Szemelvények a katonai műszaki tudományok eredményeiből II.

Hallgatói kötet

Szerkesztette
Hausner Gábor

LUDOVIKA
EGYETEMI KIADÓ

Szemelvények a katonai műszaki tudományok eredményeiből II.

Szemelvények a katonai műszaki tudományok eredményeiből II.

Hallgatói kötet

Szerkesztette

Hausner Gábor

LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2021

Szerzők

Ambrus Éva
Bodnár László
Csanádi Győző
Deák Veronika
Dévai Dóra
Domán László
Goda Zoltán
Huszár Péter
Huszár Viktor
Katona Gábor
Kralovánszky Kristóf
Kretz András
Kutassy Emese
Lakatos Bence Roland
Matusz Márk Péter
Olajosné Lakatos Boglárka
Priváczkiné Hajdu Zsuzsanna
Salamon Endre
Takács Krisztina
Terék Tamás
Tímár Attila

Szakmai lektorok

Bíró Tibor
Haig Zsolt
Padányi József
Palik Mátyás
Pohl Árpád
Restás Ágoston

Ludovika Egyetemi Kiadó
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Koltay András rektor
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Oláh Andrea
Korrektor: Bíró Csilla, Bujdosó Hajnalka
Tördelőszerkesztő: Fehér Angéla

ISBN 978-963-531-441-6 (PDF) | ISBN 978-963-531-442-3 (ePub)

Tartalom

Ambrus Éva

A kiberképességekhez szükséges szervezeti háttér

Bevezetés

A katonai műveletek negyedik dimenziója a kibertér[1] Hasonlóan a többi dimenzióhoz, osztozik benne a katonai és a civil élettér, elkülönítésük azonban nehezebb. A kibertér adta új típusú fenyegetések másként, eltérő súlyban érintik az egyéneket, a gazdasági szervezeteket és az államokat. E fenyegetésekre válaszként nemzetközi és állami szinten is létrejöttek kibervédelmi jogszabályok, stratégiák és ezeknek folyományaként a kibervédelmi és kiberműveleti szervezetek. E változásokat lekövetve, a Magyar Honvédségen belül és a NATO-szövetségi szinten is folyamatos fejlesztések folynak a kiberképességek területén. A tanulmány arra keresi a választ, hogy miként sikerült a kiberképességeket beilleszteni a honvédség szervezeti struktúrájába, amely folyamatra kihatással van az a kérdéskör, hogy milyen tevékenységeket értünk kiberműveletek alatt: defenzív, reagáló vagy offenzív hozzáállást? Ennek tükrében jelen cikk célja a hazai és a NATO-kiberstruktúrák, valamint a katonai kiberszervezetek elméleti életciklusának bemutatása. Végezetül a szervezetek humán oldalának vizsgálatára kerül sor, benne a személyi állomány és a képzési területek.

Kiberképességek megvalósulása a szervezeti struktúrában

Max Smeets tanulmányában[2] összegezte az offenzív katonai kiberszervezetek létrehozásának előnyeit és kihívásait. A nemzeti katonai kiberparancsnokságok szervezeti felépítése radikálisan eltérő képet mutat az egyes államok között annak tükrében, hogy azok mennyire központosítottak, mekkora méretűek és milyen felelősségi körük van. Az egyik alapvető dilemma a szerző szerint az államok részéről annak kérdése, hogy integrálják-e (és ha igen, hogyan) a felderítési és katonai képességeiket a támadó kiberkapacitás fejlesztéséhez.

Smeets három előnyt és kockázatot azonosított.[3] Egy ilyen integráció előnye, hogy 1) biztosíthatja a hírszerzés és a katonai tevékenységek hatékonyabb együttműködését, amely fontos szerepet játszik a kiberműveleteknél mint támogató művelet; 2) a szervezeti integráció növeli a közvetlen és közvetett tudásátadást és 3) lehetővé teszi az erőforrások hatékonyabb elosztását, csökkenti a feladatok közötti átfedéseket. A kockázatok közül

---

[1] A NATO besorolása szerint az ötödik dimenzió az űr.

[2] Max Smeets: *NATO members' organizational path towards conducting offensive cyber operations: a framework for analysis. 2019 11th International Conference on Cyber Conflict: Silent Battle.* Tallinn, NATO CCD CoE Publications, 2019. 1–15

[3] Max Smeets: Integrating offensive cyber capabilities: meaning, dilemmas, and assessment. *Defence Studies,* 18. (2018), 4. 395–410.

az első az úgynevezett kiberbiztonsági dilemma, azaz a klasszikus biztonsági dilemma megjelenése a kibertérben, elindítva egyfajta támadókapacitás-fejlesztési versenyt elrettentés céljából. A második kockázat a költségek, miután nem elégséges egy kezdeti beruházás, folyamatos fejlesztések kellenek a területen, beleértve a humánerő-fejlesztést és -megtartást. Végül a szervezeti integráció jelentheti az eredeti küldetés kiterjesztését is, azaz a katonai kiberszervezetek „kibermindenessé" válhatnak, és olyan feladatokat is elláthatnak, amelyek nem kötődnek szigorúan véve az eredeti küldetésükhöz.

Katonai kiberszervezetek elmélete és életciklusa

A katonai kiberszervezet egy nemzeti kormány fegyveres erőin belüli parancsnokságként, szolgálatként vagy egységként definiált szervezet, amelynek felhatalmazása és feladata a kiberműveletek végrehajtása. A kiberműveletek általánosságban magukban foglalnak támadó, védekező és felderítő képességeket.[4] Ezek a szervezetek eltérőek aszerint, hogy az adott országnak milyen stratégiai célkitűzései vannak, illetve milyen a jogi, szervezeti környezetük, milyen széles vagy szűk műveleti hatáskörrel rendelkeznek, mekkora létszámmal dolgoznak, milyen együttműködés van a katonai, rendvédelmi és polgári szervek között.

