NEMZETI KÖZSZOLGÁLATI EGYETEM
VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI KUTATÓMŰHELY

VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI MŰHELYTANULMÁNYOK

2021/18.

FARKAS ÁDÁM – SPITZER JENŐ

Az információs korszak és az állami rezíliencia egyes kérdései

Rólunk

A műhelytanulmány (working paper) műfaja lehetőséget biztosít arra, hogy a még vállaltan nem teljesen kész munkák szélesebb körben elérhetővé váljanak. Ezzel egyrészt gyorsabban juthatnak el a kutatási részeredmények a szakértői közönséghez, másrészt a közzététel a végleges tanulmány ismertségét is növelheti, végül a megjelenés egyfajta védettséget is jelent, és bizonyítékot, hogy a később publikálandó szövegben szereplő gondolatokat a working paper közzétételekor a szerző már megfogalmazta.

A Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok célja, hogy a Nemzeti Közszolgálati Egyetem Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely küldetéséhez kapcsolódó területek kutatási eredményeit a formális publikációt megelőzően biztosítsa, segítve a láthatóságot, a friss kutatási eredmények gyors közzétételét, megosztását és a tudományos vitát.

A beküldéssel a szerzők vállalják, hogy a mű megírásakor az akadémiai őszinteség szabályai és a tudományosság általánosan elfogadott mércéje szerint jártak el. A sorozatban való megjelenésnek nem feltétele a szakmai lektorálás.

A műfaji jellegből adódóan a leadott szövegekre vonatkozó terjedelmi korlát és egységes megjelenési forma nincs, a szerzőtől várjuk az absztraktot és a megjelentetni kívánt művet oldalszámozással, egységes hivatkozásokkal.

A szerző a beküldéssel hozzájárul, hogy a művét korlátlan ideig a sorozatban elérhetővé tegyük, továbbá vállalja, hogy a working paper alapján megírt végleges szöveg megjelenési helyéről a szerkesztőséget legkésőbb a megjelenéssel egy időben értesíti.

A kiadvány ötletét az MTA Jogtudományi Intézet Law Working Papers sorozatának sikeréből merítettük.

Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/18.

Szerző(k):
Dr. Farkas Ádám PhD százados, tudományos munkatárs
Dr. Spitzer Jenő hadnagy

Szerkesztő:
Dr. Kádár Pál PhD dandártábornok

Kiadja
Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely

Kiadó képviselője
Dr. Kádár Pál PhD dandártábornok

A kézirat lezárva: 2021. november 30.

ISSN szám
2786-2283

Elérhetőség:
Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely
1441 Budapest, Pf.: 60
Cím: 1083 Bp., Ludovika tér 2.
Központi szám: 36 (1) 432-9000

Farkas Ádám[1] – Spitzer Jenő[2]

AZ INFORMÁCIÓS KORSZAK ÉS AZ ÁLLAMI REZÍLIENCIA EGYES KÉRDÉSEI

Bevezető gondolatok

Az elmúlt évtizedek technológiai fejlődése, kiváltképpen a keletkezett eredményeknek a társadalom legszélesebb rétegei számára elérhetővé válása, így a jóformán határtalan kommunikációs lehetőségek, ebből következően az információáramlás kontinuitása és sebessége, továbbá globalizáltsága kétségkívül olyan mértékben formálja újra az egyén és a társadalom mindennapjait, hogy azzal már az állami funkcionalitás lépéstartása is jelentős kihívásként mutatkozik meg. Ez a folyamat rendkívül komoly feladatot ró a jogalkotó és a végrehajtó számára a dinamikus, hatásos keretek kialakításában, illetve működtetésében. A hadviselés negyedik generációja[3] ehhez a felgyorsult és globalizált szisztémához szervesen kapcsolódik, ami a technológiai szinten tartás és az államköziség dimenzióján túl a nem állami szereplők térnyerésével is számolni kényszerül. A hibrid szcenáriók egyik legmarkánsabb újdonságát pont az infokommunikációs környezet és annak társadalmi, gazdasági, politikai – és ezek révén biztonsági – beágyazottsága adja, ami mind a hadviselés, mind pedig a komplex biztonság lényegesen tágabb értelmezési tartományában megragadható.

A védelmi és biztonsági kihívásokkal szembeni – legnagyobbrészt nemzetbiztonsági, katonai, rendvédelmi, ugyanakkor az államigazgatás minden szegmensét érintő – tartós, eredményes helytállás megköveteli a fogalmi tisztázottságot, az egyes jellemzők gyakorlati jelentőségének felismerését. Ebben a szövetségesi, közösségi és nemzeti szabályozottság csak együttesen tud hatékonyan érvényesülni. Az információs műveletek fogalma persze nem újszerű ebben a közegben, de annak tartalma és összefüggései, nem utolsó sorban hatóképessége úgy fest, hogy korszakos bővülésen, mélyülésen megy keresztül. Azt is mondhatnánk e tekintetben, hogy egy „információs műveleti robbanás" zajlik, ami egyre inkább növeli az információs tér jelentőségét mind a hadviselés, mind pedig az azon kívüli – állami és nem állami szereplők által gyakorolt – befolyásolás és beavatkozás tekintetében. E kérdés jogi-szabályozási arcélű vizsgálata egyik oldalról a jogállamiság, másik oldalról a szabályok között működő nemzetközi közösség értéke, harmadik oldalról pedig az információs térben történő hatékony, rendszerszerű és következetes védekezés és fellépés miatt kiemelkedő fontosságú. Fontos azonban, hogy a kérdést a negyedik generációs hadviseléstől

[1] Dr. Farkas Ádám PhD százados, a Magyar Honvédség hivatásos tisztje, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Honvédelmi Jogi és Igazgatási Tanszékének tudományos munkatársa.
[2] Dr. Spitzer Jenő hadnagy, a Magyar Honvédség hivatásos tisztje.
[3] A téma kapcsán lásd: KÁDÁR Pál: A hibrid kihívások és a működő államszervezet: Gondolatok egy konferencia margójára. Honvédségi Szemle: a Magyar Honvédség központi folyóirata 148: 4; 3-10. o., 2020.; RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Negyedik generációs hadviselés. In: Honvédségi Szemle 2014/1. szám, 4-12. o.; SOMKUTI Bálint: A 4. generációs hadviselés. In: Hadtudományi Szemle 2009/2. szám, 42-51. o.; JOBBÁGY Szabolcs: A negyedik generációs hadviselés infokommunikációs aspektusai – fogalmi kitekintő. In: Hadmérnök 2017/1. szám, 203-213. o.; LIND, William S. – THIELE, Gregory A.: 4th Generation Warfare Handbook. Kouvola, Castalia House, 2015.; LIND, William S.: Understanding Fourth Generation War. In: Military Review 2004/September-October, 12-16. o.

és a hibrid fenyegetésektől elkülönítve, önállóan is a jogi elemzés fókuszába vonjuk, illetve intenzívebb vizsgálódások tárgyává tegyük a meglévő elemzéseken túl.[4]

Magától értetődőnek tűnik, hogy ebben a változó, „robbanásban lévő" közegben az érvényesülés egyik megkerülhetetlen kulcsa vitathatatlanul az információs fölényben és az abból származó előnyökben ragadható meg. A környezet megfelelő, minden más versengő félnél pontosabb és mélyrehatóbb ismerete persze régre nyúló stratégiai követelmény, fontos azonban hangsúlyozni, hogy az információs korszak egyik új hozadéka az, hogy ez a fajta fölény, vagy előny nem pusztán ismereti jellegű, hanem a korábbi korszakokhoz mérten hatványozottan nagyobb hatóképességgel is párosul. Leegyszerűsítve a kérdést: az információs korszakban az információs fölény nem csak másoknál több tudást jelent, hanem képességet arra is, hogy a versengő/ellenérdekelt felek cselekvését, környezetét, stabilitását hatékonyan befolyásoljuk. Ezzel összefüggésben kiemelendő azonban, hogy az információs műveletek aktív és passzív elemei, katonai és polgári aspektusai kizárólag harmonizáltan képesek az információs fölény lehetőségét megteremteni és azt egy hatékony védelem biztosításával lehetőleg meg is tartani.

Ennek elérése az információs társadalom technikai megközelítésére összpontosító, a szélesebb látószöget mellőző, a hagyományos értelmezésekre szorítkozó, nem adaptibilis elgondolásokkal elképzelhetetlen. A szélesebb értelmezési és vele tervezési, szervezési és cselekvési spektrum nélkül nem csak az aktív műveleti eredményesség válik kétségessé, hanem a megfelelő helyzetkép hiánya és a hatékony védelmi mechanizmusok mérsékeltebb eredményessége miatt az ellenérdekelt tevékenységekkel szembeni ellenállóképesség, így az állami rezíliencia súlyos lépéshátránya is prognosztizálható.

