordinációt igényel. Az *Ares* kiberműveleti harccsoport ISIS elleni tevékenységének tanulsága azonban rámutatott arra, hogy ez rendkívüli mértékben lelassítja a döntéshozatali ciklust, ezáltal pedig rontja a műveletek hatékonyságát.[25]

STRATÉGIAI SZINTŰ KIBERKÉPESSÉGEK AZ AMERIKAI EGYESÜLT ÁLLAMOKBAN

2009 júniusában Robert Gates akkori védelmi miniszter utasítására elkezdődött a kiberműveleti erők egyetlen, a Stratégiai Parancsnokság (USSTRATCOM[26]) egyik alparancsnokságaként (Subordinate Unified Command) működő szervezetbe történő egyesítése, aminek eredményeként 2010. május 21-én megalakult a Kiberparancsnokság (USCYBERCOM).[27] Az új szervezet magában foglalta a Védelmi Minisztérium kiberműveleti szervezeteit, parancsnoka a megalakulásától kezdve egyben a Nemzetbiztonsági Ügynökség (NSA[28]) igazgatója is.

Ezzel egy időben az egyes haderőnemeknek 2010-re szintén meg kellett szervezniük a saját kiberparancsnokságukat, amelyek a stratégiai szintű összhaderőnemi kiberparancsnokságon belül a haderőnemi támogató komponenst képviselik.[29]

1. táblázat *A JFHQ-C haderőnemi komponensparancsnokságai (Szerkesztette a szerző)*[30]

Haderőnem	Haderőnemi kiberparancsnokságok	Egyesített erők kiberparancsnokságai haderőnemenként
Szárazföldi haderő	Army Cyber Command (ARCYBER)	JFHQ-C ARCYBER
Haditengerészet	Fleet Cyber Command, 10th Fleet (FLTCYBER)	JFHQ-C FLTCYBER
Tengerészgyalogság	Marine Forces Cyber (MARFORCYBER)	JFHQ-C MARFORCYBER
Légierő	24th Air Force (AFCYBER)	JFHQ-C AFCYBER

[24] Intelligence, Surveillance, Reconnaissance – hírszerzés, megfigyelés, felderítés. 2009–2010 között a kiberműveleti tervezők szerint a kiberműveletek (ISR, DCO, OCO) 90%-a a célpontok felderítését és a célmegjelölést jelenti, és csak a maradék 10% határozza meg, hogy felderítésről, védelemről vagy támadásról beszélünk. Herbert Lin – Amy Zegart (eds.): Bytes, Bombs, and Spies – The Strategic Dimensions of Offensive Cyber Operations. The Brookings Institution, Washington D.C., 2018, 37. https://play.google.com/books/reader?id=eMhyDwAAQBAJ&hl=hu&pg=GBS.PA23 (Letöltés időpontja: 2021. 01. 17.)

[25] Mark Pomerleau: What Cyber Command's ISIS operations means for the future of information warfare. C4IRSNET, 18. 06. 2020. https://www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-means-for-the-future-of-information-warfare/ (Letöltés időpontja: 2021. 01. 04.)

[26] United States Strategic Command.

[27] U.S. Cybercommand. https://www.cybercom.mil/About/History/ (Letöltés időpontja: 2021. 10. 03.)

