12. fejezet

Lehetőségek a magyar kiberműveleti képességek fejlesztésére

Ambrus Éva

Bevezetés

A háború gyakran a technológia fejlődésének hajtóereje volt, és segített új és innovatív módszerek bevezetésében, hogy ezáltal harcászati vagy stratégiai szintű előnyhöz juttasson egy nemzetet az ellenfelével szemben. Repülőeszközöket már az I. világháborúban is használtak, meghódítva ezzel a légteret. Két évtizeddel később, a II. világháború során pedig már teljes értékű haderőnemként volt képes dönteni nemcsak csaták, hanem egész frontszakaszok sorsáról a légierő. Ahogyan a II. világháború alatt a technológia meghódította a légteret, úgy tette lehetővé a 20. század fordulóján a hozzáférést a kibertérhez. Ám míg a légtérben lehetőség van a civil és a katonai felhasználást megkülönböztetni, a kibertér esetében a jelen lévő szereplők és szándékok nehezebben szétválaszthatók.

A kibertér gyűjtőfogalma alatt azon felhasználókat, eszközöket, szoftvereket, folyamatokat, információkat, szolgáltatásokat és rendszereket értjük, amelyek közvetlenül vagy közvetetten számítógép-hálózathoz vannak kapcsolva.[1] Az elmúlt évtizedek fejlődése által előidézett összekapcsoltság szintje emeli ki ezt a területet mind a lehetőségek (például e-kereskedelem elterjedése, okosotthonok), mind a fenyegetettség (például hackertámadások sűrűsége, adatok gyűjtése és felhasználása) szempontjából. Újra elolvasva az előbb idézett definíciót, érdemes tudatosítani az egyéni szinten is, hogy hány szállal kötődik a legtöbb ember a kibertérhez, és hogy – általánosságban – milyen természetesnek vehető, hogy létezik.

Azonban a kibertér korántsem tekinthető békés dimenziónak, hiszen egyik hatása biztonsági szempontból, hogy „fegyvert" képes adni olyan csoportok és entitások számára a nagyobb világhatalmak ellen, amelyekkel kinetikus

[1] Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. 18.

https://doi.org/10.36250/01079_12

https://orcid.org/0000-0002-8354-1296

műveletek során nem lennének képesek versenybe szállni. Kinetikus műveleteknek hívjuk az ellenség elsősorban fizikai energián alapuló fegyverek által történő pusztítását (például lövedék által), míg nem kinetikusnak azokat a műveleteket, amelyek nem ezen alapulnak (például információs vagy kiberműveletek).[2] A kiberműveletek alatt az informatikai rendszerekhez, illetve azon keresztül infrastruktúrához való hozzáférés és működésük, szolgáltatásaik befolyásolása értendő.[3] A képesség a NATO meghatározása szerint olyan

> „kritikus tulajdonság, amely ahhoz szükséges, hogy a NATO védelmi tervezési folyamata által kifejlesztett katonai tevékenység sikeres legyen. […] A képességek leírják, hogy a NATO katonai szervezeteinek mit kell tudniuk teljesíteni, hogy lefedjék a Szövetség katonai küldetéseinek teljes skáláját, és garantálják a NATO katonai hatékonyságát és szabad mozgását."[4]

A kiberképességek e követelmények megjelenését jelentik a kibertér dimenziójában. A kiberműveleti képességek területén – az ország egészét tekintve – több szervezet érintett, hiszen a kibervédelem és -biztonság szerteágazó terület. A könyvfejezet elsődlegesen a Magyar Honvédség kiberképességeire fókuszál, a két érintett szervezet a Katonai Nemzetbiztonsági Szolgálat Kiberbiztonsági Központja és a Magyar Honvédség Parancsnoksága Kibervédelmi Szemlélősége, beleértve a Magyar Honvédség Parancsnoksága Kiber Képzési Központját. Az információhozzáférés okán elsősorban ez utóbbiakra fogom helyezni a hangsúlyt.

A kiberképesség-fejlesztés szintéziseként az amerikai Correia által is ismertetett[5] DOTM(A)LPFI+P angol betűszó használatát javaslom, miután egyfelől kellőképpen részletes és árnyaltan közelíti meg a kérdést, másfelől hasonlóságot mutat a NATO általi megközelítéssel, ami konvergenciát biztosít. Az eredeti, DOTLMPF betűszó az Egyesült Államok által használt, a közös képességek integrációs fejlesztési rendszerét (*Joint Capabilities Integration Development System* – JCIDS) fedi. Ez a folyamat olyan megoldásteret biztosít, amely figyelembe veszi a feladat végrehajtásához szükséges tényezőket.[6] Az Egyesült

[2] Lóderer Balázs – Stohl Róbert (szerk.): *Fegyver nélküli műveletek és háttértényezők. Tanulmánykötet*. Budapest, Honvéd Tudományos Kutatóhely, 2019. 3.

[3] Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. (2018a), 1. 113–131.

[4] NATO ACT: *Framework for Future Alliance Operations 2018 Report.* 2018. 57.

[5] João Correia: Military Capabilities and the Strategic Planning Conundrum. *Security and Defence Quarterly,* 24. (2019), 2. 21–50.

[6] US Army War College: *How the Army Runs – A Senior Leader Reference Book 2019–2020.* 2–14.

Államok által használt eredeti DOTMLPF-hez a NATO az interoperabilitás követelményét illesztette (DOTMLPF-I),[7] illetve később az Egyesült Államok is kiegészítette a szakpolitikai irányelvvel (Policy, DOTMLPF-P).

A korábbi DOTMLPF-hez képest a kibertér beemelésével új elemek jelentek meg (a logisztika, az alkalmazkodóképesség, a modularitás, az információ és az intézményközi együttműködés).