Max Smeets tanulmányában az üzleti menedzsment szakirodalomban ismert úgynevezett „üzleti életciklus" fogalmát alkalmazza a katonai kiberszervezetekre. Meglátása szerint egy szervezet fejlődése több szakaszra osztható, amelynek vannak mérföldkövei. Ennek részleteit az alábbi táblázat mutatja be:[5]

1. táblázat: Kiberszervezetek életciklusa[6]

Szint	Leírás
1. Ötletelés	A kormány elismeri az offenzív kiberberuházások fontosságát, és beszél a szervezet létrehozásának szükségességéről
2. Fejlesztés indítása	Politikai felhatalmazás van a szervezet létrehozására
3. Növekedés	A szervezet a tényleges működési kapacitás felé mozdult el
4. Kiterjesztés	A szervezet többször is offenzív kiberműveleteket hajtott végre, és felméri a további fejlesztési lehetőségeket
5. Érettség	A szervezet képes teljes spektrumú műveleteket végezni

Forrás: a szerző szerkesztése

Ez az életciklus nem lineáris trend, a szervezetek idővel előrehaladhatnak és visszafejlődhetnek. A tanulmány szerzője több pontot is kiemel az életciklussal kapcsolatban.

Először is a katonai kiberszervezetek nem politikai és szervezeti légüres térben alakulnak ki, hanem gyakran szervezetátalakítással vagy egyesítés révén jönnek létre. Másodszor, nem egyértelmű, hogy létezik-e érettségi szakaszban lévő katonai kiberszer-

[4] Joint Publication 3–12: Cyberspace Operations. II-4 – II-6. *Jcs.mil,* 8 June 2018.
[5] Smeets (2019) i. m. 4.
[6] Smeets (2019) i. m. 4.

vezet. Harmadszor, noha egyes államok jelentős költségvetést szántak a kiberszervezetükre, a legtöbb aspiráló NATO-kiberhatalomnak továbbra is meglehetősen alacsony költségvetés áll a rendelkezésére. A költségeken kívül a szerző kiemelten fontosnak tartotta, hogy a támadó kiberműveletek a küldetés szerves részeként jelenjenek meg, és bevethetők legyenek.[7]

Magyarország tekintetében az 1. szint a 2020. évi Nemzeti Biztonsági Stratégiában jelenik meg, ahol hangsúlyozzák a kiberképességek fejlesztésének fontosságát. A 2. szint, a fejlesztés indítása 2019-ben kezdődött el, a Magyar Honvédség Parancsnoksága (MHP) Kibervédelmi Szemlélőség, majd a Kibervédelmi Akadémia létrehozásával. Jelenleg a 3. szinten tartunk a valószínűsíthető kiberműveleti központ vagy parancsnokság fejlesztésével. Ahhoz, hogy a növekedési stádiumból a 4., kiterjesztési stádiumba érjen egy szervezet, szükséges az integráció és az áramvonalasítás a hatékonyság növeléséhez. A tanulmány elsősorban a katonai kibervédelemre fókuszál, azonban a polgári oldalon is többszintű koordináció és feladatmegosztás létezik jelenleg. Mindamellett, hogy fontos a terület felügyelete, egyben lassíthatja a válaszadási folyamatokat. A kibertérből érkező fenyegetések és kockázatok folyamatosak és gyors reagálást igényelnek. Az áramvonalasítás hozzájárulna az időbeli kihívásoknak való megfelelésnek, továbbá átláthatóbbá tenné a feladat- és felelősségi köröket. Példaként említhető a német szövetségi kiber- és információs parancsnokság (*Cyber-und-Informationsraum* – CIR), amely a német hadsereg hatodik ágává vált – a hadsereggel, a haditengerészettel, a légierővel, a közös orvosi szolgálattal és a közös támogató szolgálattal azonos szinten. A CIR alatt helyezkednek el a híradó-, a pszichológiai műveleti, a stratégiai felderítési (beleértve a SIGINT-et, a rádióelektronikai felderítést), a földrajzi információs (katonai műholdak) és az elektronikai hadviselés egységei.[8] Egy ehhez hasonló szervezet – és feladatintegráció – együtt jár a profiltisztítással is, mindazonáltal üzenetértékű a külvilág felé a változó stratégiai prioritásokról. Jelenleg Magyarországon a honvédelmi területen az incidenskezeléseket és a koordinációt a Katonai Nemzetbiztonsági Szolgálat (KNBSZ) végzi, míg az Magyar Honvédség (MH) kibervédelmének szervezése és a kiberműveleti erők felkészítése a szemlélőség feladata.

NATO

Mindamellett, hogy a NATO mindig is védte az információs és kommunikációs rendszereit, a 2002. évi prágai csúcstalálkozón került először napirendre a kibervédelem ügye, miszerint a Szövetségnek *meg kell erősítenie a kibertámadások elleni védekezési képességeit*.[9] A 2014. szeptemberi walesi csúcstalálkozón jóváhagyták az új kibervédelmi szakpolitika irányvonalait és az ahhoz kapcsolódó cselekvési tervet. Ezek mellett

[7] Smeets (2019) i. m. 10.

[8] Aufstellung Kommando CIR: Ein Meilenstein deutscher Sicherheits- und Verteidigungspolitik. *Bundesministerium der Verteidigung,* 05. 04. 2017.

[9] Prague summit declaration. *North Atlantic Treaty Organization,* 21 Nov. 2002.

a kibervédelmet a NATO alapvető kollektív védelmi feladatának részeként ismerték el, amelyre a nemzetközi jog alkalmazandó.[10] A 2016-os varsói csúcson a kiberteret műveleti területként ismerték el, kiemelve a szövetség védelmi jellegét, és hangsúlyozva, hogy a kibertérben ugyanolyan hatékonyan kell tudnia megvédenie magát a Szövetségnek, mint a többi műveleti térben. Ezen a csúcstalálkozón fogadták el az úgynevezett Kibervédelmi Vállalások csomagot is, amelyben a tagállamok vállalták, hogy nemzeti kibervédelmüket, beleértve a hálózatokat, infrastruktúrákat, erőforrásokat, együttműködéseiket, oktatást és képzést, erőteljesen fejlesztik.[11]

2017-ben a szövetséges védelmi miniszterek jóváhagytak egy frissített kibervédelmi cselekvési tervet a kibertér műveleti területté való fejlesztéséről.[12] 2018-ban a brüsszeli csúcstalálkozón döntöttek arról, hogy az európai műveleti parancsnokságon belül (NATO SHAPE) létrehozzák a kiberműveleti központot (*Cyber Operational Center* – CyOC), amelynek feladata a NATO kiberműveleteinek koordinálása.[13] Jens Stoltenberg NATO-főtitkár egy 2019-es cikkben pontosította, hogy „egy súlyos kibertámadás kiválthatja az 5. cikkelyt a kollektív védelemről (amely értelmezés szerint egy szövetséges tagállam elleni támadást a teljes szövetség elleni támadásként értelmez) – ez egyben ellenlépéseket is feltételez".[14]

A támadó jellegű kiberképességek és használatuk ellentmondásos terület. A NATO és szövetségesei elismerik a nemzetközi jog érvényességét a kibertérre, alkalmazása mégis egyedi problémákat vet fel. Ilyen például a kibertámadások attribúciója, azaz annak bizonyítása, hogy „ki az elkövető" és „ki a megrendelő". A technikai kérdéseken túlmenően a megtévesztés is jelen van például az úgynevezett *false flag* taktikában,[15] és szerepet játszhatnak diplomáciai érzékenységek is.