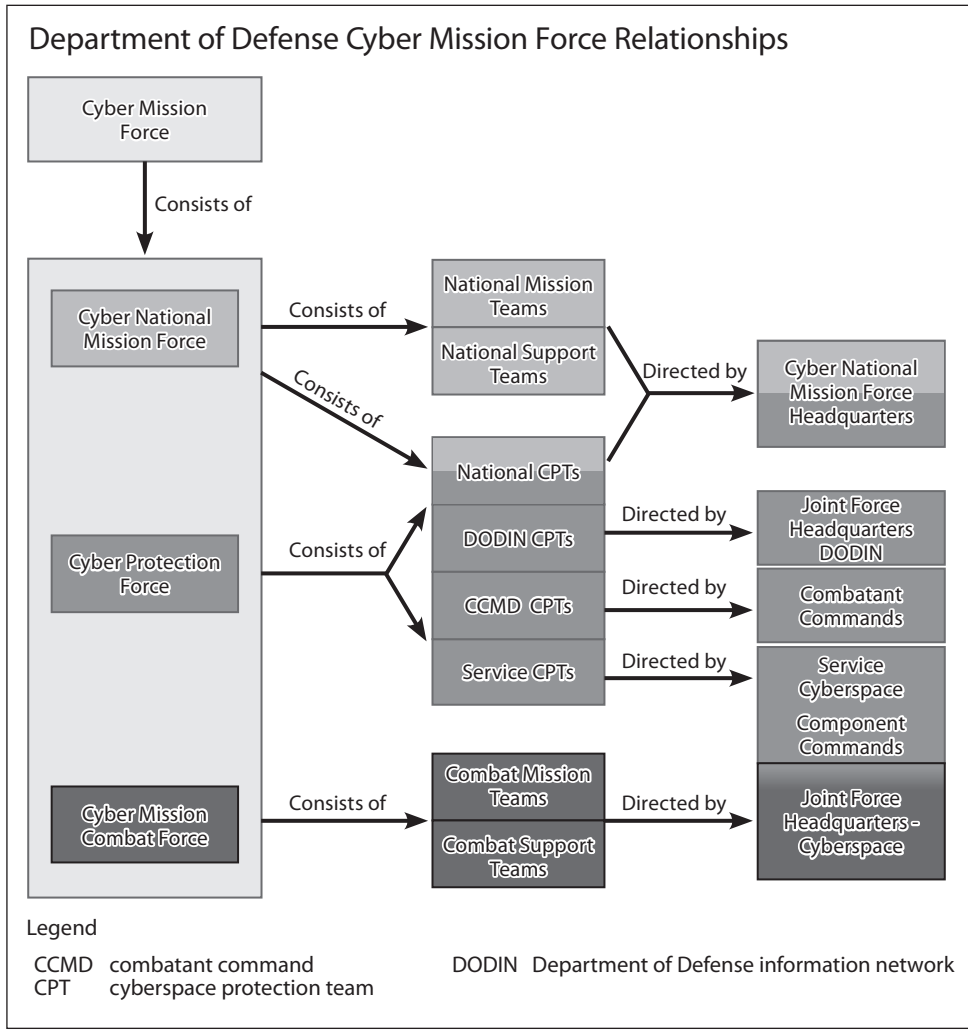
[28] National Security Agency.

[29] Jeffrey L. Caton: Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications. U.S. Army War College, 2015, 50. https://www.files.ethz.ch/isn/187504/pub1246.pdf (Letöltés időpontja: 2021. 08. 05.)

[30] Dévai Dóra: A kiberképességek fejlesztése és integrációja az Amerikai Egyesült Államok haderejében. In: Hausner Gábor (szerk.): Szemelvények a katonai műszaki tudományok eredményeiből I. Hallgatói kötet. Ludovika Egyetem Kiadó, 2021, 88. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16208/905_KDMI_II_hallgatoi_tanulmanykotet.pdf (Letöltés időpontja: 2021. 01. 04.)

A USCYBERCOM számos átalakuláson ment keresztül, míg végül 2018. május 4-én az amerikai haderő tizedik stratégiai szintű egyesített műveleti parancsnoksága lett. Felépítését tekintve öt alapvető szerkezeti elemre tagolható:

– haderőnemi kiberparancsnokságok (Services Component Commands);
– Egyesített Kiberfőparancsnokság (Joint Force Headquarters-Cyber – JFHQ-C);
– Egyesített Védelmi Minisztériumi Információs Hálózati Főparancsnokság (JFHQ-DODIN);
– Kiberműveleti Erők Főparancsnokság (Headquarters Cyber National Mission Force – HQ CNMF).



1. ábra *A CMF-erők feladatrendszere és vezetése*[31]

[31] Cyberspace Operations. Joint Publication J-P 3-12. 06. 2018., I-10.

A USCYBERCOM tevékenysége a haderőnemekkel való „munkamegosztásra" épül. Ez a kapcsolatrendszer számos sajátságos, a többi műveleti parancsnokságtól eltérő megoldást mutat. A következő részben ezeket a sajátosságokat, valamint az újonnan létrehozott kiberműveleti erők (Cyber Mission Force – CMF) tevékenységét tekintjük át.

2013-ban rendelték el a haderőnemek számára a kiberműveleti erők egységes követelményrendszer alapján történő kialakítását, ami egy 133 csapatból álló, 6200 fős állomány kiképzését írta elő 2019-re. A CMF-csapatok a haderőnemek legkiemelkedőbb tehetségeiből összeállított elit egységek, de nem tagozódnak be a haderőnemi hadosztályokba, ami nem zárja ki a velük való alacsonyabb, akár harcászati szintű együttműködést. Nemzeti és szektorális szintű stratégiai feladatokat látnak el. Felosztásuk nem a haderőnemek, hanem a feladatkör és a parancsnokság alapján történik. Az első ábra mutatja a feladatkör szerinti felosztást.