A betűszó feloldása a következő:

- Doktrína *(doctrine):* a katonai stratégia módszereinek megfogalmazása.
- Szervezet *(organization):* a harc megszervezése a dandárok és ezredek szintjein.
- Képzés *(training):* a taktikai és műveleti szinten való kiképzés (az alapkiképzéstől a közös nemzetközi képzésekig).
- Felszerelés – logisztika *(material/equipment/logistics):* minden, ami a haderő felszereléséhez szükséges, de nem igényel új fejlesztési kapacitást (rendszeresített felszerelések). A modularitás is rendkívül kritikus, figyelembe véve a fenyegetések széles skáláját, amelyekkel szemben alkalmazkodó és rugalmas válaszokat kell tudni adni.
- Alkalmazkodóképesség *(adaptability):* az alkalmazkodóképesség és interoperabilitás olyan gondolkodásmód, amely nélkül nem lehetséges több tartományt érintő műveletek végrehajtása.
- Vezetés és oktatás *(leadership and education):* a vezetők szakmai felkészítésének módjai, eszközei (szakmai fejlődés).
- Személyzet *(personnel):* képzett személyek rendelkezésre állása béke- és háborús időben, valamint különféle rendkívüli műveletekhez.
- Létesítmények *(facilites):* ingatlanok és (ipari) létesítmények (például kiképző központok).
- Információ *(information):* Az információ célja a folyamatos átfogó tudatosság fenntartása a stratégiai környezet és a kívánt képességek közt. Enélkül a stratégiai környezeti változások nyomon követésének módja elsősorban a doktrínákon keresztül történne, ami a mai gyorsan változó környezetben szükségtelen kockázatot jelenthet.
- Intézményközi együttműködés és szakpolitikai irányelvek *(interagency and policy):* minisztériumok, háttérintézmények közötti együttműködés vagy olyan nemzetközi irányelv, amely befolyásolja e lista elemeit.[8]

[7] NATO AAP-06. NATO Glossary Of Terms And Conditions. 2019.

[8] Correia (2019): i. m. 25.

Egyszerű, ám fontos megállapítás, amely az új típusú kihívásokból, a gyorsan változó biztonsági környezetből adódik: nem lehetséges megvárni az egyértelmű fenyegetések megjelenését, mielőtt létrehoznák az azok kezeléséhez szükséges struktúrákat, ezt a modern katonai képességek fejlesztésébe fektetett idő kockázatossá teszi.[9] Ezért fontos a stratégia a képességalapú tervezési folyamatban, és a fenti katonai képességdefiníció alapján lehetséges azonosítani Lykke stratégiájának három vektorát – célokat, módokat és eszközöket–, amelyekhez még figyelembe kell venni a kockázatot.[10] Mindazonáltal a célok, módok és eszközök az elmúlt időszakban született új nemzeti stratégiákban megjelentek, így a hazai helyzet elemzéséhez végül más eszközt vettem alapul.

SWOT-elemzés

A kiberműveleti képességek fejlesztési lehetőségeinek feltérképezéséhez egy jelenlegi pillanatképből kiindulva lehetséges eljutni. Ehhez az úgynevezett SWOT-elemzést[11] veszem alapul. A SWOT-elemzés egy stratégiai tervezési technika, amely segít szervezeteknek azonosítani a projekttervezéssel kapcsolatos erősségeket, gyengeségeket, lehetőségeket és veszélyeket.[12] Általánosságban a SWOT-mátrix az erősségeket és a gyengeségeket belső, azaz szervezeten belüli, míg a lehetőségeket és a fenyegetéseket gyakrabban külső, azaz a szervezeten kívüli kategóriaként determinálja.

A hagyományosan államközpontú nemzetközi rendszerben az államok saját maguk biztonságáról, annak alkotóelemeiről, területeiről és az azt fenyegető tényezőkről alkotott képe jelenti a kiindulási pontot; megtestesülése a nemzeti biztonsági stratégia (NBS). A nemzeti katonai stratégia (NKS) mindig része a nemzeti stratégiának, azt támogatja, azaz megfelel a nemzeti politikának. Az NKS a nemzeti biztonsági erőforrások, valamint a fegyveres erők

[9] Joseph R. Cerami – Richard Lacquement Jr.: *Shaping American Military Capabilities After the Cold War.* London, Praeger, 2003. 161.

[10] Arthur F. Lykke: *Toward an Understanding of Military Strategy.* In Joseph R. Cerami – James F. Holcomb (szerk.): *Guide to Strategy. USA*. U.S. Army War College, 2001. 179.

[11] A mozaikszó az angol *strength* (erősség), *weakness* (gyengeség), *opportunity* (lehetőség) és *threat* (veszély) szó kezdőbetűiből tevődik össze. Magyarul GYELV-ként is előfordul.

[12] Magyar Kereskedelmi és Iparkamara: *Exportkalauz*. (É. n.)

fejlesztésével kapcsolatos komplex nézet- és tevékenységrendszer. Az NKS már nem ismétli meg a NBS általános megállapításait.[13]

1. táblázat: A kiberképességek SWOT-mátrixa

Erősségek	**Gyengeségek**
– új biztonsági és katonai stratégia erősödő kiberszemlélete (doktrína) – szervezeti megújulás (szervezet) – képzés és oktatás (képzés, kiberakadémia, Nemzeti Közszolgálati Egyetem kiberbiztonsági mesterképzési szak) – felszerelés (Zrínyi Haderőfejlesztési Program)	– civil és katonai „kibertér” – koordináció – szakemberek vonzása és megtartása (személyzet)
Lehetőségek	**Veszélyek**
– rugalmas reagálás (alkalmazkodóképesség) – intézményközi és nemzetközi együttműködések	– gyorsan változó technológia, lekövetési nehézség – adaptábilitás lassúsága (információ)

Forrás: a szerző szerkesztése

Erősségek

Az új biztonsági és katonai stratégia erősödő kiberszemlélete (doktrína)

Az új, 2020. évi *nemzeti biztonsági stratégia* (NBS)[14] kiemeli, hogy

> „Magyarország és a magyar állampolgárok mindenoldalú […] információs és kibertérbeli biztonsága *alapvető érték*. Kiemeli a honvédelmi és rendvédelmi erők szoros *együttműködés*ének fontosságát egymással és a releváns polgári infrastruktúrával, és hogy az új biztonsági kihívások miatt *folyamatosan szükséges fejleszteni* a […] kiberhadviselés elleni védekezés rendszerét. Az információbiztonság *tudatosság*ának alacsony szintjére is felhívja a figyelmet és megállapítja, hogy a kibertér ma már […] *külön műveleti tér*nek számít”.