Magyarország

A hazai stratégiai dokumentumokban 2012-ben fogalmazódott meg a kibertér fenyegetéseivel szembeni védelem fontossága, és megjelent a kibertér hadszíntérként való meghatározása is.[16] A 2011. évi CXIII. törvény módosításával[17] a (katonai) kibertér törvényi szinten is megjelent a jogrendben. A magyar katonai kiberképességek kialakításának fő hazai kereteit a Nemzeti Biztonsági Stratégia,[18] a Nemzeti Katonai Stratégia,[19] a Nemzeti

[10] Wales summit declaration. *North Atlantic Treaty Organization,* 05 Sept. 2014.
[11] Cyber defense pledge. *North Atlantic Treaty Organization,* 08 Jul. 2016.
[12] Cyber defence. *North Atlantic Treaty Organization,* 25 Sept. 2020.
[13] Cyber defence. *North Atlantic Treaty Organization* (2020).
[14] Jens Stoltenberg: NATO will defend itself. *Prospect Magazine,* 2019.
[15] Brian Bartholomew – Juan Andres Guerrero-Saade: *Wave your false flags! Deception tactics muddying attribution in targeted attacks*. USA, Kaspersky Lab, 2016.
[16] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.
[17] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről. 40/A. A katonai kibertér műveletekre vonatkozó különös szabályok. 62/A. §.
[18] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[19] Magyarország Nemzeti Katonai Stratégiája. 2012.

Kibervédelmi Stratégia,[20] a Honvédség Kibervédelmi Szakmai Koncepciója[21] és a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program[22] jelölik ki, míg NATO szövetségi szinten a 2016-os varsói csúcstalálkozón elfogadott kibervédelmi vállalások[23] adják. A 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről kijelöli a Honvédség kiberképességeinek és műveleteinek alkalmazási, illetve fejlesztési területeit.[24] Jelenleg folyik a Nemzeti Katonai Stratégia, valamint az MH kiberműveleti doktrínájának kidolgozása. Ez utóbbi tartalmazza majd várhatóan részletesen a kiberműveletekre vonatkozó műveleti szabályokat, eljárásrendeket.

A 2012. évi Nemzeti Biztonsági Stratégiában[25] jelenik meg a kiberbiztonság, mint Magyarország biztonságát meghatározó tényező,[26] ebből eredően e térből fakadó fenyegetések és kockázatoknak a kezelése az állam feladata. A 2020. évi új Nemzeti Biztonsági Stratégiának a kiberbiztonságot érintő legfigyelemreméltóbb eleme a 101. pont, amely kijelenti, hogy „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges".[27] A Stratégiai Védelmi Kutatóintézet (SVKI) elemzése ezzel kapcsolatosan kiemeli, hogy ezzel beemelik a NATO walesi csúcsán is elfogadott, a válaszadás „kiber" vagy „fizikai" jellegű értelmezését.[28]

A 2012. évi Nemzeti Katonai Stratégiában is megjelenik a kibertér, kiberbiztonság fogalma, azonban egy lépéssel továbbmenve utal a kiberhadviselésre is: „a kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását."[29] Konkrét feladatként fogalmazza meg a dokumentum az MH tekintetében a Honvédség kibervédelmének erősítését, a rendszabályok kidolgozását, a megfelelő eszközök beszerzését és az állomány felkészítését,[30] azonban ennek keretei csak később valósulnak meg.

A 2013. évi Nemzeti Kibervédelmi Stratégia utal elsőként a magyar kibertérre mint fogalomra: „Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy

[20] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.
[21] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról.
[22] Benkő Tibor: A Magyar Honvédség jelene és jövője. *Hadtudomány,* 29. (2019), 1–2. 149–155.
[23] Cyber defense pledge. (2016) i. m.
[24] 2011. évi CXIII. törvény 62/A. §.
[25] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[26] Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018. 233.
[27] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[28] Csiki Varga Tamás – Tálas Péter: *Magyarország új nemzeti biztonsági stratégiájáról*. Stratégiai Védelmi Kutatóintézet, Elemzések, (2020), 17.
[29] Kovács (2018) i. m. 234.
[30] Kovács (2018) i. m. 236.

Magyarországra irányulnak, illetve amelyekben Magyarország érintett."[31] A feladatokat tekintve kijelenti, hogy „a meglévő és potenciálisan jelentkező kihívásokkal szemben ki kell alakítani egy hatékony megelőző, észlelési, reagálási képességet, amelybe a kibertámadások esetleges bekövetkezése esetén a helyreállítási képességek is bele kell, hogy tartozzanak".[32] Ez utóbbihoz kapcsolódóan konkrétabb feladatszabásként jelenik meg a kiberbiztonságot illetően a kormányzati koordináció és együttműködés erősítése, a megfelelő szakintézmények kialakítása, aktív részvétel a nemzetközi együttműködésekben, a kiberbiztonság jobb megjelenítése az oktatásban.[33]

A kiberképességek szervezeti kialakítása 2019-ben indult meg, amelynek állomásaként megnyitott a Magyar Honvédség Kiberakadémiája. A Magyar Honvédség Parancsnoksága (MHP) kibervédelmi szemlélője, Kovács László dandártábornok meglátása[34] szerint a kibervédelmi és kiberműveleti erők kiépítése, fejlesztése területén jó ütemben halad a Magyar Honvédség, a régióban hasonló dinamikában fejlődnek a képességek. Általánosságban elmondható, hogy a nemzeti képességfejlesztésekről kevés információ kerül nyilvánosságra, azonban valószínűsíthetően a legtöbb állam végez kiberfejlesztéseket. A kiberképességek körében megkülönböztethetők passzív és aktív védelmi képességek. A passzív védelmi képességek esetében saját hálózaton belüli hatókörű, főként megelőző, incidenskezelő, adat- és rendszerhelyreállító jellegű tevékenységeket értünk,[35] míg aktív védelmi képességek alatt egy fenyegetés megelőzésére vagy megakadályozására irányuló, saját hálózaton kívüli hatókörrel is rendelkező, támadó jellegű műveleti képességeket.[36]