Úgy véljük tehát, hogy az információs műveletek vonatkozásában – mind katonai, mind pedig azon kívüli értelemben – nem mellőzhető a megfelelő védelmi képességek erősítése, aktív képességekkel párhuzamos fejlesztése. Figyelemmel azonban arra, hogy az információs műveletek újszerű hatóereje a „mindenki számára elérhető" technológiai fejlődésen, az információs korszak és információs társadalom, illetve az ebben keletkező digitális adatok hatalmi-geopolitikai súlyának[5] létrejöttén alapul, a hagyományosan védelmi feladatokat ellátó

[4] Példaként lásd: Oxford Institute ELAC: The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities (letöltve: 2021.11.24., https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities); KATZ, Eian: Information Operations in International Humanitarian and Criminal Law: Reflections on the Oxford Statement (letöltve: 2021.11.24., http://opiniojuris.org/2021/07/22/information-operations-in-international-humanitarian-and-criminal-law-reflections-on-the-oxford-statement/); QURESHI, Waseem Ahmad: Information Warfare, International Law, and the Changing Battlefield. In: Forsham International Law Journal 2020/4., 901-937. o.; VÉGH Károly: Információs és befolyásolási műveletek a nemzetközi jog „szürke zónájában". In: FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020., 191-212. o.

[5] A téma kapcsán lásd: CATTARUZZA, Amaël: A digitális adatok geopolitikája. Hatalom és konfliktusok a big data korában. Budapest, Pallas Athéné Books, 2020.; O'HARA, Kieron– HALL, Wendy: Four Internets: Data, Geopolitics, and the Governance of Cyberspace. Oxford, Oxford Scholarship Online: July 2021.; ROSENBACH, Eric - MANSTED, Katherine: The Geopolitics of Information. Cambridge, Belfer Center for Science and International Affairs Harvard Kennedy School, 2019.; PAGANINI, Pierluigi: Data, the New Power in Geopolitics (letöltve: 2021.11.24., https://www.ispionline.it/en/pubblicazione/data-new-power-geopolitics-30657); BUCHANAN, Ben: The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics. Cambridge – London, Harvard Univeristy Press, 2020.; FARKAS Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei. In: SLRG Working Paper 2021/1.

szervek ez irányú képességfejlesztései mellett kulcsterületként kell megjelölni a nemzeti ellenállóképességet, vagyis adott nemzet vonatkozásában az állami és társadalmi rezíliencia fokozását.

A jelen írással a szerzők célja egy több aspektusból történő vizsgálat eredményeként rávilágítani az információs társadalom lényegi tulajdonságaira. Ehhez kapcsolódóan lehetőség nyílik az információs műveletek fejlődési perspektíváinak áttekintésére is, a dogmatikus és gyakorlati elemek viszonyát az utóbbi irányába pedig az Észak-atlanti Szerződés Szervezetének, az Európai Uniónak és a hazai szabályozásnak az egymás mellé állítása segítheti elő, kitekintve ennek a rezíliencia terén azonosítható főbb irányaira is.

Az információs társadalom fogalmának egyes megközelítései

Az információs társadalom, mint fogalom számos tudományterület irányából meghatározható, ezek a nézőpontok eltérő értelmezéseket jelentenek, akár a társadalomtudomány, a gazdaságtan, az informatika vagy a hadtudomány területéről megközelítve. A terminussal egyidejűleg részben eltérő tartalommal, de paralel fogalomként használatos a tudományos életben a tudás alapú társadalom, valamint a tudástársadalom. Fontos azonban leszögezni: a tudás és az információ szinonimaként való használata olyan fontos különbségeket ignorál, mint hogy az adatokból következetesen összetevődő információnál a tudás előrehaladottabb, feldogozottabb, ekképpen pedig magasabb minőségű eredmény. Ez a komplexitás pedig egyúttal a társadalom és a gazdaság rendszerében is könnyebben mérhető eredményekre vezethet. Az információs társadalomnak az államműködésben betöltött szerepe tehát ehhez mérten pozícionálandó[6], miközben a digitalizáció és a kibertér fogalmi sajátosságaira[7], egyéni és társadalmi szintű pszichológiai, szociológiai vonatkozásaira[8] is fokozott figyelmet kell fordítani.

[6] Lásd: VARGA Csaba, UHRIN Emese: Új demokrácia- és államelmélet. Budapest, Századvég Kiadó, 2007. 17-57.o.; Z. KARVALICS László: Információ, tudás, társadalom, gazdaság, technológia: egy egységes terminológia felé. Információs Társadalom. Budapest, Infonia Alapítvány, 4., 2005. 7-17. o.; NYÍRI Kristóf: Globális társadalom, helyi kultúra. IIn: GLATZ Ferenc (szerk.): Az információs társadalom. Magyarország az ezredfordulón, Stratégiai kutatások a Magyar Tudományos Akadémián VI., MTA, Budapest. 2000. 43-64. o.

[7] Példaként lásd: KELEMEN Roland – NÉMETH Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése, In: FARKAS Ádám (szerk.): Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében, Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, 147-170. o.; KELEMEN Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése, Honvédségi Szemle, 2020/4 szám, 65-81. o.; KLEIN Tamás – TÓTH András: Technológia jog – Robotjog – Cyberjog, Budapest, Wolters Kluwer, 2018.; BÁNYÁSZ Péter – KRASZNAY Csaba – TÓTH András: A NATO kibervédelmi szakpolitikája, In: SZENES Zoltán (szerk.) A mai NATO: A szövetség helyzete és feladatai, Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 2021, 130-149. o.

[8] Példaként lásd: AIKEN, Mary: Cyber-csapda – Hogyan változtatja meg az online tér az emberi viselkedést, Budapest, Harmat – Új Ember Kiadó, 2020.; DESSEWFFY Tibor: Digitális szociológia. Szociológiai képzelet a digitális korban. Budapest, Typotex Kiadó, 2019.; CASTELLS, Manuel: Az évezred vége – Az információ kora. Budapest, Gondolat Kiadói Kör, 2007.; LUPTON, Deborah: Digital Sociology. London – New York, Routledge, 2015.; IGNATOW, Gabe: Sociological Theory in the Digital Age. London – New York, Routledge, 2020.; KHADER, Majeed– NEO, Loo Seng– CHAI, Whistine Xiau Ting: Introduction to Cyber Forensic Psychology. Singapore, World Scientific Publishing Co. Pte. Ltd.; 2021.; KISS Tibor – PARTI Katalin – PRAZSÁK Gergő: Cyberdeviancia. Budapest, Dialóg Campus Kiadó, 2019.; KELEMEN Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben, JOG ÁLLAM POLITIKA: JOG- ÉS POLITIKATUDOMÁNYI FOLYÓIRAT 3. 71-85. o., (2021)

Az egyik legelfogadottabb definíció az információs társadalmat tágan értelmezi. „Elsősorban az információs és kommunikációs technológia rohamos fejlődésének és konvergenciájának következményeként, az ehhez tartozó gyártó- és szolgáltató-, valamint a médiaipar globalizálódásával a társadalomban egy új életforma, újszerű működés és viselkedés alakul ki. Új értékrendek jönnek létre. Ezt a széles körben új életmódot, magatartást, információs technológiával átszőtt gazdaságot nevezzük információs társadalomnak."[9] A megfogalmazás átfogó hatású, szélesen elterjedt információs társadalmat láttat, ami a fejlődésével a társadalmat – és vele a gazdasági, politikai, állami, biztonsági és más további dimenziókat is – globálisan összekapcsolja és átformálja. Ez a megközelítés tehát már-már paradigmaváltás szerű hatásokat tulajdonít neki, egy mindenre kiterjedő, számos összefüggést rejtő, megkerülhetetlen jelenségként bemutatva azt. Az információs társadalmat, mint elért társadalmi szintet a szakirodalom több esetben tekinti hasonlóan értékrendet és új világrendet teremtő kulturális fejlődésnek, azonban nem példa nélküli ennek a mérsékeltebb szemlélete sem, miszerint a mindent átíró fordulatok helyett inkább evolúciós lépcsőként érdemes a körülményeket értékelni.[10]