Az NMT-k – és a hozzájuk tartozó NST-k – sokrétű feladatkörrel rendelkeznek. Egyfajta „előretolt" állásban gyakran a Védelmi Minisztérium információs hálózatain kívül eső, globális ellenséges *(red space)* vagy semleges hálózatokon *(grey space)* végeznek feladatokat a stratégiai jelentőségű fenyegetések felderítése és elhárítása (korai figyelmeztetés, támadó műveletek stb.) érdekében.[32] Elsősorban a Védelmi Minisztérium kiberterének védelme a feladatuk, de szükség esetén más nemzeti érdekek védelmében – mint például kritikus infrastruktúra védelme – is bevethetők.[33]

A Védelmi Minisztérium információs hálózatainak védelméért a haderőnemek felelősek a saját használatukban lévő szegmensekben. Feladataik közé tartozik a hálózat konfigurálása, üzemeltetése és védelme. Ezért a CPT-k nagy része az adott haderőnemek közvetlen irányítása alatt áll. Feladatuk a Védelmi Minisztérium információs hálózatainak (Department of Defense Information Network – DODIN) vagy más saját műveleti terület *(blue space)* védelme, főként védelmi kiberműveletek végrehajtásával.

Az egyesített műveleti parancsnokságok számára az egyes haderőnemek által felállított kiberparancsnokságok (JFHQ-C) biztosítják a kiberműveleti támogatást. Ők vezetik tehát a támadó kiberműveletekre a műveleti parancsnokságokhoz kirendelt CMT-ket. A támogatás a tervezésben, a célkijelölésben, az összadatforrású felderítési információ formájában (ISR) és a kiberműveletek végrehajtásában valósul meg.[34] Jelentős előrelépés volt, amikor 2017-ben a Védelmi Minisztérium utasítása alapján a haderőnemi kiberparancsnokságok állandó tervezősejteket hoztak létre az egyesített műveleti parancsnokságokon belül.

A CMF rendszere tehát részben fix elhelyezkedésű elemekből, részben pedig az adott műveleti feladat igényeinek megfelelően variálható moduláris egységekből áll, ami rendkívül jó lehetőséget biztosít a rugalmasságra és a kibertérben elengedhetetlen gyors reagálásra, valamint az információ- és erőforrás-megosztásra. Egyben megoldást jelenthet az égető szakemberhiányra is.

---

[32] Mark Pomerleau: Here's How DoD Organizes Its Cyber Warriors. Fifth Domain, 25. 07. 2017. https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/ (Letöltés időpontja: 2021. 01. 04.)

[33] JP 3-12: i. m. I-9.

[34] Caton: i. m. 50.

A HADMŰVELETI ÉS A HARCÁSZATI SZINTŰ KIBERKÉPESSÉGEK AZ AMERIKAI EGYESÜLT ÁLLAMOKBAN

A haderőnemeknek tehát 2010-re létre kellett hozniuk a saját haderőnemi kiberparancsnokságukat, amely egyben a USCYBERCOM részét is képezi. Az amerikai haderő hagyományos működési rendjének megfelelően a haderőnemeknek nagyon nagy az önállóságuk a képességfejlesztés terén, így a stratégiai szinten meghatározott keretfeltételeken belül a saját paradigmáik szerint hozhatják létre a kiberképességeiket.

A folyamatot jól illusztrálja a szárazföldi haderő. Az ARCYBER, a haderőnem kiberparancsnoksága 2010 októberében kezdte meg a működését. Kettős rendeltetésénél fogva (stratégiai és hadműveleti szintű vezetés) közvetlenül a Szárazföldi Haderőnem Minisztériumának is jelent, irányítja a szárazföldi haderő kiberműveleteit, koordinálja a szárazföldi haderő globális központjaiban található öt regionális kiberközpontot.

Az ARCYBER további, a 1990-es évek eleje óta létező alegységekből áll: Információs Műveletek Parancsnoksága (Information Operations Command); 780. katonai felderítődandár (780th Military Intelligence Brigade); Hálózati Technológiai Parancsnokság (Network Enterprise Technology Command – NETCOM); kibervédelmi dandár (Cyber Protection Brigade).[35] Az ARCYBER egyrészt a saját haderőnemi kibervédelmi csapatain (CPT) keresztül, másrészt a többi közvetlen alegységén keresztül látja el a DODIN szárazföldi haderőhöz tartozó részének védelmét.

2018-ra a szárazföldi haderő új alapdoktrínát (The US Army in Multi-Domain Operations 2028) és új hadviselési koncepciót fogalmazott meg, amelyben célként a több műveleti közegben egyidejűleg alkalmazható integrált műveleti képességeket jelölte meg. A szárazföldi haderő szakdoktrínája (FM 3-38 Cyber Electromagnetic Activities – CEMA) már 2014-ben kidolgozta a kiberműveletek, az elektronikai hadviselés és a frekvenciamenedzsment műveletek integrálására épülő koncepciót, az ehhez tartozó eszközöket és felelősségi köröket.