Az NBS egyik legfontosabb eleme, hogy „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes *kiberképességeket*

[13] Mező András: *A katonai stratégiaalkotás és doktrínafejlesztés Magyarországon.* Doktori (PhD-) értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2019. 34–35.

[14] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges",[15] mindazonáltal kitér a kiberműveletek (támadások) attribúciós nehézségeire is.

A honvédelemmel kapcsolatosan újfent kiemeli a kiberteret mint műveleti területet, és hogy a „katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható *offenzív képességek*et. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit",[16] pontos irányvonalat kijelölve ezáltal. Nagy lépés, hogy megjelenik az offenzív képességek fontossága.

Továbbá elsődleges feladatként tekint többek között a *kormányzati koordináció* erősítésére, a kibertér *jogi szabályozásának* fejlesztésére, valamint a kiberbiztonsággal kapcsolatos *nemzetközi együttműködés* bővítésére.[17]

Kovács László összefoglalója alapján elmondható, hogy a stratégiában markánsan megjelenik a Magyar Honvédség kibertéri szerepe és feladatai is, meghatározza, hogy a fejlesztéseknek a kibervédelmi *(defenzív)* és kiberműveleti *(offenzív)* erői a kinetikus erők műveleteinek támogatására is alkalmasak legyenek. A főbb irányvonalak megadása után szükséges a végrehajtást elősegítő ágazati stratégiák átalakítása, létrehozása, ami tükrözi ezeket a fejleményeket. Ilyen a 2021. évi *nemzeti katonai stratégia,* illetve az előkészület alatt álló *nemzeti kiberbiztonsági stratégia,* amelyekben megjelenik a katonai kiberműveleti képességek helye és szerepe.[18]

A katonai stratégia „a katonai végcélok, a katonai módszerek és a végrehajtásra biztosított katonai eszközök együttese".[19]

A 2021. évi *nemzeti katonai stratégia*[20] (NKS) meghatározza, hogy a hagyományos (katonai, gazdasági, politikai, társadalmi és környezeti) biztonsági elemek mellett azt a kiber- és az információs dimenziók is alkotják.[21] Ahogyan az NBS-ben, úgy itt is megjelenik az a fajta szemlélet, hogy a hazánk „fizikai biztonságát veszélyeztető vagy jelentős anyagi károk okozására képes

[15] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[16] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[17] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[18] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18.
[19] Lykke (2001): i. m. 3.
[20] 1391/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról.
[21] 1391/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról.

kiberképességeket fegyvernek, alkalmazásukat pedig akár *fegyveres támadásnak tekinti,* amelyre adott esetben katonai válaszadás is lehetséges",[22] amelyhez szükséges többek között a kibertér-eszközrendszerek fejlesztése. A *katonai kibertérműveleti erők* a kibertérben végrehajtott (offenzív vagy defenzív) műveleteikkel támogatják a haderőnemeket, és aktívan közreműködnek a nemzeti kibervédelmi feladatokban.

Az alkalmazkodóképességet erősíti az a megállapítás is, hogy a Magyar Honvédség képességei *moduláris rendszerben* épülnek fel annak érdekében, hogy a műveleti igények szerint lehessen őket alakítani. Ehhez szükséges, hogy minden műveleti szinten *passzív és aktív* kibervédelmi *képességeket* alakítsanak ki.

Az NBS-hez képest az NKS tovább bontja a feladatokat a kiberműveletek tekintetében, amikor részletezi, hogy azoknak offenzív jellegűnek is kell lenniük, támogatniuk kell a szárazföldi és légierő műveleteit passzívan és aktívan, és ehhez moduláris, rugalmas rendszerű képességekre van szükség.

Szervezeti megújulás (szervezet)

A honvédelmi miniszter 32/2021. (VII. 23.) HM utasítása[23] rendelkezett a Magyar Honvédség Kiber- és Információs Műveleti Központ (MH KIMK) kialakításával összefüggő egyes feladatokról. Ennek eredményeként a Magyar Honvédség parancsnokának alárendeltségébe tartozó kiber- és információs műveleti feladatokat ellátó honvédségi szervezetek szervezeti felépítése és feladatrendszere átalakul.

Az MH katonai kibertérműveleti képességeinek fejlesztése érdekében az *MH Civil-katonai Együttműködési és Lélektani Műveleti Központ* 2021. december 31-ei hatállyal megszűnt, és annak jogutódszervezeteként az MH PK közvetlen szolgálati alárendeltségében 2022. január 1-jei hatállyal MH KIMK megnevezéssel új költségvetési szerv jött létre.

Kovács László kibervédelmi főszemlélő korábbi cikkében utalt a szervezet lehetséges átfogóbb feladataira is:

> „Az MH fejlesztése során általánosságban a kibertér műveleti képességek fejlesztése, illetve a kibertéri műveletek tervezéséhez, szervezéséhez és vezetéséhez szükséges szervezeti keretrendszer kialakítása az első cél. Az ezeket a feladatokat a jövőben megvalósító

[22] 1391/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról.
[23] *Hivatalos Értesítő. A Magyar Közlöny Melléklete.* 6. 2021. július 23. 3482–3483.

szervezetnek három nagy csoportra osztható feladategyüttese várható: 1. kibervédelmi és kiberműveleti fejlesztések koordinálása és ezek vezetése; 2. a kiberműveleti tevékenységek vezetése és végrehajtása különböző szinteken (hadműveleti szint, harcászati szint); 3. a kiberműveletek integrálása a szárazföldi csapatok és a légierő műveleteibe."[24]

Képzés és oktatás (képzés, kiberakadémia)

A Magyar Honvédség kiberképzési központját (kiberakadémia) 2019 júniusában adták át. Ez a szervezet végzi az oktatási, képzési és kiképzési feladatokat, beleértve a honvédség felhasználóinak kibertudatossági képzését, illetve a jövőbeli kiberműveleti erők felkészítését.[25]

Az egyik ilyen feladat az oktatás, képzés és kiképzés rendszerének és akár intézményrendszerének a megteremtése. Ez nemcsak a saját állomány felkészítését jelenti, hanem a Magyar Honvédség egészére vonatkozó, elsősorban kibervédelmi képzéseket is. Ezekkel a képzésekkel lehetséges emelni a kiberbiztonsági tudatosság és elkötelezettség szintjén. Nyilvánvalóan ezek a képzések és kiképzések az eltérő szinteken eltérő célokkal is párosulnak, hiszen amíg az említett kiberbiztonsági tudatossági képzéseket minden szinten folytatni kell, addig a kiberműveletek stratégiai kérdéseit a katonai felső vezetés szintjén, de a konkrét technikai végrehajtást műveleti és harcászati szinten szükséges oktatni.