A tág, társadalom-evolúciós álláspontthal, ha nem is szembe helyezkedve, de sokkalta szűkebb látásmódot képvisel a technológiai-infrastrukturális szemlélet. Az egyik direkció az információs társadalmat az információ és kommunikáció technológiák (information and communication technologies, azaz ICT) kifejezéssel is helyettesíti, azzal a véleménnyel, hogy az egy kommunikációs és informatikai (információszerző és -kezelő) természetű technológiai fejlettségi státuszként határozható meg. Ez nem jelenti automatikusan a társadalmi-gazdasági jellegű fejlődés megkérdőjelezését, csupán a technológiai-technikai eszközök és azok felhasználásának katalizátor szerepét.[11] Az információs társadalom ilyen módon a társadalmi és a gazdasági fejlődést kiegészíteni tudja, az ebben való effektivitása pedig a technológiai innováción és annak a társadalomra gyakorolt hatásaitól, a társadalom általi elsajátításától függ. A szemléletet ezen a ponton érdemes kritikával illetni, hiszen – ahogyan az a későbbiekben az információs műveletek vonatkozásában kifejtésre kerül – az információs közeg ilyen szintű leegyszerűsítése, függetlenül az infrastrukturális kitettségtől, egyrészt azt materiális dobozba zárja, nem számol azzal, hogy az egyén és a társadalom pszichológiája és kommunikációja is számos egyéb szempont szerint kerülhet hatás alá. Másrészről azt is kijelenthetjük, hogy a technikai eszközök eredményei csakis az egyénnek, illetve a közösségnek az innováció iránti befogadóképességéig terjedhetnek. Amint ez a produktivitás visszaesik, vagy adott esetben megszűnik, az információ nem éri el a célját: a fejlődéshez szükséges tudás nem képződik meg belőle és a társadalmi-gazdasági evolúcióhoz szükséges újabb döntések sem születnek meg általa. Természetesen látni kell az információs technológia fejlődésének lépcsőzetes természetét a felhasználói kör kiszélesedése terén. A rádiózás, majd a televíziózás, az internet, a közösségi média mind-mind megmutatta ezt, igaz egyre gyorsuló

[9] FODOR István: Merre megy a világ gazdasága, merre mehetünk mi? In: GLATZ Ferenc (szerk.): Az információs társadalom. Magyarország az ezredfordulón, Stratégiai kutatások a Magyar Tudományos Akadémián VI., MTA, Budapest. 2000. 97.o.; Lásd: Uo. 95-113. o.

[10] KOLIN Péter: Evolúció és kultúra. Budapest, Információs Társadalom, Infonia Alapítvány, 3. 58-78. o.; MÉSZÁROS Rezső: A kibertér és a globalizáció. 2004, eVilág, 4., 4-9. o.;

[11] Ennek kapcsán lásd: HEEKS, Richard: Do information and communication technologies (ICTs) contribute to development? 2010. Journal of International Development, 22(5), 625–640. o

történelmi ütemmel. Ezen fokozatos terjedés miatt azonban – a kritikai felvetés mellett is – komoly figyelmet érdemel az információs tér.

Az, hogy akár az állam működése tekintetében, akár védelmi és biztonsági szempontból, akár katonai (információs műveleti) cél relációjában a tág, vagy a szűkebb megfogalmazás felé mozduljon el a döntéshozó, esetileg vizsgálandó, illetve a vizsgálat/tervezés/cselekvés horizontjától is függ, vagyis attól, hogy stratégiai-hadászati/hadműveleti/harcászati szintről van-e szó. Összességében megállapítható, hogy a konkrét végrehajtás felé közeledve erősödhet csak fel a technológiai-infrastrukturális szemlélet térnyerése, míg a tág értelmezés a stratégiai szinteken alapvetésként kell, hogy álljon. Fodor definícióját alapul véve azt is elfogadhatjuk, hogy az információs társadalmat egyik nagy elemére (társadalmi vagy technológiai értelemben vett információs) sem egyszerűsíthetjük le, hiszen pontosan ezek konvergenciájából képződött meg összetett egésszé.[12]

Az információs hadviselés és az információs környezet

Napjaink egyik talán legtöbbet és legszélesebb spektrumban használt fordulata az innováció, a folyamatos és a gondolkodók által gyakran paradigmaváltónak ítélt változások. Habár ennek a való életre mért hatásai eltérőek lehetnek, vitathatatlan, hogy a hadviselés a technológiai fejlődésnek köszönhetően mind személyi körében, mind a képességek és a kapcsolódó tendenciák vonatkozásában jelentős átalakuláson megy keresztül.

A hadviselést a szakirodalom konszenzusosan négy generációra bontja, amelyben a legújabbat a korábbiakkal szemben több markáns különbséggel határozhatjuk meg. Végleg elengedi a háború kizárólagos államközi jellegét, a reguláris erők szembenállását és sok esetben a korábbi célok is merőben más irányt vesznek, így az ellenséges erők totális megsemmisítése helyett az akaraterő rövid-középtávú megtörése nagyobb szerepet kaphat. Mindez magával hozza azt is, hogy a konfliktus nem feltétlenül eredményezi a békeállapottól eltérő, a korábbiakban tapasztalt drasztikus – tisztán katonai konfliktusos – eltérést. Megjelent ugyanakkor a globalizáció és a regionális perspektíva kettőssége is, hiszen míg a társadalom és a gazdaság – kiváltképpen az információs világot is érintve – kapcsolataiban elmosódnak az államhatárok, a kontinenseken belül egy-egy térség regionális feszültségei erősödnek fel. Az azokban való részvétel, a választott módszerek és nem tradicionális eszközök pedig ebből a kettősségből adódóan egy szinte bárkire kiterjedő személyi kört és bárki által alkalmazható, hatékony eszközrendszer egy-egy elemét is jelentik. Ebből a folyamatosan bővülő, a műveleti környezetet átalakító halmazból pedig kétségkívül emelkedik ki többek között a kiberhadviselés, de az információs térben folytatható egyéb (pl. dezinformációs, befolyásoló) tevékenységek is. A példák előrevetítik azt a jelenséget is, hogy a hadviselés egyes szegmensei egyre inkább elszakadnak a fizikai világtól, noha a következményeik, már ott lesznek képesek eredményre vezetni, azaz a közvetett hatások jelentősége érdemben értékelődik fel.[13]

[12] Ennek kapcsán lásd: BALOGH Gábor: Egy túlterhelt fogalom. Információs Társadalom, Infonia Alapítvány, 1. 2006. 25. o.

[13] Ennek kapcsán lásd: PORKOLÁB Imre: Az aszimmetrikus hadviselés adaptációja: A tradicionális és irreguláris hadikultúrák összecsapásainak vizsgálata. Budapest, Magyarország : Ludovika Egyetemi Kiadó, 2020; KISS Álmos Péter: A hibrid hadviselés természetrajza Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata 147:4.

Az információs hadviselést e körben meghatározni úgy lehet, hogy annak célja a technikai megközelítésnél (így a kibertér kereteinél is) lényegesen szélesebb környezetben a célpontok és az általuk használt információk általi, a célpontok tudta – vagy beavatkozásra vonatkozó bizonyossága – nélküli manipuláció annak érdekében, hogy azok a saját érdekükkel sokszor alapvetően ellentétes, de az információs hadviselést folytató érdekeinek megfelelő döntéseket hozzanak. Ennek hatására ugyanis a megcélzott közösség működési szisztémája akárcsak átmenetileg is működésképtelenné válhat, a funkcionális minimumértéke alá eshet, illetve legitimációjában, többségi társadalmi támogatottságában kérdőjeleződhet meg. Ez magában foglalhatja a taktikai információk gyűjtését, a szerzett információk hitelességének és érvényességének a biztosítását, a propaganda vagy a dezinformáció terjesztését, az ellenség és a nyilvánosság demoralizálását vagy manipulálását, az ellenség információi minőségének aláásását, valamint az információgyűjtési lehetőségeinek korlátozását, ellehetetlenítését. Még inkább központi objektívaként emelendő ki az ezek megvalósításához elengedhetetlen információs fölény megszerzése és fenntartása. Fontos kiemelni, hogy az információs hadviselés a fentiekből adódóan és jelen korunkban az átalakuló hadviselés sajátságai miatt is nehezen szorítható időbeli és eredményességi keretek közé, hiszen annak eleje és a vége nehezen határozható meg, közvetlen és közvetett hatásai pedig bármikor változhatnak.[14] Ez pedig a „hadviselési" jelleg „mellett" felerősíti a diplomáciai-politikai-titkosszolgálati dimenzió szerepét ebben a térben, amelyek mindegyikéhez stabil és a megfelelően felkészült és felkészített, (biztonság)tudatos társadalmi háttér szükségeltetik.

Vitán felüli továbbá az is, hogy a napjaink haderőnemeihez kapcsolódó hadszíntereket – nagyban a hálózatalapú, hálózatos szisztémának köszönhetően – az információs hadviselés, az információs hadszíntér képes összekapcsolni. Erre a megállapításra csatlakozva határozandó meg az információs környezet, amely az információs hadviselés mozgásterét, céljai megvalósításához rendelkezésre álló közegét jelenti. Egy meglévő rend, működési mechanizmus megzavarása vagy végérvényes ellehetetlenítése zavar keltésével, tartós diszfunkcionalitás megteremtésével, ami a katonai dimenzió esetében is kiterjed a „semleges, nem hadviselő felekre", legyenek akár állami entitásként függetlenek vagy nem állami szereplőként az ellenségeskedésben akár csak érintett (még ha közvetlenül részt nem is vevő) civil elemek.