Elsőként a szárazföldi haderő valósította meg 2014-ben a kiberműveletekre szakosított állomány kialakítását és képzését *(17 series, cyber branch)* a katonai és a civil állomány számára. Innen a legjobban teljesítők mehetnek tovább a kiberműveleti erők képzési programjába. 2018-ban az elektronikai hadviselés szakcsapatokat integrálták a kiberállományba.

A fent említett harcászati szintű kiberképességek integrálására fókuszálva 2015–2018 között zajlott a „harcászati szintű kiber-elektromágneses (Cyber Electromagnetic Activities – CEMA) támogatás a hadtestek és a kisebb egységek részére" témájú kísérleti program. A célja az volt, hogy a haderőnem kiképzési rendszerén keresztül szimulációs sorozatok során kikísérletezzék a kiberműveletek hatékony harcászati szintű alkalmazásához szükséges vezetés-irányítást, a haderőnemi műveleti tervezésbe történő integrációt, illetve a CEMA-egységek és -képességek legmegfelelőbb méretét, feladatorientált összetételét és a harcászati szintű integrációját.[36] 2019-re a program során nyert tapasztalatok alapján új harcászati szintű egységeket állítottak hadrendbe, amelyek a CMF-fel ellentétben a haderőnem állandó, integráns részét képezik:

[35] US Army Cyber Command. https://www.arcyber.army.mil/ (Letöltés időpontja: 2020. 05. 12.)

[36] David Ruderman: Command establishes enlisted pathways to become a cyber operations specialist. U.S. Army Human Resources Command Public Affairs, 10. 06. 2015. https://www.army.mil/article/149776/command_establishes_enlisted_pathways_to_become_a_cyber_operations_specialist (Letöltés időpontja: 2020. 05. 12.)

1. Az expedíciós CEMA-egységek (40-45 fő) a kiképzés és a hadműveletek során a dandárok[37] műveleti tervező törzsébe integrálódnak, de az expedíciós rajon (Expeditionary Team) keresztül alacsonyabb szintű harctéri vezetési pontra is küldhetőek. A parancsnok utasítása alapján a CEMA feladata a támadó és a védelmi kiberműveletek, a rádióelektronikai felderítés, az elektronikai hadviselés és az információs műveletek tervezése, integrációja és részleges végrehajtása. A CEMA ugyanis nem rendelkezik önálló támadó kiberműveleti képességgel. Ebben az esetben csak közvetítő szerepe van a dandár parancsnoka és az ARCYBER között *(reachback capability).*
2. 915. kiberhadviselést támogató zászlóalj (915th Cyber Warfare Support Battalion) a 780. katonai felderítődandár és így az ARCYBER alárendeltségébe tartozik. Egyedül ez az egység rendelkezik a támadó műveletekhez szükséges összes képességgel: felderítés (ISR), rádióelektronikai felderítés, információs műveletek, tűzcsapás. Védelmi és támadó műveleteket végez a szárazföldi haderő állandó és harctéri informatikai rendszerein. Hadműveleti és harcászati szintű egységek mellé rendelhető századokból áll. A zászlóalj jelenleg 100 fős, és 2025-re éri el a teljes műveleti képességet. Távoli műveletek végrehajtására vagy támogatására is alkalmas a hozzá rendelhető 12 expedíciós CEMA-egységen keresztül.
3. Felderítő-, információs, kiber-, elektronikai hadviselési és űregység (Intelligence, Information, Cyber, Electronic Warfare and Space unit – I2CEWS). Zászlóaljszintű egység, amit a többdimenziós műveleti alkalmi köteléken (Multi-Domain Task Force) belül hoztak létre. Jelenleg a csendes-óceáni térségben működik. A nevében szereplő műveleti terület bármelyikén vagy akár egyidejűleg mindegyikén képes műveleteket tervezni és irányítani. Csak támadó kiberműveleteket végez.[38]
4. Az erőforrások hatékony kihasználása érdekében a 2010-es évek végétől a hangsúly a stratégiai és a harcászati szintű kiberképességek közötti együttműködésre tevődött át. Kialakultak a USCYBERCOM CMF és a haderőnemek hadműveleti és harcászati szintjei közötti együttműködés formái. Így, a szárazföldi hadseregnél a haderőnemi parancsnok adott esetben igényelheti a stratégiai szintű CMF segítségét is.[39] Hasonlóképpen, 2018-ra a légierő is kialakította a saját integráns kiberképességét, a kiberszázadok rendszerét, amelyen keresztül a feladat igényei szerint összeállított műveleti védelmi csapatot (Mission Defence Teams)[40] egy-egy ezredhez vagy hadművelethez rendelik. Ott támadó kiberműveleti feladatokat hajtanak végre, valamint bizonyos kiemelt informatikai hálózatokat és fegyverrendszereket védenek. Szükség