Benkő Tibor honvédelmi miniszter 2020. évi honvédelmi bizottsági ülésén elmondta, hogy a tárgyév decemberéig a kiberakadémián 19 tanfolyamot bonyolítottak le, és 3000 fő vett részt a biztonságtudatosítási tanfolyamon.[26]

Felszerelés (Zrínyi Honvédelmi és Haderőfejlesztési Program)

A 2021. évi honvédelmi költségvetés 778 milliárd forint volt, a 2022. évi 1003 milliárd forint, amely 28,9%-os nominális emelést jelent. A nemzeti összterméhez viszonyítva is jelentős a bővülés, az idei 1,66% után jövőre meghaladja az 1,7%-ot a honvédelmi kiadások GDP-hez viszonyított aránya, így

[24] Kovács (2020): i. m. 16.

[25] Draveczki-Ury Ádám: „Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül". *Honvédelem.hu,* 2020. július 3.

[26] Jegyzőkönyv az Országgyűlés Honvédelmi és rendészeti bizottságának 2020. december 8-án, kedden, 11 óra 04 perckor az Országház Széll Kálmán termében (főemelet 64.) megtartott részben zárt üléséről. 29.

egyre közeledünk a NATO által elvárt 2%-os mértékhez, amelyet a vállalások alapján 2024-re kell elérni.[27] Ennek a költségvetési növekedésnek központi eleme a Zrínyi Honvédelmi és Haderőfejlesztési Program, amely egyszerre jelent hadiipari és haderőfejlesztést. A két elem egymást támogatva hosszabb távon képes biztosítani a honvédség ütőképességét, hogy a befektetések ne egyszeriek legyenek, hanem folyamatosan fenntartsák és igazítsák képességeiket a kor követelményeihez.

Gyengeségek

Civil és katonai „kibertér" és koordináció

Alapvetésnek tűnik, de érdemes újra felidézni azt a tényt, hogy a kibertérben nehezen elkülöníthető a katonai és a civil „szféra". Maga a kibertér és az abból fakadó fenyegetések bonyolultak, összetettek és változékonyak. Ezek mellett a kiberműveletek száma és sebessége is növekszik. A fenyegetések korábban a fizika korlátjához igazodtak, azonban a kibertérben folyamatosak. Ez elkerülhetetlenül kihívások elé állítja a döntés- és reagálási képességet. Nem utolsósorban nemcsak a civil és katonai megkülönböztetés, hanem az attribúció, azaz egy-egy kiberművelet „gazdájának" a meghatározása is időigényes, továbbá más-más következménye lehet annak, hogy egy kiberműveletet támadásnak, kémkedésnek vagy bűncselekménynek tekintenek-e.

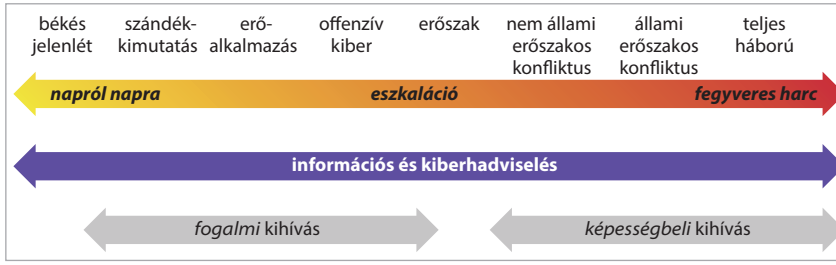
A hazai kibervédelmi szervezeti rendszer mind a civil, mind a katonai térben két részre bontható, egy stratégiaira (koncepciók kidolgozása, koordináció) és egy operatívra (gyakran hatósági funkciót ellátva, gyakorlati végrehajtás). A civil oldalon a stratégiai szinten a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok találhatók,[28] míg az operatív szintet – több esetben hatósági funkciókkal is kiegészülve – a Nemzetbiztonsági Szakszolgálat keretein belül működő

[27] Baranyai Gábor: Jövőre is nő a honvédelemre fordítható összeg. *Magyar Nemzet,* 2021. május 1.

[28] A Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet módosításáról szóló 259/2021. (V. 20.) Korm. rendelet a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról.

Nemzeti Kibervédelmi Intézet jelenti.[29] A katonai oldalon található meg a MH Kibervédelmi Főszemlélősége, alatta a Kiberakadémiával, és a Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ a Katonai Nemzetbiztonsági Szakszolgálat égisze alatt.

A katonai és civil együttműködés fontosságát és összetettségét az *1. ábra* mutatja be.



1. ábra: A verseny-konfliktus spektrum a hatalom katonai dimenziójához

Forrás: US Navy Chief of Naval Operations: *A Design for Maintaining Maritime Superiority. Version 2.0.* 2018. december[30]

Még kevés konkrétum van arról, hogy a fegyveres erők hogyan tudnak hozzájárulni a nemzeti és nemzetközi kiberbiztonság védelméhez (egy fegyveres konfliktuson kívül), és összetett kérdéskör továbbra is, hogy a kormányok hogyan kezelik a kiberbiztonság és a létfontosságú infrastruktúra védelmének összehangolásával kapcsolatos feladatokat. Bár a fegyveres erők és a polgári hatóságok közötti szoros együttműködés szükségességét kifejezetten figyelembe veszik a különböző szakstratégiákban, kevés konkrétum elérhető ennek megvalósítása felől.

Az új szakpolitikai terület a szervezetek közötti küzdelemhez vezethet az erőforrásokat illetően, illetve fontos tisztázni a felelősségmegosztásokat is. Egy válsághelyzetben az ilyen bizonytalanság negatív hatással lehet a reagálás hatékonyságára, ezért is szükséges közös gyakorlatok szervezése minden érdekelt féllel.