A meghatározás globális és ágazati szinten is lehetséges, melyek közül a jelen írás elsődlegesen a katonai dimenzióra koncentrál. A NATO összhaderőnemi információs műveletek doktrínája az információs környezetet úgy határozza meg, mint ami magában foglalja

- egyrészt magát az információt,
- az azokat gyűjtő, feldolgozó és továbbító egyéneket, szervezeteket és rendszereket, valamint

2019. 17-37. o; LIND,William S.: The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, Vol. 73, No. 10 1989. 22–26. o.

[14] LIBICKI, Martin: What is Information Warfare? US National Defence University ACIS Paper 3. 1995. 2. o.; ALBERTS, David S., GARSTKA, John J., HAYES, Richard E., SIGNORI, David A.: Understanding Information Age Warfare, Washington, DC, DoD CCRP, 2001. 35-53. o.; ALBERTS, David S.: Information Age Transformation: Getting to a 21st Century Military. Washington DC, DoD CCRP, 2002.

– azt a kognitív, virtuális és fizikai teret, amiben ez létrejön.[15]

Ugyanezt Munk Sándor úgy határozza meg, hogy a „katonai információs környezet alatt a globális információs környezet azon szereplőinek, eszközeinek és erőforrásainak, valamint információinak összességét értjük, amelyek lényeges hatással vannak egy adott katonai művelet végrehajtására."[16] A két megközelítés egységesen úgy tekint az információs környezetre, hogy az a katonai műveletekre kiható információk és a szereplők összessége, az információs hadviselés eseményeinek helyszíne. Az viszont, hogy a katonai művelet a már műveleti hadszíntérként értelmezhető információs hadszíntérben mely síkokon mehet végbe, melyek az egyénekre hatást gyakorló, azokat összekapcsoló közegek, csak a NATO megfogalmazásból vezethető le. Ez alapján elhatárolhatunk fizikai, információs (virtuális) és kognitív dimenziókat. Egyszerű logikai következtetés, hogy ezek kizárólag összhangban képesek működni és egyiknek sincs érdemi hatása a másik nélkül.

A fizikai dimenzió a rendelkezésre álló eszközök és infrastruktúrák összességét, valamint az ezek elleni vagy ezek védelmében végrehajtott műveletek összességét jelenti. Az egyének és a szervezetek az információval kapcsolatos tevékenységeihez használt mindennemű materiális eszközt magában kell foglalnia, így a papíralapú adathordozótól a különböző adatgyűjtő és feldolgozó eszközökön át az összetett vezetési-irányítási rendszerekig. A negyedik generációs hadviselés alapvetései ezesetben is irányadók, így a katonai és alapvetően az állami kereteken túlterjeszkedő, komplex és globális környezetben szükséges a fizikai dimenziót megközelíteni.[17] Az információs dimenzió azokat a hadszíntéri elemeket koncentrálja, amelyek a materiális téren kívül helyezkednek el. A kör ugyanakkor nem korlátozódik magára az adatokból összetevődő információra, az egyének és szervezetek azzal folytatott tevékenységeire (információgyűjtés, tárolás, feldolgozás, továbbítás) is kiterjed. Tekintettel arra, hogy a releváns tevékenységek teljes körét lefedi az információs dimenzió, az információs környezet ellen támadólag irányuló és a védekező hadviselési mozzanatok is beleértendők ebbe.[18]

A kognitív sík az információs környezet leginkább szubjektív eleme, az egyén tudata felől közelíti meg annak tevékenységét, hogy az az információt miképpen észleli, milyen értelmet társít hozzá, milyen minőségben és milyen eredménnyel képes azt feldolgozni, majd végül mindez hogyan fogja döntéseinek meghozatalában befolyásolni, illetve mennyiben képes a befolyásolást észlelve az ellen védekezni. Ez az egyénre vetítettség a legmagasabb politikai és katonai vezetőktől a legkisebb egység katonájáig érvényes tartalommal bírhat és méginkább hatást tud kifejteni a civilek körében, így akár háborús, akár békeműveleti környezetben vizsgálva is a legjelentősebb dimenziónak tekinthetjük, ami már önmagának a békétől való elmozdulásnak vagy az abban megmaradásnak is központi kérdése. Tekintettel e dimenzió szubjektivitásra, az adott terület, régió, indokolt esetben az egyén társadalmi,

[15] NATO Allied Joint Doctrine for Information Operations (AJP-3.10) LEX-7. 2015. Online: https://info.publicintelligence.net/NATO-IO.pdf (Elérés időpontja: 2021. november 2.)

[16] MUNK Sándor: Információs színtér, információs környezet, információs infrastruktúra. Nemzetvédelmi Egyetemi Közlemények, 6. évf. 2. sz. 2002. 140. Onlinehttp://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1083/nek_2002_2_munk.pdf?sequence=1&isAllowed=y (Elérés időpontja: 2021. november. 2.)

[17] Ezzel összefüggésben lásd: FREDERICKS, BRIAN: Information Warfare: The Organizational Dimension. Institute for National Strategic Studies, 1996.

[18] HAIG 152. o.

politikai, kulturális, tradicionális szempontok szerint értékelendő, kiegészítve többek között az érzelmi, tapasztalati és mentális jellemzőkkel. Az információs műveletek számos megközelítés szerint rendszerezhetők[19], a kognitív dimenzió okán tud kicsúcsosodni a lélektani műveletek (Psychological operations, PSYOPS[20]) jelentősége, továbbá annak eredményességéhez szorosan tapad a felderítés és a hírszerzés információszerző tevékenységének teljes spektruma, beleértve azoknak az elemző-értékelő tevékenység eredményeként történő szintetizálását, de akár a befolyásoló tevékenységeket is.

Az információs hadviselés és az információs környezet fogalmát, valamint az átalakuló hadviselést figyelembe véve egyre kevésbé maradhat vita tárgya, hogy a kiterjedt hálózatos környezetben a civil szereplők megjelenése és az infokommunikációs technika széles körű elérhetősége a területet alapelemmé teszi, ezzel egyidejűleg pedig a befolyásolási lehetőségek potenciálja is jelentősen emelkedik. Mind az elméleti, mind a gyakorlati szempontok körében megjelennek ennek hatásai, a hálózatok kiépültsége, az internet elterjedtsége, a közösségi média felületeinek (az ott megjelenő tartalmak korlátozhatóságának és ellenőrizhetőségének deficitjeivel számolva) a civil lakosság körében kialakult primer szerepe, alapvetően pedig a civilekkel való együttműködés fontossága a katonai oldalon is növelte az információs műveletek technológiai megközelítésével szemben a kognitív szempontú orientációt.[21] Ez irányba hat még a hibrid fenyegetésekből következő „küszöb alatti" krízisek jelensége, ahol a katonai elem lakossági beágyazottsága és kooperációja mellett kimagasló szerepe van a közigazgatási, rendészeti és nemzetbiztonsági szereplőkkel való együttműködésnek, illetve az állami és civil rezíliencia erősítésének. E körben érdemes számításba venni azt is, hogy az információs térben zajló aktív és passzív (műveleti) tevékenységek – beleértve ebbe az ellenérdekelt cselekmények körét is – jogi vonatkozásai osztják a hibrid fenyegetésekkel és az új típusú hadviseléssel kapcsolatos többi jogi kérdés sorsát.[22] A „küszöb alattiság" és a nem

[19] John Arcquilla és David Ronfeldt az információs hadviselés négy alapvető kategóriáját különböztetik meg, növekvő intenzitással, az alábbiak szerint: hálózati/hálózatközpontú hadviselés, politikai hadviselés, gazdasági hadviselés és kiber hadviselés. Lásd: ARQUILLA, John; RONFELDT, David: Cyberwar is Coming! Comparative Strategy, 12. évfolyam 2. szám 1993. 141–165. o.
Ezzel szemben a korábbiakban hivatkozott Martin Libicki klasszikusan hét, egymással az idő múlása okán már jelentős átfedésbe kerülő kategóriát definiál, ezek: vezetési és irányítási hadviselés (magában foglalva a lélektani műveleteket és az elektronikai hadviselést), hírszerzésalapú hadviselés, elektronikai hadviselés, pszichológiai hadviselés, hackerhadviselés, gazdasági információs hadviselés és kiberhadviselés.

[20] A téma kapcsán lásd: LAURENCE, Janice H.; MATTHEWS, Michael D.: The Oxford Handbook of Military Psychology. Oxford University Press, 2012.