[37] 2016 óta a szárazföldi haderő olyan modellre (Brigade Combat Team – BCT) váltott, ahol a dandárok rendelkeznek a harcoló (manőver-) alegységekkel és a szükséges közvetlen harctámogató és harctámogató-kiszolgáló alegységekkel, egyetlen szervezetben. U.S. Military Units. Department of Defense. https://www.defense.gov/Multimedia/Experience/Military-Units/Army/#army (Letöltés időpontja: 2021. 03. 12.)

[38] Mark Pomerleau: A new company-level unit to support information warfare. C4ISRNET, 08. 07. 2020. https://www.c4isrnet.com/information-warfare/2020/07/08/heres-what-tactical-army-cyber-units-will-use-to-conduct-operations/ (Letöltés időpontja: 2020. 10. 04.)

[39] Robert K. Ackerman: Army Extending Cyber Capabilities. Signal Magazine, 17. 02. 2021. https://www.afcea.org/content/army-extending-cyber-capabilities (Letöltés időpontja: 2021. 02. 20.)

[40] Military Units. Department of Defense. https://www.defense.gov/Experience/Military-Units/Air-Force/#air-force (Letöltés időpontja: 2021. 01. 12.)

esetén segítséget kérhetnek a saját stratégiai CPT-erőiktől.[41] A légierő által használt repülésirányítási, navigációs, fegyver- és egyéb informatikai rendszerek száma igen nagy szakértelmet kíván, ezért – a haditengerészet mellett – itt kereskedelmi szolgáltatókat is bevontak a kibervédelmi munkába, és létrehoztak egy új fegyverrendszer-védelmi hivatalt (Cyber Resiliency Office for Weapon Systems).

Két további szempontot érdemes itt kiemelni a kiberképességek integrációja kapcsán. Mint láttuk, a szárazföldi haderő a stratégiai (ARCYBER), valamint a hadműveleti és a harcászati szinten[42] létrehozott új egységekbe szinte teljes mértékben integrálta az elektronikai hadviselést és a kiberműveleti képességeket (doktrína, állomány, szervezet, harctéri haditechnikai eszközök), illetve magában foglalja az információs hadviselést is.

Ezt a mintát követi a többi három haderőnem is, valamint egyes európai országok, mint például Németország és Csehország. Eredetileg a szárazföldi haderőből kiindult kezdeményezés volt egyrészt az elektromágneses térben zajló műveletek egységes kezelése, másrészt a többdimenziós hadviselés elve. A két átalakítást egy időben, egymásra épülve valósítják meg. A harctéren a szárazföldi haderő rendelkezik a legtöbb szenzorhálózattal és elektronikai hadviselési eszközzel, amelyek számos informatikai eszközzel együtt egyre inkább az elektromágneses térben létesített vezeték nélküli hálózatokon keresztül kommunikálnak. Arról nem is beszélve, hogy ebben az esetben az elektromágneses spektrum segítségével megvalósított kiberműveletek nem igényelnek új engedélyeztetést. A kibertér és az elektromágneses tér konvergálása egyrészt sebezhetőség, másrészt lehetőség. A NATO kiberműveleti doktrína is előírja a kiberműveletek és az elektronikai hadviselés, valamint az információs műveletek közötti szoros koordinációt.[43] Sőt, a harctér átalakulását elemezve a jövőbeli hadviselésre felkészítő NATO Szövetséges Transzformációs Parancsnokság (Allied Command Transformation – ACT) már egy új, az információs hadviselést felváltó koncepcióról, a tudati dimenzióban zajló kognitív hadviselésről beszél.[44]

Szintén ebbe az irányba mutat az új hadviselési koncepció, a többdimenziós hadműveletek elve. Az amerikai haderőben, és különösen a szárazföldi csapatoknál a képességfejlesztés már az új koncepció jegyében történik,[45] miszerint a jövő hadszínterén többféle művelet

[41] Mark Pomerleau: Here's how the Air Force is fighting in the cyber domain. Fifth Domain, 28. 07. 2017. https://www.fifthdomain.com/dod/air-force/2017/07/28/heres-how-the-air-force-is-fighting-in-the-cyber-domain/ (Letöltés időpontja: 2019. 02. 13.)