[29] Kovács Zoltán: Kibervédelem és biztonság. In Kiss Tibor (szerk.): *Kibervédelem a bűnügyi tudományokban.* Budapest, Dialóg Campus, 2020. 65.; Munk Sándor: Kiberbiztonsági eseménykezelő szervezetek rendeltetése, feladatai. *Hadmérnök,* 13. (2018b), 3. 430.

[30] „Az Egyesült Államok Védelmi Minisztériuma (DoD) vizuális információinak megjelenése nem jelenti a DoD jóváhagyását."

Szakemberek vonzása és megtartása (személyzet)

Az elmúlt években érezhetően nőtt a verseny az informatikai munkaerőpiacon a világban. A kibervédelmet is érinti a megfelelően képzett munkaerő hiánya, azonban egy szervezet számára több lehetőség is kínálkozik, hogy könnyebben elérje vagy megtartsa a munkaerőt. A NATO Kooperatív Kibervédelmi Kiválósági Központjának tanulmánya[31] foglalkozott a kibervédelem területét érintő személyügyi problémákkal. A pénzügyi ösztönzést alapvetően rövid távú megoldásnak tekintették, meglátásuk szerint a munkaerő számára egy bizonyos fizetési szint felett a pénzügyi ellentételezés nem elsődleges motiváció. A nem pénzbeli ösztönzők, mint például az értelmes munka, a továbbképzési és fejlődési lehetőség, az elismerés vagy a munkakörnyezet, tekinthetőek hosszú távú megoldásnak a munkaerő megtartásában. A Rand Corporation tanulmánya azt támasztotta alá, hogy a közszférában egy kihívásokban gazdag feladat ellátása az (informatikában) átlagos fizetés mellett erős kapcsot teremtett a munkavállaló, a szervezet és annak küldetése között.[32]

A területen nem csupán a kiberbiztonsági szakértőkből van hiány, hanem az állami és a magánszektor is verseng a rendelkezésre álló tehetségekért. A szakképzett személyek toborzása és megtartása a fegyveres erőkben közös kihívás a legtöbb NATO-tagállamban, tekintettel a jövedelmezőbb civil területekre. Továbbá, bár a katonaság érdeke lehet, hogy a legjobb tehetségeket toborozza, az is a nemzeti érdeket szolgálja, hogy e személyek az iparban támogassák a nemzetgazdaságot.

A korábban említett Magyar Honvédség Kiber Képzési Központja nagyban hozzájárul a szakemberek át- és kiképzéséhez. További hazai jó gyakorlat a Honvédelmi Minisztérium által indított Mészáros Lázár-ösztöndíj, amely többek között az informatika területén is támogatást nyújt a hallgatók számára, vállalva, hogy a képzés befejezését követően az MH-val létesített szerződéses szolgálati viszonyát legalább az ösztöndíj folyósításával megegyező ideig fenntartja.[33] Továbbá fontos szerep jut a Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Karán létrejött kiberbiztonsági mesterképzésnek.

[31] Erwin Orye – Gunnar Faith-Ell: *Cyber Workforce Recruitment and Retention: An Awareness Assessment.* CCDCOE, Tallinn, 2020. 14.

[32] Orye–Faith-Ell (2020): i. m. 15.

[33] Honvédelmi Minisztérium: *Pályázati felhívás honvédségi ösztöndíjra* (2021. június 1.).

Lehetőségek

Rugalmas reagálás (alkalmazkodóképesség)

A jelenlegi elképzelések szerint a többdimenziós műveletek (*multidomain operations* – MDO) biztosítják a rugalmas reagálást a haderőnek a változó kihívásokkal szemben. Az MDO alapgondolata a képességek mélyebb integrálása a különböző (szárazföldi, légi, tengeri, kiber-, információs) dimenziók között; az idő, a tér és a képességek konvergenciájának elérése érdekében, hogy független manővereket végezhessen, és dimenziók közötti csapásokat hajthasson végre.[34] A többdimenziós műveletek koncepciójának célja az ellenfél integrált védelmi képességeinek leküzdése, a dimenziók elszigetelésének elkerülése, valamint a cselekvési szabadság megőrzése.

Ennek továbbgondolt változata a NATO által is átvett közös össztartományi műveletek (*Joint All Domain Operations* – JADO) koncepció, amely figyelembe veszi a rendszerek összekapcsoltságát a mai haderőben. Ennek az elméletnek a meglátása, hogy a hagyományos haderőnemi struktúrák, amelyek elsődlegesen a saját tartományukra fókuszálnak, a jövőben is eredményesek lehetnek. Valószínűsíthető, hogy előnyösebb helyzetben lesz az a haderő, amelyik képes könnyedén, gyorsan, agilisan és szinkronban manőverezni az összes dimenzión keresztül, ezért tartja fontosnak a NATO az MDO kiterjesztését.[35]

Következő lépés lehetne a NATO-nak saját, különálló doktrína kifejlesztése a több dimenzióra kiterjedő műveletekről, amelyeket a szövetségesek a saját jövőbeli képességeikhez, erőforrásaikhoz és követelményeikhez tudnának igazítani, ezzel úgymond megelőlegezve az interoperabilitást ezen a területen is. A több dimenzióra kiterjedő műveletek sikere attól függ, hogy képesek vagyunk-e az elgondolást a doktrínához, a szervezethez, a képzéshez, a felszereléshez, a vezetéshez és az oktatáshoz, a személyzethez és a létesítményekhez szükséges képességekhez és az anyagkorszerűsítési követelményekhez igazítani. Ennek eléréséhez szükséges többek között a kiberképességek fejlesztése, amely hozzájárul a megfelelő információk biztonságos továbbításához a szervezeten belül, lehetővé téve a gyorsabb döntést és cselekvést, ugyanakkor korlátozva

[34] Franz-Stefan Gady – Alexander Stronnel: *Cyber Capabilities and Multi-domain Operations in Future High-Intensity Warfare in 2030.* CCDCOE, é. n. 155.

[35] 'NATO JADO': *A Comprehensive Approach to Joint All Domain Operations in a Combined Environment.* JAPCC, 2021.

az ellenfelek mozgásszabadságát az „elektronikus harctéren". A hazai fejlesztések ezen a területen is pozitív irányba mutatnak.