[21] HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest. 2018. 158-167. o. (a továbbiakban: HAIG)

[22] SARI, Aurel: Blurred Lines: Hybrid Threats and the Politics of International Law. Helsinki, The European Centre of Excellence for Countering Hybrid Threats, 2018.; SARI, Aurel: Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats. Exeter, Exeter Centre for International Law, 2019.; SARI, Aurel: Hybrid Warfare, Law and the Fulda Gap (letöltve: 2021.07.30., https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2927773_code957129.pdf?abstractid=2927773.&mirid=1); VIKMAN László: A művelettervezés jogi feladatai. In Honvédségi Szemle 2021/2. szám, 44-56. o.; FARKAS Ádám – RESPERGER István: Az úgynevezett "hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai. FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020., 132-149. o.; FARKAS Ádám: Komplex biztonság, hibrid konfliktusok, összetett válaszok. In Honvédségi Szemle 2020/4. szám, 11-23. o.; KELEMEN Roland: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban, In: SmartLaw Research Group Working Paper, 2021/2. szám, 1-17. o.

tisztán katonai reagálást igénylő jelleg egyértelműen eltérő jogi rezsim alkalmazását vonja maga után nemzetállami, mind pedig nemzetközi viszonylatban, ami fejlesztés nélkül akár a fellépés legitimációjára is visszahathat.[23]

Az információs fölény

Az információs műveleteknek a fentiekben kifejtett célkitűzései, annak támadásban és védekezésben megnyilvánuló dinamizmusa képes kimunkálni az információs fölényt, amelynek elérése és fenntartása a hadviselő egyértelmű, központi érdeke. Az információs fölény az a képesség, hogy az információ folyamatos áramlását átfogják, a szerzett információkat sikeresen feldolgozzák és felhasználják, miközben megakadályozzák az ellenség arra irányuló törekvéseit, hogy ugyanezt megtehesse, ezzel egy egyértelmű képességbeli különbség fenntartását célozva.[24]

Az információs fölény három elv szerint rendeződik:

- Domináns manőverezés. Az információs fölény lehetővé teszi a gyorsan mozgósítható egységek számára, hogy gyorsan támadják az ellenség súlypontjait a harctér teljes spektrumában. Az összehangolt és tartós támadásokat az információs hálózat által integrált, de egyébként haderőnemekben, lokációban és feladatokban tagolt erők érik el.
- Precíziós hadviselés. A célpontokra vonatkozó, közel valós idejű információk lehetővé teszik a célpontok térbeli és időbeli pontossággal történő támadását és visszatámadását. A megfelelő hely és a megfelelő idő kihasználásának nagyfokú lehetősége.
- Fókuszált logisztika. Az információs fölény lehetővé teszi a különböző szakanyagok hatékony szállítását a harctéren, optimalizálva a logisztikai folyamatot.

[23] Ezt kiválóan tükrözi a „lawfare" és a jogi sérülékenység kérdésköre, amely a jogállamok szabályozásának korszerűtlenségeit, hiányosságait, illetve a nemzetközi jog versengő instrumentumait teszi hatékony eszközzé az állami és nem állami szereplők számára is. A téma kapcsán lásd: DUNLAP, Charles J. JR.: Law and Military Interventions: Preserving Humanitarian Values in 21 st Conflicts. (letöltve: 2021.06.10., https://people.duke.edu/~pfeaver/dunlap.pdf); KITTRIE, Rode F.: Lawfare. Law as a Weapon of War. New York, Oxford University Press, 2016.; BACHMANN, Sascha Dov– MOSQUERA, Andres B. Munoz: Lawfare and hybrid warfare – how Russia is using the law as a weapon. Amicus Curiae, Journal of the Society for Advanced Legal Studies, Summer 2015, 25–28. o.; ANSAH, Tawia: Lawfare: A Rhetorical Analysis. Case Western Reserve Journal of International Law, Vol. 43, 2010, 87–119. o.; KEARNEY, Michael: Lawfare, Legitimacy and Resistance: The Weak and the Law. In: Ardi IMSEIS (ed.): The Palestine Yearbook of International Law. Martinus Nijhoff Publishers, Leiden, 2010, 79–129. o.; HÓDOS László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai. In: Honvédségi Szemle 2020/4. szám, 49-64. o.; HÓDOS László: A nemzetbiztonsági szolgálatok közelmúltbeli tevékenységét befolyásoló mérföldkövek,avagy az új típusú biztonsági kihívások jelentette veszélyek és az azokra adott kormányzati, illetve jogalkotói válaszok 2010 és 2020 között. In Szakmai Szemle 2021/1. szám 134-149. o.

[24] WALTZ, Edward: Information Warfare: Principles and Operations, Artech House, Inc., Norwood, 1998, 108-110.o. (a továbbiakban: WALTZ)

- Teljes spektrumú védelem. Az erők védelme csak akkor valósul meg, ha a felsőbbrendű információ folyamatosan aktuális marad a fenyegetettségekkel szemben, biztosítva az akciók szabadságát.[25]

Az, hogy ennek az információs fölénynek a fenntartása milyen időhorizonton lehetséges, többféleképpen tagolható. Az elért képességbeli különbség és az ahhoz fűződő műveleti előny lehet

- állandó,
- ideiglenes,
- tartós, valamint
- változó.[26]

A fenti alapelvek láthatóan a hadviselés hagyományosabb megközelítését tükrözik, a konfliktusban érintett fegyveres erők/katonák közötti közvetlen információs reláció elvén klasszifikálják a kérdéskört. Ahogy azt viszont a jelen írás több ponton hangsúlyozta: a negyedik generációs hadviselés fő jellemzője a béke és a háború, valamint a katonai és a civil terület közötti határvonalak elmosódása, ami ebben az aspektusban is megjelenik. Ez nem csak azt jelenti, hogy az ellenséggel szembeni információtöbbletet biztosítani kell, hanem azt is, hogy a civil lakosságot meg lehessen nyerni a katonai műveletek támogatására, vagy legalábbis elfogadására, csökkentve az aszimmetrikus hadviselés kialakulásának potenciálját. Ezek alapján az információs fölényt hagyományos és adaptív megközelítés szerint is vizsgálhatjuk.[27]

A hagyományos megközelítésű információs fölény a konvencionális katonai műveletek körére korlátozódik, jellemzően technikai dominanciával, a rendelkezésre álló infokommunikációs, rádióelektronikai képességekre, azok alkalmazhatóságára és az ellenséges képességek tartalmi és adatközlés szerinti felderítésére, az így szerzett adatok és információk megszerzésére, feldolgozására és felhasználhatóságára. A terület a katonai tevékenységkörök egészét lefedi, amit az is jól mutat, hogy a hírszerzés és felderítés egyik ága, a rádióelektronikai felderítés (Signals Intelligence, SIGINT) a rádióforgalmazás teljes spektrumára kiterjed és külön ágakra bontva képes a távközlés tartalmát, technikai jellemzőit, telemetriai adatközlését vizsgálni.[28] Ha az információs fölényt ebben a hagyományos irányban elemezzük, a vele szemben támasztott feltételek is eszerint lesznek körülhatárolhatók. A fölénynek feltétele lesz az eszközpark és a rendszer számszerű többlete és magasabb minőségi szintje, aminek a valós műveleti értékét a precíz döntés-előkészítés és a képességek praktikus

[25] WALTZ 173-174. o.

[26] MUNK Sándor: Az információs fölényről. Hadtudomány, 11. évf. 3. sz. 2001. 43–52. o.

[27] Ennek kapcsán bővebben lásd: RÓZSA Tibor: Az információs műveletek vizsgálata, különös tekintettel a befolyásolási képességek alkalmazásának lehetőségeire a magyar honvédség feladatrendszerében. PhD-értekezés kézirata. Budapest, NKE Hadtudományi Doktori Iskola 2006. Online: http://archiv.hhk.uni-nke.hu/uploads/ media items/rozsa-tibor-ezredes-az-informacios-muveletek-alkalmazasanak-lehetosegei-a-magyar-honvedseg-feladatrendszereben.original.pdf (Elérés időpontja: 2021. november 2.); SZABÓ András: Az információs hadviselés és hadtudomány. Hadtudomány, 8 évfolyam4. szám 1998. Online: http://www.zmne.hu/kulso/mhtt/hadtudomany/1998/ht-1998-4-5.html (Elérés időpontja: 2021. november 2.)

[28] Lásd: BALOGH Péter: A magyar katonai rádiófelderítés története. Rendvédelem-történeti Füzetek XXIII. évf. (2013) 31-34. szám. 15-16. o.

kihasználása okán élvezi a döntéshozó.[29] Ebben a folyamatban egyaránt fontos az akkurátus információigény, a pontos, valós és hiteles adatszerzés, de még inkább a megfelelő elemző-értékelő munka, ami képes a döntési alternatívákra rávilágítani, egyúttal kellőképpen felkészült a dezinformáció felismerésére és kezelésére. Így válik elérhetővé a megfelelően – a végrehajtó állománytól egészen a legfelső döntéshozó szintjéig – kiépült és működtetett, a megfelelő védelmi mechanizmusokat is kialakított infokommunikációs hálózat.[30]

Első olvasatra könnyen feltételezhető, hogy ezek a képességek és munkafolyamatok a defenzív képességekre és a döntés-előkészítés fejlesztésére szorítkoznak, de mindenkor ide értendő az a tény, hogy a védekezés párhuzamos szála lehet az ellenséges erő törekvéseinek felismerésével annak megtévesztésére való törekvés is. Kiemelendő továbbá, hogy felderítés során szerzett információk egyúttal az ellenséges erők vezetés és irányítási, valamint technikai lehetőségeit is feltérképezik, ami, habár – a defenzív szálon említettekkel összhangban – magában hordozza a dezinformáció veszélyeit, utat nyit azok funkcionális hátráltatására, félrevezetésére, a valószínűsíthető információ kényszerhelyzetébe vagy időbeli hátrányba juttatására. Mindezekre tekintettel megállapítható, hogy az információs fölény a hagyományos keretek között aktív és passzív, így defenzív és offenzív síkon is hasznosítható, nélkülözhetetlen helyzeti előny.