[42] Az Amerikai Egyesült Államokban – Oroszországgal és Kínával ellentétben – tulajdonképpen a kezdetektől, azaz az 1960-as évektől a technológiai fejlődést előtérbe helyezve, az információs műveletek mellett egy külön utat járt be a számítógép-hálózati vagy kiberképességek fejlődése, míg végül egyesített műveleti parancsnoksággá alakult. Ezt a „hibát" felismerve a 2014-es ukrajnai invázió és az amerikai félidős választások alatt elkövetett tömeges befolyásolás után, valamint az erősödő kínai katonai képességek hatására az amerikai politikai és katonai gondolkodás a technikai és kognitív képességek szinergiái felé fordult. Lásd Peter L. Jones et al.: Russian New Generation Warfare. Unclassified Summary of the U.S. Army Training and Doctrine Command Russian New Generation Warfare Study. TRADOC G-2, US Army, 2016. https://www.armyupress.army.mil/Portals/7/online-publications/documents/RNGW-Unclassified-Summary-Report.pdf?ver=2020-03-25-122734-383 (Letöltés időpontja: 2019. 02. 13.)

[43] NATO AJP 3.20: i. m. 8–9.

[44] François du Cluzel: Cognitive Warfare. Innovation Hub, NATO ACT, June–November 2020. https://www.innovationhub-act.org/sites/default/files/2021-01/20210113_CW%20Final%20v2%20.pdf (Letöltés időpontja: 2021. 10. 04.)

[45] Mark Pomerleau: A force in flux: Military adjusts to emergent domains of warfare. C4ISRNET, 02. 05. 2017. https://www.c4isrnet.com/intel-geoint/isr/2017/05/02/a-force-in-flux-military-adjusts-to-emergent-domains-of-warfare/ (Letöltés időpontja: 2020. 11. 23.)

folyik majd egyszerre egy, a dimenziókon átívelő integrált és együttműködő rendszerben, ahol a művelet az elektromágneses térben továbbított rendkívül nagy mennyiségű valós idejű információra támaszkodva zajlik. Az egyik legjelentősebb különbség a korábbi koncepcióhoz – az Air-Land Battle elméletéhez – képest, hogy nem hadtestszintű katonai szervezetek tevékenységének koordinálását ambicionálja, hanem jóval kisebbekét, a zászlóaljharccsoport és annál kisebb léptékben akár a műveleti raj alkalmazása is lehet többdimenziós.[46]

KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK A MAGYAR HONVÉDSÉG KIBERKÉPESSÉGEINEK KIALAKÍTÁSÁHOZ

A fentiek alapján megállapítható, hogy a hadsereg által a kibertérben megvalósított feladatok tömege miatt a katonai vezetés mindhárom szintjén szükségessé vált a kiberképességek kialakítása. Ezen a területen azonban általános probléma a szakemberhiány. Emellett a kiberképességek hatékony alkalmazása egy vegyes profilú szakállomány kialakítását igényli. Ezért az eddigi tapasztalatok alapján olyan kisebb alakulatok, az amerikai haderő esetében zászlóalj vagy ennél kisebb, akár raj méretű kötelékben szolgáló alegységek a legmegfelelőbbek a kiberműveleti feladatokra, amelyek alkalmasak a gyors mozgósításra, méretükben és összetételükben modulárisan a feladatra szabhatók és az adott vezetési szintű műveletтervező törzsbe integrálhatóak, valamint a NATO többdimenziós műveleti feladataira is alkalmasak.

Jóllehet amerikai sajátosság, hogy az összhaderőnemi stratégiai vezetés mellett a haderőnemek jelentős autonóm jogkörökkel rendelkeznek, és így a hadászati és a harcászati szintű képességfejlesztés hangsúlyos, ezért a kibertér a fent említett sajátosságai miatt (a kibervédelem napi rutinfeladatai, a fegyverrendszerek speciális partikuláris igényei, a gyors döntéshozatal) mindenképpen nagyobb teret igényel a harcászati szintű kibervédelmi képességekben is.

A kiberműveleti egységek összetétele az amerikai példa alapján a következő képességeket foglalja magában: ISR, műveleti tervezés, DCO és OCO tervezése, rádióelektronikai felderítés, elektronikai hadviselés és információs műveletek. Így már a műveлettervezés szakaszában jól ki tudják használni a szinergiákból adódó lehetőségeket. A technológiai kiberképességek mellett a kognitív kiberképességek katonai alkalmazása az információs műveletek, mint az egymás hatásait kihasználó információs tevékenységek integrált alkalmazásai mára új értelmet nyertek.[47] Az új hadviselési elvek már integráltan kezelik a fizikai, a logikai és a kognitív térben alkalmazott képességeket. Ezért szükségszerű, hogy ezt elősegítse az ezekért a képességekért felelős szervezetek nagyon szoros együttműködése, lehetőség szerint szervezeti integrációja mindhárom vezetési szinten.