Intézményközi és nemzetközi együttműködések

Az intézményközi együttműködés fontos a tudástranszfer megvalósulásához; amennyire lehetséges, együtt kell működnie a polgári és a katonai területeknek, amennyiben hasonló technológiai megoldásokkal tudnak hozzájárulni a probléma megoldásához. Együttműködés lehetséges a kiberbűnözés-megelőzéssel foglalkozó hatóságokkal, amit például az EU kibervédelmi szakpolitikai keretrendszer javasol.[36] A polgári-katonai együttműködés a kiberügyek területén többek között a bevált jó gyakorlatok cseréje, az információcsere és a korai előre jelző mechanizmusok, az eseményekre adott kockázatértékelések és a figyelemfelkeltés, valamint a képzés és a gyakorlatok tekintetében lehet gyümölcsöző.

Regionális szinten fontos az ilyen típusú együttműködések tekintetében a PESCO. A PESCO (*Permanent Structured Cooperation,* állandó strukturált együttműködés) az Európai Unióban megteremti annak a lehetőségét, hogy a tagországok jobban összedolgozzanak a védelem és a biztonság terén. A tagállamok önkéntes alapon vesznek részt az együttműködésben, de a bekapcsolódáshoz vállalásokat kell tenniük az együttműködés előmozdítására.[37] Magyarország alapító tagként vesz részt Németország (koordinátor), Franciaország és Hollandia mellett a PESCO Kiber- és Információs Domain Koordinációs Központjának (*Cyber and Information Domain Coordination Center* – CIDCC) létrehozásában. A CIDCC célja az információcsere és -áramlás javítása, valamint uniós műveletek és missziók tervezése és vezetése a kiberdimenzióban, hozzáadott értéke az egységesített helyzetjelentések készítése a kiber- és információs térről, támogatva az uniós műveletek és missziók katonai tervezési és irányítási folyamatát.[38]

Ahogyan a kiberműveleti főszemlélő fogalmazott:

> „Az a közös tapasztalat, hogy komoly kihívást jelent a valós idejű – minden kibertéri és minden információs téri – veszélyhelyzetre történő, megfelelő hatékonyságú válaszadás.

[36] Council of the European Union: *EU Cyber Defence Policy Framework (2018 update) 14413/18.* 16.

[37] Az EU állandó strukturált együttműködéséről átfogó információk olvashatók: https://pesco.europa.eu/

[38] Bunderministerium der Verteidigung: *Cyber and Information Domain Coordination Centre (CIDCC).* (É. n.).

> […] Így szükségessé vált, hogy a szövetségünk 4000 kilométeres sugarú körében az EU által támogatott műveleteket kiber-helyzetképpel erősítsük meg. A CIDCC képes lesz arra, hogy a tagországok információit összegyűjtse és egységesítse, ezzel biztosítva az EU katonai törzsének a katonai feladatvégrehajtás során szükséges kiber-információkat."[39]

Veszélyek

Gyorsan változó technológia, lekövetési nehézség

Rob Murray, a NATO Innovációs Egysége vezetőjének véleménye, hogy „azok a nemzetek nyernek [a technológiai] versenyben, amelyek a leggyorsabb bürokráciával, nem pedig a legjobb technológiával rendelkeznek".[40] Az, hogy egy szervezet mennyire és milyen gyorsan képes alkalmazkodni, egyre nagyobb előnyt jelent. Azonban a gyorsan fejlődő technológiák mellett nem mindig egyértelmű, hogy milyen irányba érdemes befektetni.

Barno és Bensahel – megvizsgálva az Egyesült Államok erőfeszítéseit az iraki és afganisztáni operatív kihívások leküzdésére – állítja, hogy az alkalmazkodóképesség a háború alapvető tantétele. Meglátásuk szerint, miután a jövő kihívásait nehéz megjósolni, a stratégiai és taktikai sokkok leküzdésére irányuló szervezeti rugalmasság a legfontosabb, és ez az alkalmazkodóképességi követelmény a jövőben még hangsúlyosabb lesz.[41]

Az elmúlt bő másfél év felgyorsította az alkalmazkodás szükségességét több területen is. Ahogyan fizikailag távolságot kellett tartani, úgy kerültek testközelbe a kibervilág lehetőségei és veszélyei. Az online oktatás, a távmunka, a telemedicina előretörése többségünket érintette, a hálózatok védelmének fontosságára, a kritikus infrastruktúrák kibervédelmére így több figyelem jutott.

Az „alkalmazkodási ollónak" három hajtóereje van a szerzők szerint: *1.* számtalan potenciális ellenfél szembenállása (nagyhatalmi versenytársak, globális szereplők vagy rosszindulatú nem állami szereplő) és a globális események által okozott volatilitás (például az éghajlatváltozás, a tömeges migráció és a növekvő

[39] Ördög Kovács Márton: „Közös feladatot látunk el a kibertér védelme érdekében". Interjú prof. dr. Kovács László dandártábornokkal, kibervédelmi szemlélővel. *Honvedelem.hu,* 2020. november 30.

[40] Rob Murray: Building a Resilient Innovation Pipeline for the Alliance. *NATO Review,* 2020. szeptember 1.

[41] David Barno – Nora Bensahel: *Adaptation under Fire: How Militaries Change in Wartime.* Oxford Scholarship Online, 2020. 1–3.

városiasodás). A *2.* hajtóerő a közelmúltban két új műveleti dimenzió megjelenése: a világűr és a kibertér. A kiberműveletek következményeit ezeken a területeken még nem lehet felmérni az empirikus adatok hiánya miatt. A *3.* hajtóerő a technológiai fejlődés növekvő léptéke és üteme. A mesterséges intelligencia, a robotika és az új fegyverrendszerek megjelenése befolyásolja a hadviselés jellegét. Ezek a hajtóerők együttesen megnehezítik a konfliktusok előrejelzését, és alátámasztják a konfliktusokhoz való alkalmazkodóképesség szükségességét.[42]

Hogy hogyan lehet alkalmazkodni az állandóan változó környezetben, arra példát adhatnak a különböző online szolgáltatók, szolgáltatások, hiszen az üzemzavarok és a kiesések a legtöbbjüknél előfordulnak. Ahogyan egyre több szolgáltatás elérhető online – akár például az e-közigazgatás területén, akár a terjedő otthoni munkavégzés okán –, egyre fontosabb, hogy minden szervezet tudjon a megfelelő időben reagálni a váratlan eseményekre. Ehhez szükséges, hogy a szervezet számítson a váratlan helyzetre. Az első jeleknél érdemes a megfelelő biztonsági lépéseket megtenni. Tisztázni kell azt is a szervezeten belül, hogy a különböző szinteken a szereplők hogyan koordinálják tevékenységüket, hogy lépést tudjanak tartani az események tempójával. Fontos, hogy a reagálási készségek az események bekövetkezte előtt rendelkezésre álljanak a szervezet számára, és emellett folyamatos, proaktív tanulás jellemezze a szakembereket.[43] Mindez a kihívások, módszerek, készségek és képességek folyamatos felülvizsgálatát igényli.