Az adaptív megközelítés nem technikai súlyú, sokkalta inkább a kognitív dimenzióra fektet hangsúlyt, ahol felerősödik a manipulálás, a befolyásolás szándéka. Ennek az eredményessége a globalizált világban és annak információterjedésében kevésbé hosszú távú és pontosan a hírszerzés már taglalt jelentősége miatt főleg harcászati szinten képes sikereket elérni. A hatásfok elsősorban az információs infrastruktúrával kevésbé ellátott ellenséges erők irányában lehet jelentős, ahol a hagyományos információs fölény megléte már meghaladott állapot, továbbá a civilek körében, ahol maga a technikai megközelítés katonai értelemben alig releváns. A civilek tekintetében a legegyszerűbb technikai megoldások is elegendőek lehetnek, hiszen velük szemben nem a vezetési-irányítási rendszerük ellehetetlenítése a cél, hanem a katonai művelet érdekeihez igazodó vélemény kialakítása, az azt segítő befolyás elérése, amihez a legközvetlenebb, legegyszerűbb, a széles rétegek számára leginkább önazonos érzetet biztosító instrumentumokat választja meg a gyakorlat. Ezek az eszközök elsődlegesen a közösségi média egyes felületei, de az életkori összetétel okán nem hanyagolhatók el a konvencionális médiumok sem.[31] Kiemelendők egyúttal olyan fejlődő területek, amelyek növekvő és megkerülhetetlen tényezővé válnak, úgy mint a deepfake (manipulált hamis audiovizuális tartalmak) és a fake news (álhírek), amelyek már jelenleg is alkalmasak a széles tömegek megtévesztésére, utat törhetnek a hagyományos média műsorszórásában is, továbbá a valóságtól való megkülönböztetésük a jövőben egyre komolyabb, már-már szakmai szintű kihívásokat fog eredményezni. Egy állami vagy katonai vezetőhöz társított hamis tartalom órákon belül rendezheti át a megtévesztett civilek széles

[29] HAIG 162-164. o.

[30] Lásd: KELTON, Kari: Learning from the Enemy: Approaches to Identifying and Modelling the Hidden Enemy Organization In KOTT, Alexander (szerk.): Information Warfare and Organizational Decisionmaking, Norwood, MA: Artech House, 2007, 29-63. o.; MAVOR A. S.; PEW R. W.: Modeling Human and Organizational Behavior: Application to Military Simulations, Washington, D.C.: National Academy Press, 1998

[31] Ezzel kapcsolatban lád: KAPLAN, A.- HAENLEIN, M.: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010; BÁNYÁSZ Péter: a közösségi média, mint az információs hadszíntér speciális tartománya. Hadmérnök XII. Évfolyam „KÖFOP" szám – 2017. október. 108-121. o.

rétegének magatartását egy konfliktusban és békeidőben is, egyúttal a technikában rejlő lehetőségek még a szigorú parancsuralmi rendszereket is képesek kikezdeni: a hamis tartalom miatt erőket tud az érdekei szerint mozgósítani, vagy éppen a „hamis parancs" félelme miatt csapatokat béníthat meg. Ennél kisebb hatása sem becsülhető le, hiszen a tartós, kis intenzitású dezinformálás tartós bizonytalanságot eredményezhet, vagy akár egyes vezetők arculatvesztését is, így demoralizáltságot és belső feszültséget. A haditechnika, vagy akár csak a hagyományos információs fölény műszaki dominanciája pedig a mögötte tevékenykedő humán tényező stabilitása nélkül, az autonóm vagy alapvetően mesterséges intelligenciára épülő szisztémák ellenére sem tarthatók fenn. Szintén az adaptív oldal rugalmasságát és sokoldalú kihasználhatóságát erősíti, hogy az ilyen információs fölény megszerzéséhez az előzetes felderítés is jóval egyszerűbb, alapvetően a nyílt forrású hírszerzési módszerek (Open Source Intelligence, OSINT) megfelelő adatokat és információkat szolgáltathatnak. Az államok működésének elektronizáltsága (pénzügy, közigazgatás, műsorszórás stb.) viszont a megfelelő technikai felkészültséggel eredményesen segítheti az információs művelet célját.[32]

Összességében megállapítható, hogy ahogyan az információs környezet egyre jelentősebb szeletét teszi ki a kognitív dimenzió, úgy ennek a tendenciának az okai – kiváltképpen a hibrid hadviselés, a béke és a háború határvonalainak elmosódása és a civil lakosság érintettségének fokozódása, de a hálózatosság és az információáramlás felgyorsultsága is az információs műveletek legfontosabb célját, az információs fölény elérését is más megvilágításba helyzete. A hagyományos, technokrata és konvencionálisan katonai szempontok a hagyományos hadviselésben továbbra sem hanyagolhatók el, de az adaptív megközelítés, a befolyásolás közvetett és közvetlen hatásaiban rejlő eshetőségek új és irreverzibilis folyamatokat betonoztak be a hadviselés egészében.

Az információs műveletek NATO felfogása, az információs védelem megközelítése az Európai Unióban

Az információs környezet meghatározásánál már alapul vett NATO összhaderőnemi információs műveletek doktrínája (NATO Allied Joint Doctrine for Information Operations, AJP-3.10) legutóbb 2015-ben került megújításra. A doktrína megerősíti a nem hagyományos hadviselés térnyerését, ezáltal a műveletek jellegének, az eszközök és az érintettek körének a szükségszerű változását is, aminek a dinamikájában kulcsszerepet játszik az információs forradalom, így az információhoz való hozzáférés, információ megosztás és a döntéshozatallal szemben támasztott követelmények formálódása.

Az információs környezet elemeinek felosztásakor az AJP-3.10. következetesen a virtuális jelzőt használja az információs tartomány megjelölésekor, ami egyrészt szintén erősíti az információs forradalom lenyomatát és a digitalizációt, másrészt a 2014-es walesi csúcshoz igazodva a kiberteret is elhelyezi a hadviselésben.[33] A kognitív rész tekintetében a doktrína kiemeli az egyén és az egyének által képzett csoportok jelentőségét, így az individuum döntési

[32] NAGY Viktor, ERDÉSZ Viktor: Az információs védelem és az információs műveletek szerepe a nemzetvédelemben. Felderítő Szemle X. évfolyam 3-4. szám . szeptember-december 51. o.

[33] A NATO a a 2014. évi walesi csúcson kiberteret hadszíntérré nyilvánította, amire kiterjed a nemzetközi jog, így a kollektív védelem keretei is. A 2014-es walesi NATO csúcstalálkozón az Észak-atlanti Tanács ülésén résztvevő NATO-tagállamok állam- és kormányfőinek közös nyilatkozata, 72-73. bekezdések. Online: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Elérés dátuma: 2021. november 4.)

és helyzetfelismerési képességeinek fontosságát. A fizikai teret érintően hangsúlyozza a hálózatos információs technológia, a mobil infokommunikációs eszközök, az internet és a közösségi média hatásának és szerepének kardinalitását.