A hazai katonai kiberképességeket tekintve két szervezetet kell kiemelni: a Katonai Nemzetbiztonsági Szolgálatot (KNBSZ) és az MHP-n működő kibervédelmi szemlélőséget. Előbbi feladatait a 2019. évi CV. törvény egyes törvények honvédelmi kérdésekkel összefüggő módosításáról 12. § (3) pontja állapította meg, így új feladatként jelentkezett, hogy a KNBSZ „információkat gyűjt a honvédelmi érdeket veszélyeztető kibertevékenységekről és -szervezetekről, jogszabály keretei között ellátja a honvédelmi ágazat elektronikus információbiztonsági feladatait, biztosítja a honvédelemért felelős miniszter által vezetett minisztérium, valamint a Magyar Honvédség Parancsnoksága információvédelmi tervező munkájához szükséges információkat, továbbá kibertér műveleti képességeivel ellátja a honvédelmi érdekek nemzetbiztonsági jellegű védelmét és a Magyar Honvédség kibervédelmének és műveleteinek támogatását".[37] A kibervédelmi képesség ennek tükrében jelent figyelő és információjelentő tevékenységet (defenzív

[31] 1139/2013. (III. 21.) Korm. határozat, (3) pont.
[32] 1139/2013. (III. 21.) Korm. határozat, (9) *a)* pont.
[33] 1139/2013. (III. 21.) Korm. határozat, (10) *a), b), c), e), g)* pontok.
[34] Draveczki-Ury Ádám: „Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül". *Honvedelem.hu,* 2020. 07. 03.
[35] Rain Liivoja – Maarja Naagel – Ann Väljataga: *Autonomous cyber capabilities under international law.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2019. 11.
[36] Dorothy E. Denning: Framework and principles for active cyber defence. *Computers & Security,* 40. (2013), 108–109.
[37] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, 6. § *g)* pont.

képességet), valamint beavatkozó tevékenységet (reagáló képességet).[38] Mint látható, explicit módon nem jelenik meg a támadó jelleg.[39]

A honvédelmi miniszter 3/2019. (I. 31.) HM utasításában, a honvédelmi szervezetek 2019. évi feladatainak, valamint a 2020–2021. évi tevékenységek fő irányainak meghatározásáról megjelenik „a jóváhagyott fejlesztési programok megvalósításának folytatása, figyelemmel a technikai adatszerző eszközpark korszerűsítésére, a honvédelmi szervezetek minősített összeköttetéseinek biztosítására, a honvédelmi ágazati szintű kibervédelmi képességfejlesztésre".[40] A 2019. évi éves beszámolóban[41] egyfelől megjelenik, hogy az MH fő feladatai Magyarország szuverenitásának, határainak – ezen belül területe, légtere és kibertere – védelméhez, valamint a szövetségi rendszerekben vállalt kötelezettségek ellátásához szükséges katonai képességek kialakítása és fenntartása, továbbá az ezekhez szükséges feltételrendszer biztosítása. Ennek biztosítása érdekében a KNBSZ „információkat gyűjt […] a honvédelmi érdeket sértő kiber-tevékenységről, továbbá a műveleti területén lévő alakulatok és azok állománya ellen irányuló törekvésekről és tevékenységekről".

A másik szervezet az MHP-n belüli Kibervédelmi Szemlélőség, amely az MHP-nak az MH kibervédelmének és kiberműveleti képességeinek stratégiai szintű képességkialakító, az MH kibervédelmi szakterülete fejlesztését irányító és felügyeletét ellátó önálló szervezeti egysége. Munkáját a szemlélő vezeti és irányítja az MHP, valamint az MH hadrendjébe tartozó katonai szervezetek kibervédelmi és kiberműveleti tevékenységét. Meghatározza a szakterülete vezetéséhez szükséges szervezeti kialakítás alappilléreit, struktúráját. Az MHP Infokommunikációs és Információvédelmi Csoportfőnökséggel együttműködve koordinálja a kibervédelmi képességfejlesztést, valamint harmonizálja ezen képességek kialakítását.[42] A kibervédelmi képességfejlesztés egyik első lépése a kibervédelmi képzések szervezetszintű létrehozása. E szervezetek közül elsőként az MH Kiberakadémiája jött létre, amelynek keretében történik a honvédségi állomány kibertudatossági képzése és kiberműveleti felkészítése. Ez utóbbi folyamatban van, elsődleges feladatuk a műveleti támogatás lesz. Az állomány felkészítése és kiképzése a terület fontossága és változékonysága miatt azt is jelenti, hogy állandóan naprakész információval és tudásanyaggal kell rendelkezni. Az együttműködés mind a szélesebb hazai szereplőkkel (társszervek, vállalatok, egyetemek) elengedhetetlen. A kiberképességeket érintően alapvetően védelmi (defenzív) tevékenységre fókuszálnak, azonban – ahogy a legtöbb ország – előreláthatólag offenzív képességekkel is fognak rendelkezni.

---

[38] Szentgáli Gergely: Csendben szolgálni. *Hadtudomány,* 25. (2015), 3–4. 85.

[39] Azonban az új Nemzeti Biztonsági Stratégiában már megjelenik, lásd 101. pont.

[40] 3/2019. (I. 31.) HM utasítás a honvédelmi szervezetek 2019. évi feladatainak, valamint a 2020–2021. évi tevékenysége fő irányainak meghatározásáról.

[41] XIII. Honvédelmi Minisztérium költségvetése. 2020.

[42] A Magyar Honvédség Parancsnoksága. *Honvedelem.hu,* 2020. 07. 31.

Támadó, védekező, támogató funkció

A kibervédelem mindenkinek feladata, az egyéntől az államokig. Egyéni szinten ez a megfelelő kiberhigiéné követéséből áll (például víruskereső program, tűzfal, megfelelő jelszavak használata). A szervezeteknek óvatosabbaknak kell lenniük, hiszen általában nagyobb a tétjük: egész informatikai rendszereket, eszközöket és információkat kell megvédeniük más szervezetekkel, bűnözőkkel vagy akár államokkal szemben.