Az adaptábilitás lassúsága (információ)

Az egyik visszatérő elem a szakirodalomban az információ központi kérdése a modern konfliktusokban, hadviselésben. A 21. században a rendelkezésre álló rengeteg információ ellenére a fegyveres erőknek nehézségeik voltak az ezen információk adta előnyök kiaknázásával kapcsolatban. Például Peter Mansoor kijelenti, hogy az Egyesült Államok kezdetben nem rendelkezett az iraki környezet megfelelő megértésével és a hatékony információs műveletek

[42] Barno– Bensahel (2020): i. m. 245–47.

[43] David D. Woods: The Strategic Agility Gap: How Organizations Are Slow and Stale to Adapt in Turbulent Worlds. In Benoît Journé et al. (szerk.): *Human and Organisational Factors*. Springer, 2020.

végrehajtásának képességével.[44] Egy másik megfigyelése az, hogy az iraki és az afganisztáni háborúkban a bevetett fegyveres erők elavult megközelítésekkel és elképzelésekkel dolgoztak, amelyek hangsúlyozták a kinetikai szerepvállalást, majd fokozatosan növelték képességeiket a nem kinetikus szerepvállalások területén (mint amilyen például a civil-katonai kapcsolatok).[45] A kialakulóban lévő, EU-s szintű kiberműveleti együttműködés (PESCO CIDCC) a kibertérben lévő információhiányt kívánja többek között pótolni, azonban ehhez tagállami együttműködés szükséges, a duplikációk elkerülése mellett, a szövetségi rendszerek között. A *2. ábra* fentebb szemlélteti azt a fajta széttöredezettséget, amely a kiberteret jellemzi, eszerint pedig fogalmi tisztázás szükséges, hogy a kibertérben mi számít szándékkimutatásnak vagy éppen offenzív kibertámadásnak, és hogy arra milyen válasz adható, adandó, és kinek. Sajnos vagy szerencsére, de ezen a területen még nem rendelkezünk elég tanulsággal, hogy kialakuljanak minták vagy jó gyakorlatok szövetségi szinten. Mindenesetre előremutató elem, hogy a hazai Kiber- és Információs Műveleti Központ (KIMK) magában foglalja majd a MH Civil-katonai Együttműködési és Lélektani Műveleti Központját, és a vitéz Szurmay Sándor Budapest Helyőrség Dandár szervezetéből és feladatrendszeréből az elektronikus eseménykezelői feladatokat végző szervezeti egység is átkerül.

Összegzés

A képességfejlesztés alapja a doktrínákban megjelenő politikai akarat. Ennek további leképeződése a szakstratégiák megjelenése, ahonnan pontosabb kép rajzolódik ki a cél megvalósulását illetően. A kibertér ötödik műveleti területté emelése mellett a fejlesztési akarat igen fontos kifejezése volt az offenzív kiberképességek szükségességének megfogalmazása. Ezen elgondolásoknak ad fizikai keretet a Honvédelmi és Haderőfejlesztési Program, amely nemcsak a (hadi-) technikákat, hanem a személyzetet is érinti. További lehetőségek vannak még az együttműködés fokozásában mind a hazai, mind a nemzetközi területen, ezzel is hozzájárulva a személyzet képzéséhez, motivációjához

[44] Peter R. Mansoor: Lessons of the Iraq War. In Thomas G. Mahnken (szerk.): *Learning the Lessons of Modern War*. Stanford (CA), Stanford University Press, 2020. 55–57.

[45] Carter Malkasian: Afghanistan and the Crisis of Counterinsurgency, 2001–2014. In Mahnken (2020): i. m. 109–115.

és a jó gyakorlatok elsajátításához. Szükséges a megújulás a rugalmas reagálás területén is, és habár e könyvfejezetben nem esett szó róla, a Magyar Honvédségen belül fontos szerep jut e területen a Transzformációs Parancsnokságnak. Nagyobb szervezeti átalakulást hozhat az átállás a többdimenziós műveletekre (MDO), amely elgondolást az Egyesült Államok és részben a NATO is kutatja. Ahogyan a technológiai fejlődés is folyamatos, úgy a szervezeti fejlődésnek is szükséges követnie azt. A nagyobb műveleti területről a kisebb egységekre fókuszálva látszik, hogy a kinetikus és nem kinetikus egységek együttes használatának fontossága tovább erősödik. Az intézményi keretrendszer kialakítása, a hamarosan létrejövő Kiber- és Információs Műveleti Központ egyik origója lehet mindennek, azonban mint a többi EU- és NATO-tagállamnak is, kihívást fog jelenteni a szakemberek toborzása, megtartása. A honvédség megújulása e területen is lehetőséget biztosíthat a munkakörülmények fejlesztése, az intézményközi együttműködések és az egyedi kihívások által. Nem lehet eléggé hangsúlyozni az információmegosztás fontosságát és gyorsaságát, egy-egy kiberművelet tempóját, és ezt tartania kell a döntéshozatalnak is a megfelelő válaszreagálás érdekében. Összességében: az elmúlt években a kiberműveletek területén Magyarországon nagy előrelépések történtek, lépést tartva a többi európai tagállammal, ezalatt közös kihívásokkal és lehetőségekkel szembenézve.