Stratégiai szinten – az amerikai haderőhöz hasonlóan, ahol részben a különleges műveleti képességek kialakítása szolgált mintául – az MH-ban is a különleges műveletek vezetésének analógiájára a kibervédelmi haderőnemi szemlélő szakmailag irányítaná, felügyelné és koordinálná egyrészt az MH Civil-katonai Együttműködési és Lélektani Műveleti Központ kiberműveleti feladatokra kijelölt állományának tevékenységét, valamint

[46] Hegedűs–Hennel: i. m. 7.
[47] Haig: i. m. 269.

a katonai kibertérműveleti erők szervezeteit.[48] Hadműveleti szinten ezt a műveletтervezést és végrehajtást koordináló feladatot a jelenleg szervezés alatt álló Kibervédelmi Központ látná el.[49]

A stratégiai szintű erőforrások hatékony felhasználása a hadászati és a harcászati szintekkel kialakított munkamegosztást és közvetlen kapcsolatot igényel. Az Amerikai Egyesült Államokban jelenleg a támadó kiberműveletek a saját (nemzeti vagy szövetségesi katonai) hálózatokon kívül közvetlen stratégiai szintű irányítás alatt állnak, a közeljövőben azonban várható, hogy ezen a területen a hadműveleti és akár a harcászati szintű vezetés-irányítás itt is nagyobb szerephez jut majd. Magyarországon a támadó kiberműveletek alkalmazásának jogszabályi háttere még kialakulóban van, de ahogyan a Hvt. alapján már láttuk, Magyarországon is stratégiai politikai döntéshez kötött a nemzeti biztonságot sértő vagy fenyegető rendszerekkel szembeni katonai kibertérműveleti fellépés.

Annak érdekében azonban, hogy ez a képesség is közvetlenül elérhető legyen alacsonyabb vezetési szinten is, a következő megoldások alkalmazhatóak: a stratégiai, a hadműveleti és a harcászati szint közötti kapcsolat és együttműködés megvalósítása például a haderőnemek kötelékében lévő kiberműveleti összekötő tisztek, valamint a Kibervédelmi Központban található *reachback* képességeken, illetve az innen telepíthető OCO- és DCO-képességeken keresztül; döntéshozatali szcenáriók kidolgozása és a döntési jogkör automatikus delegálása a hadseregparancsnok vagy a kiberparancsnok szintjére, utólagos törvényhozói vagy kormányzati jóváhagyással, amennyiben szükséges.

FELHASZNÁLT IRODALOM

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020/81., 2101–2119. https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/

2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről. https://net.jogtar.hu/jogszabaly?docid=a1100113.tv

42/2020. (VIII. 14.) HM utasítás egyes NATO egységesítési egyezmények nemzeti elfogadásáról. Magyar Közlöny, 2020/46., 4296.

Ackerman, Robert K.: *Army Extending Cyber Capabilities*. Signal Magazine, 17. 02. 2021. https://www.afcea.org/content/army-extending-cyber-capabilities

AJP 3.20 – Allied Joint Doctrine for Cyberspace Operations. Edition A, Version 1. January 2020. NATO Standardization Office (NSO). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

A Magyar Honvédség Parancsnoksága. https://honvedelem.hu/a-magyar-honvedseg-parancsnoksaga.html

Caton, Jeffrey L.: *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications.* U.S. Army War College, 2015. https://www.files.ethz.ch/isn/187504/pub1246.pdf

Cluzel, François du: *Cognitive Warfare*. Innovation Hub, NATO ACT, June–November 2020. https://www.innovationhub-act.org/sites/default/files/2021-01/20210113_CW%20Final%20v2%20.pdf

Cyberspace Operations Concept Capability Plan 2016–2028. TRADOC Pamphlet 525-7-8. 22. 02. 2010. https://fas.org/irp/doddir/army/pam525-7-8.pdf

[48] MHP: i. m.

[49] Kovács: i. m. 12.

Dévai Dóra: *A kiberképességek fejlesztése és integrációja az Amerikai Egyesült Államok haderejében*. In: Hausner Gábor (szerk.): Szemelvények a katonai műszaki tudományok eredményeiből I. Hallgatói kötet. Ludovika Egyetem Kiadó, 2021, 83–97. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16208/905_KDMI_II_hallgatoi_tanulmanykotet.pdf

Draveczki-Uri Ádám: *Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül*. *Interjú dr. Kovács László dandártábornokkal.* Honvédelem.hu, 2020. 07. 03. https://honvedelem.hu/hirek/hazai-hirek/egy-korszeru-harckocsi-is-szamitogep-halozat-csak-70-tonna-vas-veszi-korul.html =