Az információs műveletek megfogalmazása tekintetében az információs tevékenység elemzését, tervezését és értékelését a NATO elgondolás egy törzsfunkcióban integrálja, így az információs művelet fő funkcióit nem az általános katonai funkciók körében határozza meg, hanem egy stratégiai, koordinatív szerepként, amiben a technikai tényezők csak egy egység a sok közül, továbbá a törzs szintje az, ahol átfogóbb hatások érhetők el.[34]

Az Európai Unió Belbiztonsági Stratégiája[35] szintén a fókuszpontjába helyezi az információs környezetből jelentkező kihívások kezelését. A NATO elgondolással megegyezően elismeri a digitális forradalom hatásait, a közösség jellegéből adódóan azt sokkalta globálisabban megközelítve jut el az információs biztonságig, a digitális infrastruktúrák védelméig, valamint a kognitív, társadalomra levetített szintekig, kitérve a politikai kampányok sérülékenységére, a COVID-19 világjárvány dezinformációs tapasztalataira, továbbá a kiberbűnözés, a kémkedés és az adatbiztonság kölcsönhatásának kifejtésére. Kiemelt prioritásként kezeli a biztonsági környezet időtállóságát, aminek elemeiként sorolja fel a kritikus infrastruktúrák védelmét és a kibervédelmet is. Egyes célok elérését kulcsfontosságúnak tartja, úgy mint:

- a kritikus infrastruktúra védelmére és rezílienciájára vonatkozó közösségi szintű jogszabályok megalkotása,
- a hálózati és információs rendszerek biztonságáról szóló irányelv felülvizsgálata,
- a pénzügyi szektor rezílienciájának fokozása,
- a kritikus energetikai infrastruktúra védelme és kiberbiztonsága,
- az uniós intézmények, szervek és ügynökségek által alkalmazandó, az információbiztonságra és a kiberbiztonságra vonatkozó közös szabályok az EU Kiberbiztonsági Stratégiája[36] és Kiberbiztonsági Jogszabálya[37] mentén

Az EU azonban a NATO-tól eltérően a nem katonai szférára fókuszál és a rezílienciát helyezi a gondolkodás középpontjába, szükségképpen erősítve az állami-társadalmi, illetve az államon belül az összkormányzati megközelítést és kooperációt. Ez nem jelenti azt, hogy a NATO hanyagolná a rezílienciát vagy hogy éles ellentét feszülne e téren a NATO és az EU között, csupán a két szervezet eltérő természetét és fókuszát tükrözi. A szövetségi – e körben a NATO-t és az EU-t is jelentő – szint azonban egyértelműen a rezíliencia felé mozdul el a

[34] AJP-3.10 2015, 1–5.

[35] Az Európai Unió Belbiztonsági Stratégiának legújabb kiadását 2020 júliusában fogadták el, 2020-2025 időszakára. Lásd: Communication from the Commission on the EU Security Union Strategy, COM (2020) 605 Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 (Elérés dátuma: 2021. november 6.)

[36] Joint Communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade. Online: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (Elérés dátuma: 2021. november 6.)

[37] Az Európai Parlament És A Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály)

hatékony védelem érdekében, ami persze a szükség esetén előkerülő, „hagyományosabb", elrettentő-versengő attitűdöt is támogatni tudja.

A rezíliencia erősítésének jelentősége az információs korszakban

Az információs társadalom, információs hadviselés/műveletek, információs fölény vonatkozásában eddig leírtak a minket körbevevő valóság tapasztalataival összhangban irányítják rá a figyelmet az infokommunikáció fejlődésének rendkívül komplex társadalmi, pszichés, technológiai, politikai, gazdasági és ezek révén biztonsági vonatkozásaira is. Történelmi értelemben az sem meglepő fordulat, hogy a fejlődés vívmányait az állami és nem állami szereplők is törekednek a saját érdekeik másokkal szembeni érvényre juttatására alkalmazni. Ez a globális kapitalizmus versengéseitől, a hatalmi rivalizáláson át a bűnözésig terjedő skálán számos újszerű, vagy a technikai lehetőségek miatt megváltozó jelenséget tár elénk.

A változó környezetben az államnak, mint az egyének és az azokból felépülő társadalmak rendezett, fejlődést segítő együttélését biztosító szervezeti szisztémának, alkalmazkodnia kell a változásokhoz. A technológia robbanásszerű fejlődéséhez fel kell zárkózni, annak vívmányait ki kell használni, mind a nemzeti érdekek előmozdítására, mind pedig a társadalmi rend viszonylatában illegitim[38] – akár állami, akár nem állami – cselekvések semlegesítésére, kártételeinek mérséklésére. Ez az állami képességek, struktúrák és jogállamok esetén messze nem utolsó sorban a jogi szabályok fejlesztését vonja maga után mind a passzív (védekező), mind pedig az aktív (érdekérvényesítő/megelőző) lehetőségek terén.

Az információs technológiák széles körű, mondhatni globális társadalmi elérhetősége és hatásai, a gazdaság működését szisztematikusan érintő volta, ezek mellett pedig a politikai környezetet és a biztonsági szisztémát is érintő kiterjedtsége azonban rendkívül újszerű helyzetet hoz magával. A hatékony védekezéshez és érdekérvényesítéshez ugyanis egy ilyen kiterjedt és nagy szabadságfokú, hálózatosan működő szisztémában alapvető fontosságú az egyének és a társadalom biztonságtudatossága, biztonsági öngondoskodása és állami fellépéssel való egyetértése, ez utóbbi felé ható támogatása. Az információs térben való hatékony helytállás tehát a biztonság szempontjából csak akkor szavatolható, ha az állami-társadalmi szisztémát egységként kezelve, az egyének biztonságfokozó lehetőségeit és tudatosságát segítve és támogatva a nemzeti ellenállóképességet, a rezílienciát[39] erősítjük

[38] Tehát a többségi társadalmi érdekek, különösen a békés, rendezett, biztonságos együttélés ellen ható és ezért társadalomra veszélyes tevékenységek értendők ide.

[39] A téma kapcsán lásd: TOWNSEND, Jim– AGACHI, Anca: Build Resilience for an Era of Schocks. In: Christopher SKABULA (eds.): NATO 20/2020. Twenty Bold Ideas to Reimagine the Alliance after the 2020 US Election. Washington, The Atlantic Council, 2020.; NATO CDS: Enhancing the Resilience of Allied Societies through Civil Preparedness (letöltve: 202.07.30., https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/011%20CDS%2021%20E-%20RESILIENCE%20THROUGH%20CIVIL%20PREPAREDNESS_0.pdf); HAMILTON, Daniel S. (eds.): Forward Resilience. Protecting Society in an Interconnected World. Washington, Center for Transatlantic Relations – Johns Hopkins University, 2016.; KESZELY László: A védelmi igazgatás szerepe a nemzeti szintű átfogó megközelítés megvalósításában. Budapest, Nemzeti Közszolgálati Egyetem, doktori értekezés, 2017.; MOLNÁR Ferenc: A reziliencia kérdése és a NATO. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/15. (letöltve: 2021.11.28., https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20M%C5%B1helytanulm%C3%A1nyok%202021_15_%20Moln%C3%A1r%20Ferenc_A%20reziliencia%20k%C3%A9rd%C3%A9se%20%C3%A9s%20a%20NATO.pdf); VIKMAN László:

meg. Fontos azonban kiemelni, hogy kiszámítható biztonság nélkül sérül az egyéni, a társadalmi, a politikai és a gazdasági bizalom is; csökken az alkotói, innovációs és termelői produktivitás és végső soron a szabadságfok is, ami egyértelműen össztársadalmi veszteségként értelmezendő.

Nem véletlen, hogy számos produktív és modell értékűnek tartott államban (például Svájcban vagy akár Szingapúrban) a társadalmi és gazdasági produktivitáshoz egyértelműen kapcsolódik a hatékony védelmi-biztonsági rendszer és a biztonságtudatossági állami és társadalmi együttműködésen alapuló erősítése. Hasonló példaként hívható fel az elmúlt évek tapasztalata a skandináv és balti államok társadalmi kooperációra építő biztonságerősítő törekvései tekintetében.[40] Ezt az irányt tükrözi a NATO és az EU elmúlt években tapasztalható fejlesztési irányultsága is, hiszen az államok és azok szövetségei – legalábbis idővel – felismerik saját korlátjaikat is, de nem felejtik el – ahogy társadalmaik sem – alapvető, biztonságszavatoló kötelezettségeiket.

Az információs technológia, de emellett a jóléti/fogyasztói társadalom fejlődését megalapozó közszolgáltatások – kritikus vagy létfontosságú infrastruktúrák – átfogó fejlődése és alapvető szükségletté válása egyértelműen egy olyan kiterjedt, komplex, hálózatos és ez által több pólusú és sokszoros kitettségű rendszert hozott létre, amelyben a biztonságot nem tudja csak az állam garantálni, legalábbis megfelelő társadalmi támogatás, attitűd és biztonságtudatosság nélkül nem. Azt gondolni, hogy tisztán állami eszközökkel, a társadalom „felett" cselekedve fenntartható ebben a környezetben a biztonság, önámítás vagy illúzió. Hasonlóan utópisztikusnak tűnik azonban az egyéni és társadalmi szintű önszerveződés és önképzés állami fellépést kiváltó gondolata arra hivatkozva, hogy a mindenki számára elérhető

A közműszolgáltatások és a reziliencia egyes kérdései,
különös tekintettel a kiberbiztonságra. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/14. (letöltve: 2021.11.28.; https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK_M%C5%B1helytanulm%C3%A1nyok_2021_14_Vikman%20L%C3%A1szl%C3%B3_A%20k%C3%B6zm%C5%B1szolg%C3%A1ltat%C3%A1sok%20%C3%A9s%20a%20reziliencia%20egyes%20k%C3%A9rd%C3%A9sei,%20k%C3%BCl%C3%B6n%C3%B6s%20tekintettel%20a%20kiberbiztons%C3%A1gra.pdf); KESZELY László: A nemzeti ellenállóképesség fejlesztésének trendjei. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/6. (letöltve: 2021.11.28.; https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20M%C5%B1helytanulm%C3%A1nyok%202021_6_Keszely%20L%C3%A1szl%C3%B3_A%20nemzeti%20ellen%C3%A1ll%C3%B3k%C3%A9pess%C3%A9g%20fejleszt%C3%A9s%C3%A9nek%20trendjei.pdf)