Irodalomjegyzék

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt

1391/2021. (VI. 24.) Korm. határozat Magyaroszág Nemzeti Katonai Stratégiájáról. Online: https://magyarkozlony.hu/dokumentumok/2a94d595e4bc33b3515c09b0f6f04c4ca3df69c6/megtekintes

259/2021. (V. 20.) Korm. rendelete a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról. Online: https://magyarkozlony.hu/dokumentumok/9aa09f19cee0c53e21021218e25abe1d10f560c7/megtekintes

Baranyai Gábor: Jövőre is nő a honvédelemre fordítható összeg. *Magyar Nemzet,* 2021. május 10. Online: https://magyarnemzet.hu/belfold/2021/05/jovore-is-no-a-honvedelemre-fordithato-osszeg

Barno, David – Nora Bensahel: *Adaptation under Fire: How Militaries Change in Wartime*. Oxford Scholarship Online, 2020. Online: https://doi.org/10.1093/oso/9780190672058.001.0001

Bundesministerium der Verteidigung: *Cyber and Information Domain Coordination Centre (CIDCC).* (É. n.). Online: www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service

Cerami, Joseph R. – Richard Lacquement Jr.: *Shaping American Military Capabilities After the Cold War.* London, Praeger, 2003.

Correia, João: Military Capabilities and the Strategic Planning Conundrum. *Security and Defence Quarterly,* 24. (2019), 2. 21–50. https://doi.org/10.35467/sdq/108667

Council of the European Union*: EU Cyber Defence Policy Framework (2018 update) 14413/18*. Online: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

Draveczki-Ury Ádám: „Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül". *Honvedelem.hu,* 2020. július 3. Online: https://honvedelem.hu/hirek/hazai-hirek/egy-korszeru-harckocsi-is-szamitogep-halozat-csak-70-tonna-vas-veszi-korul.html

Gady, Franz-Stefan – Alexander Stronnel*: Cyber Capabilities and Multi-domain Operations in Future High-Intensity Warfare in 2030.* CCDCOE, (é. n.). Online: https://ccdcoe.org/uploads/2020/12/8-Cyber-Capabilities-and-Multi-Domain-Operations-in-Future-High-Intensity-Warfare-in-2030_ebook.pdf

Jegyzőkönyv az Országgyűlés Honvédelmi és rendészeti bizottságának 2020. december 8-án, kedden, 11 óra 04 perckor az Országház Széll Kálmán termében (főemelet 64.) megtartott részben zárt üléséről. Online: www.parlament.hu/documents/static/biz41/bizjkv41/HOB/2012081.pdf

Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018.

Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18. Online: http://dx.doi.org/10.35926/HSZ.2020.5.1

Kovács Zoltán: Kibervédelem és biztonság. In Kiss Tibor (szerk.): *Kibervédelem a bűnügyi tudományokban*. Budapest, Dialóg Campus, 2020. 65–90. Online: http://real.mtak.hu/107378/7/web_PDF_Kibervedelem_bunugyi_tudomanyokban-66-91.pdf

Lóderer Balázs – Stohl Róbert (szerk.): *Fegyver nélküli műveletek és háttértényezők. Tanulmánykötet.* Budapest, Honvéd Tudományos Kutatóhely, 2019.

Lykke, Arthur F. Jr.: *Toward an Understanding of Military Strategy.* In Joseph R. Cerami – James F. Holcomb (szerk.): *US Army War College Guide to Strategy.* (H. n.), Strategic Studies Institute, 2001. 179–185.

Magyar Kereskedelmi és Iparkamara: *Exportkalauz.* (É. n.). Online: https://mkikexport.uzletahalon.hu/?q=exportprojekt/elemzes/fogalomtar

Malkasian, Carter: Afghanistan and the Crisis of Counterinsurgency, 2001–2014. In Thomas Mahnken (szerk.): *Learning the Lessons of Modern War.* Stanford (CA), Stanford University Press, 2020. 102–121.

Mansoor, Peter R.: Lessons of the Iraq War. In Thomas Mahnken (szerk.): *Learning the Lessons of Modern War.* Stanford (CA), Stanford University Press, 2020. 55–57.

Mező András: *A katonai stratégiaalkotás és doktrínafejlesztés Magyarországon.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2019. Online: https://bit.ly/3Akcewh

Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. (2018a), 1. Online: https://doi.org/10.17047/HADTUD.2018.28.1.113

Munk Sándor: Kiberbiztonsági eseménykezelő szervezetek rendeltetése, feladatai. *Hadmérnök,* 13. (2018b), 3. 427–436. Online: http://hadmernok.hu/182_30_munk.pdf

Murray, Rob: Building a Resilient Innovation Pipeline for the Alliance. *NATO Review,* 2020. szeptember 1. Online: www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/index.html

NATO AAP-06. NATO Glossary Of Terms And Conditions. 2019. Online: https://nso.nato.int/natoterm/Web.mvc

NATO ACT: *Framework for future alliance operations 2018 report.* 2018. Online: www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf

NATO JADO: *A Comprehensive Approach to Joint All Domain Operations in a Combined Environment*. JAPCC, 2021. Online: www.japcc.org/portfolio/nato-joint-all-domain-operations/

Orye, Erwin – Gunnar Faith-Ell: *Cyber Workforce Recruitment and Retention: An Awareness Assessment.* CCDCOE, Tallinn, 2020. Online: https://ccdcoe.org/uploads/2021/02/Workforce-Sep_20_v5.pdf

Ördög Kovács Márton: „Közös feladatot látunk el a kibertér védelme érdekében". Interjú prof. dr. Kovács László dandártábornokkal, kibervédelmi szemlélővel. *Honvedelem.hu,* 2020. november 30. Online: https://honvedelem.hu/hirek/kozos-feladatot-latunk-el-a-kiberter-vedelme-erdekeben.html

US Army War College: *How the Army Runs – A Senior Leader Reference Book 2019–2020.* Online: https://ssl.armywarcollege.edu/dclm/pubs/HTAR.pdf

US Navy Chief of Naval Operations: *A Design for Maintaining Maritime Superiority. Version 2.0.* 2018. december. Online: https://media.defense.gov/2020/May/18/2002301999/-1/-1/1/DESIGN_2.0.PDF

Woods, David D.: The Strategic Agility Gap: How Organizations Are Slow and Stale to Adapt in Turbulent Worlds. In Benoît Journé – Hervé Laroche – Corinne Bieder – Claude Gilbert (szerk.): *Human and Organisational Factors*. Springer, 2020. Online: https://doi.org/10.1007/978-3-030-25639-5_11