Az *Encyclopedia of cyber warfare* című könyvben a kibervédelmet[43] a kiber ellenállóképesség szükséges, de nem elegendő részeként definiálták. Elsősorban az Egyesült Államok szemszögéből a fenyegetések elleni fellépést öt lépésre bontották le:

1) a támadások megelőzése;
2) óvás a támadásoktól, amikor azok bekövetkeznek;
3) tompítani a támadások hatását;
4) válaszolni a támadásokra;
5) helyreállni a támadásokból.

Általánosságban az adott állam felelős a kiberbiztonsági jogszabályok, szakpolitikák, szervezetek fejlesztéséért és fenntartásáért. Emellett szükséges összehangolnia a szakstratégiákat az oktatási és képzési rendszerrel az elegendő és megfelelő szakemberképzés érdekében. A korábban bemutatott szervezeti integrációról szóló részt figyelembe véve megfontolandó a kiberbiztonság beépítése a nemzetbiztonságba, ezáltal e dimenzióban is védve a kritikus infrastruktúrákat és a nemzeti szuverenitást.

Ennek a magasabb szintű védelmi rendszernek a következő fő céljai lehetnek:[44]

- *átirányítás:* elirányítja a támadó fél tevékenységét (célponttévesztés, megtévesztés);
- *kiküszöbölés:* hatástalanná teszi a támadók erőfeszítéseit;
- *akadályoztatás:* a támadó feleknek keményebben vagy hosszabb ideig kell dolgozniuk;
- *észlelés:* azonosítja a támadó tevékenységeket vagy azok hatását;
- *korlátozás:* a támadók hatékonyságát csökkentik a következmények korlátozásával;
- *kitettség:* a támadó fél veszít előnyéből a hírszerzési együttműködés fejlesztésével és megosztásával.

Nem feltétlenül az a legfontosabb, hogy az egyének felfogják a kibervédelem technikai részleteit, hanem egyszerűen meg kell érteniük, hogy a kibervédelem fontos. A támadók folyamatosan megpróbálnak kihasználni minden sérülékenységet, és az emberek a legkiszolgáltatottabb elemei minden számítógépes rendszernek. Ezért kiemelt figyelmet kell fordítani a képzésre és a tájékoztatásra.

A szakirodalomban nehéz pontos információkat találni az egyes államok támadó kiberképességeit illetően, érthető (biztonsági) okokból nagyon általánosan fogalmaznak e területen. Természetesen létezik tapasztalatcsere zárt fórumokon és esettanulmányok

[43] Paul J. Springer (ed.): *Encyclopedia of cyber warfare.* Santa Barbara, ABC-CLIO, 2017. 47.
[44] Springer (2017) i. m. 48.

feldolgozása. Az információáramlás nemcsak szövetségi és tagállami szinten történik, hanem a katonai és a civil szféra között is, hiszen a kibertér nem szigorúan elválasztható katonai és nem katonai területekre. Az elméleti részben kifejtett küldetés kiszélesítése *(mission creep)* azzal is járhat, hogy a hadsereg közreműködik a civil rendszerek védelmében, mint például teszi azt az Egyesült Államok kiberparancsnoksága az amerikai elnökválasztás kiber (vagy hibrid) befolyásolásának megakadályozása érdekében. Hazánk esetében ez a különleges jogrend esetében áll fenn.

Nemzetközi példák: Németország és Csehország

A kiberbiztonsági német nemzeti együttműködés alapja a német szövetségi kormány által 2016-ban elfogadott kiberbiztonsági stratégia.[45] A kiberbiztonságért a német szövetségi belügyminisztérium felel, míg a 2016. évi fehér könyv kimondja, hogy a nemzeti kiberbiztonsági szerkezet védelmi vonatkozásai a német szövetségi védelmi minisztérium feladatai, és alkotmányosan a Bundeswehrhez van rendelve.[46]

Németország esetében 2017. április 5-én állt fel bonni székhellyel a Kiber- és Információs Parancsnokság (*Kommando Cyber- und Informationsraum* – KdoCIR), amely a Bundeswehr kibertevékenységet végző egységeit olvasztotta magába, és a kiber-, IT- (hálózati), katonai hírszerzési, geoinformációs és műveleti kommunikációért felelős.[47] A kiberparancsnokság alá két korábbi önálló parancsnokságot és egy központot rendeltek: a stratégiai felderítő parancsnokságot (*Kommando Strategische Aufklärung,* Gelsdorf), a Bundeswehr informatikai parancsnokságát (*Kommando Informationstechnik der Bundeswehr,* Bonn), valamint a Bundeswehr geoinformációs központját (*Zentrum für Geoinformationswesen der Bundeswehr,* Euskirchen). Ez mintegy 13 500 fős állományt foglal magában.[48]

A kiber- és az információs műveletek parancsnoksága[49] biztosítja Csehország biztonságát és védelmét a kiber- és információs területen, amely 2019-ben állt fel. Létszámát 500 fő hivatásos állomány teszi ki.[50] Taktikai szinten figyelemmel kísérik, tervezik és ellenőrzik a kiber- és információs műveleteket, ideértve a Cseh Köztársaság hadseregének stratégiai kommunikációs (STRATCOM) támogatását is. A parancsnokság erői képesek megvédeni a cseh kiberteret, valamint információs, pszichológiai és civil-katonai műveleteket végrehajtani. A kibervédelem területén szorosan együttműködnek

[45] Samuel Rothenpieler: *National Cyber Security Strategy 2016.* Athens, 26th of April 2017.
[46] White paper on German security policy and the future of the Bundeswehr. *The Federal Government,* 2016. 38.
[47] Aufstellung Kommando CIRCyber- und Informationsraum: Ein Meilenstein deutscher Sicherheits- und Verteidigungspolitik. *Bundesministerium der Verteidigung,* 05. 04. 2017.
[48] *Bundesministerium der Verteidigung* (2017).
[49] Cyber forces command. *Ministry of Defence and Armed Forces of the Czech Republic,* February 27, 2020.
[50] Czech military cyber forces might have headquarters in Brno. *Prague Monitor.*

a katonai hírszerzéssel, és egyéni képességeik kiegészítik egymást.[51] A cseh kormány kibervédelmi stratégiájában fogalmazták meg 2018-ban, hogy „fejleszteni kell [a kiber] képességeit a katonai műveletek támogatására. Ezek taktikai szintig lefedik az operatív tevékenységeket, és magukban foglalják a harci támogatást más területeken, valamint a kizárólag a kibertérben végrehajtott műveleteket."[52]