Haig Zsolt: *Információs műveletek a kibertérben*. Dialóg Campus, 2018. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12651/web_PDF_Informacios_muveletek_a_kiberterben.pdf;jsessionid=3C9322D937E5956BBE25D745755A8DFD?sequence=1

Hegedűs Ernő – Hennel Sándor: *Többdimenziós (multidomain) hadműveletek*. Hadtudomány, 2020/2., 3–28. https://www.mhtt.eu/hadtudomany/2020/2020_2szam/HT-2020-2_Egyben_col_PDF-A_WEB.pdf, DOI: 10.17047/HADTUD.2020.30.2.3

Joint Publication 3-12 – Cyberspace Operations. US Joint Chiefs of Staff, 08. 06. 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Jones, Peter L. – Waddell, Ricky – Blythe, Wilson C. Jr. – Pappas, Thomas: *Russian New Generation Warfare. Unclassified Summary of the U.S. Army Training and Doctrine Command Russian New Generation Warfare Study*. TRADOC G-2, US Army, 2016. https://www.armyupress.army.mil/Portals/7/online-publications/documents/RNGW-Unclassified-Summary-Report.pdf?ver=2020-03-25-122734-383

Kovács László: *A kiberbiztonság és a kiberműveletek megjelenése Magyarország új nemzeti biztonsági stratégiájában.* Honvédségi Szemle, 2020/5., 3–18. https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/120, DOI: 10.35926/HSZ.2020.5.1

Lin, Herbert – Zegart, Amy (eds.): *Bytes, Bombs, and Spies – The Strategic Dimensions of Offensive Cyber Operations.* The Brookings Institution, Washington D.C., 2018. https://play.google.com/books/reader?id=eMhyDwAAQBAJ&hl=hu&pg=GBS.PA23

Military Units. Department of Defense. https://www.defense.gov/Experience/Military-Units/Air-Force/#air-force

Pernik, Piret: *Preparing for Cyber Conflict: Case Studies of Cyber Command.* International Center for Defence and Security, Tallinn, 12. 2018. https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf

Pomerleau, Mark: *A force in flux: Military adjusts to emergent domains of warfare*. C4ISRNET, 02. 05. 2017. https://www.c4isrnet.com/intel-geoint/isr/2017/05/02/a-force-in-flux-military-adjusts-to-emergent-domains-of-warfare/

Pomerleau, Mark: A new company-level unit to support information warfare. C4ISRNET, 08. 07. 2020. https://www.c4isrnet.com/information-warfare/2020/07/08/heres-what-tactical-army-cyber-units-will-use-to-conduct-operations/

Pomerleau, Mark: *Authorities Complicate Use of Cyber Capabilities.* Part 1. Fifth Domain, 09. 01. 2017. https://www.fifthdomain.com/home/2017/01/09/authorities-complicate-the-use-of-cyber-capabilities/

Pomerleau, Mark: *Here's How DoD Organizes Its Cyber Warriors*. Fifth Domain, 25. 07. 2017. https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/

Pomerleau, Mark: *Here's how the Air Force is fighting in the cyber domain*. Fifth Domain, 28. 07. 2017. https://www.fifthdomain.com/dod/air-force/2017/07/28/heres-how-the-air-force-is-fighting-in-the-cyber-domain/

Pomerleau, Mark: *What Cyber Command's ISIS operations means for the future of information warfare*. C4IRSNET, 18. 06. 2020. https://www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-means-for-the-future-of-information-warfare/

Porche, Isaac R. III – Paul, Christopher – Serena, Chad C. – Clarke, Colin P. – Johnson, Erin-Elizabeth – Herrick, Drew: *Tactical Cyber. Building a Strategy for Cyber Support to Corps and Below*. RAND Corporation, Santa Monica, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf

Ruderman, David: *Command establishes enlisted pathways to become a cyber operations specialist*. U.S. Army Human Resources Command Public Affairs, 10. 06. 2015. https://www.army.mil/article/149776/command_establishes_enlisted_pathways_to_become_a_cyber_operations_specialist

Schulze, Matthias: *Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations.* In: Jančárková, Taťána – Lindström, Lauri – Signoretti, Massimiliano – Tolga, Ihsan – Visky, Gábor (eds.): 2020 – 12th International Conference on Cyber Conflict – 20/20 Vision: The Next Decade. NATO CCDCOE, Tallinn, 183–198. https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf

Szakértői közlés. NKE Nemzetbiztonsági Szakkollégium Workshop, 2021. 04. 28.

US Army Cyber Command. https://www.arcyber.army.mil/

U.S. Cybercommand. https://www.cybercom.mil/About/History/

U.S. Military Units. Department of Defense. https://www.defense.gov/Multimedia/Experience/Military-Units/Army/#army