Képzés és állomány

A hadsereg kötelékében, a kibervédelemben dolgozó hivatásos katonákat szokták kiberharcosoknak is nevezni.[53] Tevékenységüket tekintve folytathatnak támadó vagy védekező kiberműveleteket, céljuk a stabil és biztonságos kibertér fenntartása és biztosítása. Kétség sem férhet hozzá, hogy a technológia (és a technológiai fölény) fontos a kibertérben és a kiberműveletekben, de a műveletek sikerét továbbra is az egyének határozzák meg. Az amerikai hadsereg négy olyan értéket vázolt fel, amelyek a kiberharcosokat jellemzik:

1. professzionalizmus, a kiberműveletekben képzett elit csapatok;
2. bizalom;
3. fegyelem;
4. precizitás (a járulékos károk ugyanolyan károsak lehetnek a virtuális térben, mint bármely más harctéren).[54]

Nagy igény van a munkaerőre, több hadsereg nemcsak hivatásosokat, hanem civil szerződéseseket is alkalmaz ezen a területen. Azonban kihívást jelent a munkakörök, feladatok és hatáskörök meghatározása, a párhuzamosságok elkerülése. A szaktudást érintően egyeseket a szükséges képzettséggel vesznek fel, de sok pozíciót belső képzési lehetőségek által töltenek fel. A verseny a szakemberekért kihívást jelent, azonban ez nemcsak az informatikai szakembereket jelenti, hanem a kibervédelemhez kapcsolódó műveleti, jogi szakpolitikához értőket is.

A Magyar Honvédségen belül az oktatási és felkészítési feladatokat a korábban ismertetett Kibervédelmi Akadémia látja el. Ahogyan a többi nemzeti hadseregben, így hazánkban is civileket és hivatásosokat alkalmaznak ezen a területen, különböző szaktudási szinteken. NATO szinten a Kibervédelmi Kiválósági Központ (*NATO Cooperative Cyber Defence Centre of Excellence* – CCD CoE)[55] a tapasztalat- és információcsere, a képzés és a kutatás területén kiemelten fontos szerepet tölt be, ezen képzéseken

[51] *Cyber forces command.* 2020.
[52] *Cyber defence strategy of the Czech Republic 2018–2022.* National Cyber Operations Center, 2018. 11.
[53] Springer (2017) i. m. 75–67.
[54] Springer (2017) i. m.
[55] NATO Cooperative Cyber Defence Centre of Excellence.

a magyar szakemberek is rendszeresen részt vesznek. A kibergyakorlatok – amikor egy kibertámadást szimulálnak különböző szinteken – a gyakorlati képességfejlesztést segítik elő. Az előbb említett kiválósági központon túl a NATO több oktatási programot indított az elmúlt években. A Kommunikációs és Információs Ügynökség (*NATO Communication and Information Agency* – NCIA)[56] létrehozott egy külön információstechnológiai rendszereket oktató iskolát, míg a római Védelmi Főiskola (*NATO Defence College* – NDC)[57] az elméleti és szakpolitikai kutatásban vesz részt.

Az oktatandó témakörök lehetnek:

- szervezeti struktúrák, beleérve a szerepeket és felelősségi köröket mind nemzeti (katonai és polgári), mind nemzetközi (NATO, EU) szinten;
- a stratégiai és műveleti tervezés, azon belül, hogy hogyan és hol kapcsolódik vagy kapcsolódhat be egy kiberművelet;
- a technikai képzések a kibertérről, kezdve a fizikai infrastruktúrától egészen a szofisztikáltabb támadásokig;
- a kiberképességek nemzeti és szövetségi szinten, beleértve a védelmi és támadóképességeket;
- a kiberműveletek jogi és szakpolitikai környezetének megismerése, a nemzetközi jog megjelenését a kibertérre vonatkozóan, a különböző nyilatkozatokat és irányelveket.[58]

A RAND tanulmányában[59] három szinten javasolja a kibergyakorlatok megvalósítását: taktikai, műveleti és stratégiai szinten. Taktikai szinten először egyéni és katonai egység szinten kell a képzéseket tartani, majd ezek után NATO taktikai kibergyakorlatokon részt venni. Műveleti szinten először forgatókönyveken alapuló vezetési és irányítási gyakorlat lenne megfelelő, majd a műveleti parancsnoksági szinten történik a kibergyakorlatok végrehajtása. Stratégiai szinten először szakpolitikai kerekasztalt, majd gyakorlati, forgatókönyveket létrehozó gyakorlatokat lehetne végezni. E háromszintű gyakorlati képzés végül először NATO vezetési és irányítási, illetve NATO-kibergyakorlattá alakulna, majd egy, a kiberképességek és -műveletek teljes spektrumát megjelenítő NATO-gyakorlatot eredményezne. Ez a folyamat elősegítené a szövetségen belüli interoperabilitást.

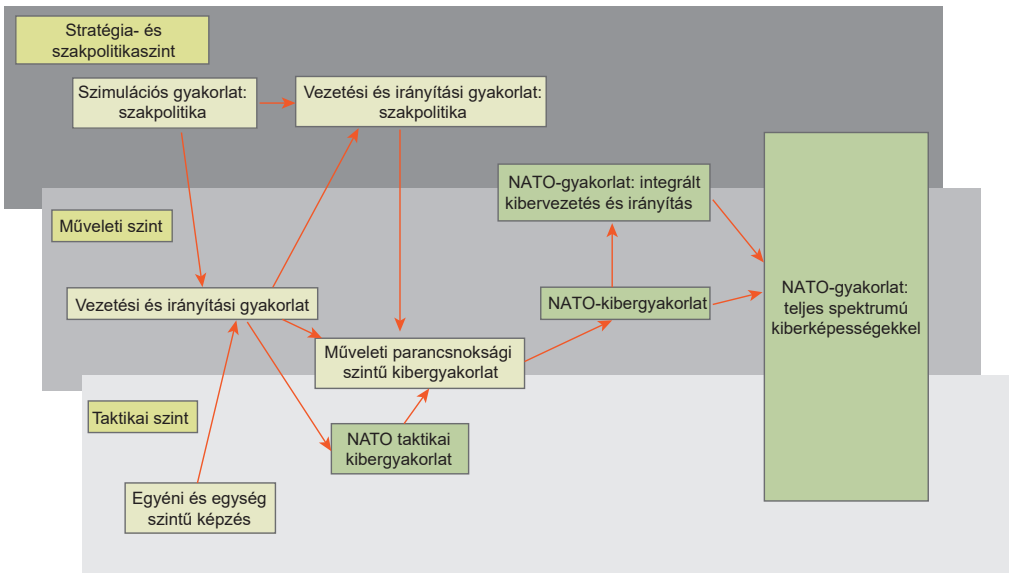
---

[56] NATO Communication and Information Agency.

[57] NATO Defense College.

[58] Lillian Ablon et alii: *Operationalizing Cyberspace as a Military Domain. Lessons for NATO.* Santa Monica, RAND Corporation, 2019. 16–17.

[59] Ablon et alii (2019) i. m. 13.



1. ábra: Javaslat a gyakorlatra
Forrás: Ablon et alii (2019) i. m.

A kiberműveletek és a kibertámogatás beemelése az összhaderőnemi folyamatokba kritikus. Első lépésként a szervezeti átalakításokat érdemes meghatározni, azaz hogy hogyan integrálódnak majd a hagyományos fegyveres erők kötelékébe. Ez a szervezet minden szintjére igaz, hiszen a kiberműveletek jelenleg támogató jellegűek a műveleti szinten, azonban a stratégiai szinten kell a jóváhagyás. A műveleti szintű kibergyakorlatok eredményei ideális esetben megjelennek a műveleti tervezési és végrehajtási folyamatokban, ezáltal segítve a (hazai) felkészülést, a kiberműveletek tervezését, végrehajtását, értékelését. Ez az integrációs folyamat – azaz a kibertér műveleti területté, alkalmassá tétele – folyamatban van, mind nemzeti, mind NATO-szinten.

Következtetések

A kibertér mint negyedik dimenzió a hadviselésben, régebben megjelent elméletben, mint a gyakorlatban. A kiberképességek integrálása a hagyományos katonai szervezetben több kérdést vet fel egyfelől a támadóképességek fejlesztésének fontosságáról, másfelől a konkrét szervezeti átalakításról, hiszen jelenleg a kiberműveletek támogató funkciót látnak el. Ahogyan a kiberképességek fejlődnek, és a terület fontossága növekszik, ezt felismerve elképzelhető egy tényleges összhaderőnemi integrálódás. Magyarország e tekintetben nincs elmaradva. Az új Nemzeti Biztonsági Stratégia egyértelműen kijelöli a fejlesztési irányokat, amelyek a hamarosan megjelenő szakpolitikai stratégiákban is tükröződni fognak. Szervezetileg is elindult egy fejlesztés a *Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program* keretében, a létrejött Kibervédelmi Akadémiával és az ala-

kulófélben lévő kiberparancsnoksággal. Mindazonáltal a nemzetközi példákat látva a további szervezeti átalakításnak is lennének hozadékai, mind a személyi felkészültség összevonása és tudásátadása, mind a hatékonyságnövelés szempontjából. Az információs műveletek égisze alatt a pszichológiai műveletek, a kiberműveletek és a többi nem kinetikus képesség koordinált alkalmazása elengedhetetlennek tűnik, ahogy azt több ország már felismerte. Ez azonban nem egy új keletű kérdés, hiszen az információs műveletek tudományos irodalma ezt már korábban is tárgyalta.

Egy ilyen összhaderőnemi integrálódás azonban minden állam és szervezet számára rendkívüli költségeket jelent mind technikai, mind személyi állomány tekintetében. A legtöbb állam számára kihívás a megfelelő képzettségű szakemberek képzése és szervezetben való tartása. Ennek megoldásaként átgondolandó az elvárt képzési szintek meghatározása, a belső és külső továbbképzések szervezése és a meglévő állomány át- és továbbképzése. Ezt a feladatot látja el a 2019-ben felállított Kibervédelmi Akadémia a Kibervédelmi Szemlélőség felügyelete alatt. A képzések területén a Nemzeti Közszolgálati Egyetemen 2007 óta létezik a védelmi infokommunikációs rendszertervező mesterképzési szak, valamint 2019-ben elindult kiberbiztonsági mesterképzési szak. A felsőfokú, egyetemi végzettséget adó képzéseken túl – miután nem minden feladat ellátására szükséges ennyire elmélyült tudás – érdemes lenne egyfelől rövidebb, általánosabb részképzéseket, kurzusokat is figyelembe venni, amellyel a más szakterületekről érkező állomány készülhetne fel; másfelől az általános képzésen túl szakfeladatra szabott moduláris képzéseket.

A támadó kiberképességek fejlesztése magával vonhat egyfajta kiberbiztonsági dilemmát is, miután az államok – elrettentés céljából – nemcsak védekező, hanem támadó képességeiket is fejleszteni fogják. Ez komoly kihívást és egyben egyensúlyra törekvést jelent nemzeti és európai szinten. A nemzetközi környezetben jelenleg kevés, mindenki által elfogadott norma van, és a megengedett, megengedhető válaszlépések sem tisztázottak. A terület mindenképpen folyamatos figyelmet és felügyeletet érdemel, kiemelve az együttműködést mind a katonai és a civil szektor között, mind a szövetség szintjén, miután jelenleg egy közös kibertér létezik.

Felhasznált irodalom

3/2019. (I. 31.) HM utasítás a honvédelmi szervezetek 2019. évi feladatainak, valamint a 2020–2021. évi tevékenysége fő irányainak meghatározásáról. Online: https://magyarkozlony.hu/dokumentumok/4318de0071e1f86c5e8b65a8775f95b18d4deecf/megtekintes

60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról. Online: https://net.jogtar.hu/getpdf?docid=A13U0060.HM&targetdate=&printTitle=60/2013.+%28IX.+30.%29+HM+utas%C3%ADtás&getdoc=1

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Online: https://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Online: https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf

1162/2020. (IV.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Online: www.kozlonyok.hu/nkonline/index.php?menuindex=200&pageindex=kozltart&ev=2020&szam=81

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. Online: https://net.jogtar.hu/jogszabaly?docid=99500125.tv

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

2019. évi CV. törvény egyes törvények honvédelmi kérdésekkel összefüggő módosításáról. Online: www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK19205.pdf

XIII. Honvédelmi Minisztérium költségvetése. 2020. Online: www.parlament.hu/irom41/10710/adatok/fejezetek/13.pdf

Ablon, Lillian et alii: *Operationalizing Cyberspace as a Military Domain. Lessons for NATO.* Santa Monica, RAND Corporation, 2019. 1–42. Online: www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf

A Magyar Honvédség Parancsnoksága. *Honvedelem.hu,* 2020. 07. 31. Online: https://honvedelem.hu/a-magyar-honvedseg-parancsnoksaga.html

Aufstellung Kommando CIR: Ein Meilenstein deutscher Sicherheits- und Verteidigungspolitik. *Bundesministerium der Verteidigung,* 05. 04. 2017. Online: www.bmvg.de/de/aktuelles/aufstellung-kommando-cir-11120

Bartholomew, Brian – Guerrero-Saade, Juan Andres: *Wave your false flags! Deception tactics muddying attribution in targeted attacks*. USA, Kaspersky Lab, 2016. Online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf

Benkő Tibor: A Magyar Honvédség jelene és jövője. *Hadtudomány,* 29. (2019), 1–2. 149–155. Online: http://mhtt.eu/hadtudomany/2019/2019_1_2/2019eA%20Magyar%20Honvédseg%20jelene_Benko%20Tibor.pdf

Cyber defence. *North Atlantic Treaty Organization,* 25 Sept. 2020. Online: www.nato.int/cps/en/natohq/topics_78170.htm

Cyber defense pledge. *North Atlantic Treaty Organization,* 08 Jul. 2016. Online: www.nato.int/cps/en/natohq/official_texts_133177.htm

Cyber defence strategy of the Czech Republic 2018–2022. National Cyber Operations Center, 2018. Online: www.vzcr.cz/uploads/69-Cyber-Defence-Strategy-2018.pdf

Cyber forces command. *Ministry of Defence and Armed Forces of the Czech Republic,* February 27, 2020. Online: www.army.cz/en/armed-forces/organisational-structure/cyb/cyber-forces-command-218593/

Csiki Varga Tamás – Tálas Péter: *Magyarország új nemzeti biztonsági stratégiájáról*. Stratégiai Védelmi Kutatóintézet, Elemzések, (2020), 17. Online: https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/SVKI_Elemzések_2020_17_Az%20új%20magyar%20Nemzeti%20Biztonsági%20Stratégiáról%20_(Csiki%20Varga%20T.%20%20-%20Talas%20P.).pdf

Denning, Dorothy E.: Framework and principles for active cyber defence. *Computers & Security,* 40. (2013), 108–109. Online: 10.1016/j.cose.2013.11.004

Draveczki-Ury Ádám: „Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül". *Honvedelem.hu,* 2020. 07. 03. Online: https://honvedelem.hu/hirek/hazai-hirek/egy-korszeru-harckocsi-is-szamitogep-halozat-csak-70-tonna-vas-veszi-korul.html

Joint Publication 3–12: Cyberspace Operations. II-4 – II-6. *Jcs.mil,* 8 June 2018. Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Kovács László: *Kiberbiztonság és -stratégia*. Budapest, Dialóg Campus, 2018. 233. Online: https://nke-repo.uni-nke.hu/xmlui/bitstream/handle/123456789/12639/web_PDF_Kiberbiztonsag_es_strategia.pdf;jsessionid=0810DA87496E6179B39358E605116DF1?sequence=1

Liivoja, Rain – Naagel, Maarja – Väljataga, Ann: *Autonomous cyber capabilities under international law.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), 2019. Online: https://ccdcoe.org/uploads/2019/07/Autonomy-in-Cyber-Capabilities-under-International-Law_260619-002.pdf

Magyarország Nemzeti Katonai Stratégiája, 2012. Online: https://2010-2014.kormany.hu/download/9/ae/e0000/nemzeti_katonai_strategia.pdf – !DocumentBrowse

NATO Communication and Information Agency. Online: www.ncia.nato.int/

NATO Cooperative Cyber Defence Centre of Excellence. Online: https://ccdcoe.org/

NATO Defense College. Online: www.ndc.nato.int/

Prague summit declaration. *North Atlantic Treaty Organization,* 21 Nov. 2002. Online: www.nato.int/cps/en/natohq/official_texts_19552.htm

Rothenpieler, Samuel: *National Cyber Security Strategy 2016.* Athens, 26th of April 2017. Online: www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf

Smeets, Max: Integrating offensive cyber capabilities: meaning, dilemmas, and assessment. *Defence Studies,* 18, (2018), 4. 395–410. Online: https://doi.org/10.1080/14702436.2018.1508349

Smeets, Max: *NATO members' organizational path towards conducting offensive cyber operations: a framework for analysis.* 2019 11th International Conference on Cyber Conflict: Silent Battle. Tallinn, NATO CCD COE Publications, 2019. 1–15. Online: https://ccdcoe.org/uploads/2019/06/Art_09_NATO-Members-Organizational-Path.pdf

Springer, Paul J. (ed.): *Encyclopedia of cyber warfare.* Santa Barbara, ABC-CLIO, 2017.

Stoltenberg, Jens: NATO will defend itself. *Prospect Magazine,* 2019. Online: www.prospectmagazine.co.uk/content/uploads/2019/08/Cyber_Resilience_October2019.pdf

Szentgáli Gergely: Csendben szolgálni. *Hadtudomány*, 25. (2015), 3–4. 77–90. Online: http://real.mtak.hu/29827/1/2015_3_4_8.pdf

Wales summit declaration. *North Atlantic Treaty Organization,* 05 Sept. 2014. Online: www.nato.int/cps/en/natohq/official_texts_112964.htm

White paper on German security policy and the future of the Bundeswehr. *The Federal Government,* 2016. Online: https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf

A Katonai Műszaki Doktori Iskolában folyó képzés és kutatás a műszaki tudományterülethez tartozó tudományágaknak a teljes védelmi szektorban történő alkalmazására irányul. A hallgatók tudományos tevékenységüket gyakran több tudományterület és tudományág határterületén művelik, és a kutatásaik során azok interdiszciplináris kérdéseire, szinergiáira fókuszálnak.

Mindezt az ebben a kötetben található írások is igazolják. A szerzők olyan tudományos problémákat feszegetnek, mint például a blokkláncok és a mesterséges intelligencia alkalmazhatósága a kiberhadviselésben, a Mi–24 helikopterek elektronikai hadviselési képességeinek fejlesztése vagy az állami célú adatátviteli rendszerek integrálhatóságának kérdései. A környezetbiztonság és a vízgazdálkodás, valamint a vízbiztonság területéhez köthetően is több írással találkozhatunk a kötetben.