[40] Ezek kapcsán példaként lásd: BÉRZINA, Ieva: Total defence as a comprehensive approach to national security. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 71-89. o.; WITHER, James Kennet: Back to the future? Nordic total defence concepts. In: Defence Studies Vol. 20. 2020, 61-81. o.; JOHANSSON, Per: Total defence demands new types of collaborations (letöltve: 2021.07.30., https://soff.se/en/our-focus/total-defense/); S&D MAGAZINE: Resilience: Planning for Sweden's "Total Defence" (letöltve: 2021.07.30., https://sd-magazine.com/avis-experts/resilience-planning-for-swedens-total-defence).; SALONIUS-PASTERNAK, Charly: Finland's ambiguous deterrence: mixing deterrence by denial with ambiguous extended deterrence. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 110-127. o.; PRAKS, Henrik: Estonia's approach to deterrence: cimbining central and extended deterrence. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 146-162. o.; VANAGA, Nora: Latvia's defence strategy: challenges in providing a credible deterrence posture. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 163-179. o.; JANELIŪNAS, Tomas: The deterrence strategy of Lithuania: in search of the rigth combination. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 180-198. o.;

digitális tér egyben páratlan tudás- és szerveződési bázis is. Utóbbiak alapjait nem megkérdőjelezve ugyanis fel kell hívni arra a figyelmet, hogy

- az érintett emberek és csoportok képességbeli és világnézeti heterogenitása nem alakul át gyökeresen ezektől;
- a digitális térben elérhető információk a végtelennek ható sokaságuk ellenére sem tesznek minden tudást korlátok nélkül elérhetővé a tudásbirtokosok anyagi és adott esetben hatalmi érdekei miatt; valamint
- a digitális térben cselekvő emberek fizikai és egzisztenciális kötöttségei sok tekintetben fennmaradnak, így az infokommunikációval járó „gyorsulás" sem végtelen.

Erre figyelemmel úgy véljük, hogy a kihívás megoldása a két véglet között van. Ott, ahol elfogadjuk és elismerjük, hogy kulcsfontosságúvá vált az egyéni és társadalmi szintű önképzés, önszerveződés és biztonságtudatosság, de ezek hatékonyságának növelése érdekében elfogadjuk és támogatjuk az állami képességek korszerűsítését és a társadalmi-állami együttműködést. Ez lehet ugyanis a rezíliencia igazi bázisa, ahol az oktatás-neveléstől, a közigazgatás működésén át a védelmi és biztonsági tevékenységekig egy olyan törekvés alakul ki, ami az ellenállóképesség terén túllép a merev állami-társadalmi elhatároláson és kooperációra épül.

A rezílienciában ugyanis hatalmas lehetőség rejlik, mivel az nem csak a magunk megvédésének záloga egyéni, társadalmi és állami dimenzióban is a korszerű felkészültség és a szisztematikus reagálóképesség kialakításával. Az ellenállóképesség hatékony erősítése magával hozza az ehhez szükséges felhasználói, termelői, innovációs, elméleti-tudományos és gyakorlati képességek fejlődését is, ami egyben a biztonságon túl a társadalmi és állami produktivitást is növelheti.[41]

Ehhez azonban el kell fogadni, hogy az ellenállóképesség gondolatiságát, területeit és erősítését fokozatos építkezéssel be kell emelni az állami és szabályozási térbe, valamint az itt rejlő erőforrások és támogatási potenciál révén fokozni kell a társadalmi dimenzióban is. Ehhez egyszerre szükséges:

- a hiteles elemzések és értékelések a kapcsolódó környezeti változások és kihívások kapcsán;
- az állami szervek és szabályozás hiteles és megalapozott, majd hatékonyan működő korszerűsítése;
- a biztonságot érintő tájékoztatás és kommunikáció hazai és nemzetközi politikai versengéstől a lehető legteljesebb mértékben történő elhatárolása és hitelesítése;
- az egyéni ás társadalmi szintű önképzést és biztonságtudatosítást segítő – önszerveződésen alapuló – törekvések irányítás nélküli támogatása;
- a rezílienciát erősítő innovációk fokozott támogatása; valamint

[41] Ennek vonatkozásában lásd: KÁDÁR Pál: A nemzeti ellenállóképesség és a kormányzás folytonossága – Rendvédelmi összefüggések. Pécsi Határőr Tudományos Közlemények 2021: 23. 19-28. o.

- az állami felügyelettel és szervezéssel, de folyamatos társadalmi egyeztetés mellett megvalósuló nevelési és oktatási programok fokozása.

Egy ilyen megközelítésben jól látható, hogy az ellenállóképesség fokozása legalább két aspektusból is megközelíthető. Az egyik a NATO immár hagyományosnak mondható terület szerinti tagolása, a másik azonban az érintett szakterületi/cselekvési dimenziók szerinti felosztás. Az előbbi felosztás szerinti fő területek a következők:

- az államműködés/kormányzás és a kritikus kormányzati szolgáltatások folytonosságának biztosítása;
- az energetikai rendszer ellenállóképessége;
- az ellenőrizetlen tömeges személyi mozgások kontrollálásának képessége;
- az ellenállóképes élelmiszer- és vízellátás szavatolása;
- a tömeges sérülésekkel járó helyzetek kezelésének képessége;
- az ellenálló kommunikációs rendszer biztosítottsága;
- az ellenálló polgári közlekedési rendszer szavatolása.[42]

E területek hatékony kialakítása, működtetése, fenntartása tekintetében azonban kulcsfontosságú a másik megközelítés is, hiszen az fel tudja oldani azt a prima facie kézenfekvő, mégis meglátásunk szerint hibás nézőpontot, hogy mindezek az állam – elsősorban védelmi és ezzel összefüggő államigazgatási – képességeivel önállóan szavatolhatók.

Az ellenállóképesség területei ugyanis mind olyanok, amelyekben a társadalmi szereplők mint szakemberek és mint felhasználók/szereplők is jelen vannak. A hatékony ellátásuk tehát nem korlátozható „csak" az állami szolgálatban, illetve az adott szolgáltatás biztosító szektorokban feladatot ellátó személyi körre és annak tudatosságára. Ezek körében ugyanis a társadalom egésze ilyen-olyan módon, az ellátási láncok, a közszolgáltatások és a rendezett élethez szükséges napi tevékenységek révén közvetve és közvetlenül is érintett.

Ebből adódóan az ellenállóképesség fenti területein történő hatékony fejlesztésekhez kulcskérdés a támogató társadalmi közeg erősítése, ami egyszerre érinti az oktatás-nevelést, a szakmai kultúrák/kamarák/képzőhelyek kérdését, a kutatás-fejlesztést és civil szerveződések szféráját, mint közvetítő közegeket. Ezeken felül e területek működési kereteinek szakmai és állami-szabályozási kereteinek megadása és korszerűsítése is az államon túlmutató perspektívát jelent, akárcsak az egyes területeken megjelenő – visszaéléseken alapuló – anomáliák társadalmi megítélésének az össztársadalmi rendet és hatékonyságot szolgáló előmozdítása. Ebben a körben tehát a rezíliencia fokozása nem csupán összkormányzati – vagyis a kormányzaton belüli szakmai-ágazati tagoltságon átívelő –, hanem össztársadalmi

[42] Vö.: ROEPKE, Wolf-Diether– THANKEY, Hasit: Resilience: the first line of defence (letöltve: 2021.07.30., https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html); NATO: Strengthened Resilience Commitment. 14. Juny 2021. (letöltve: 2021.07.30., https://www.nato.int/cps/en/natohq/official_texts_185340.htm); NATO: Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016. (letöltve: 2021.07.30., https://www.nato.int/cps/en/natohq/official_texts_133180.htm)

feladat és kihívás egyben, amihez az állam bizonyos pontokon a társadalom számára elfogadható kereteket, célzott támogatásokat és hiteles alapinformációkat adhat és csak ezektől eltérő más pontokon lehet a tevőleges fellépés kizárólagos vagy elsődleges letéteményese a védelmi és biztonsági szervei útján.[43]

Zárszó

Az előzőekben leírtak összegzéseként tehát azt mondhatjuk, hogy az információs korszak számos átütő változást hozott magával. Ezek közül csak példálózással emelhetők ki a fizikai térben eddig erősnek tekintett távolságok, korlátok jelentőségének mérséklése, a 0-24 órás információáramlás és elérhetőség, a hálózatos jellegből adódó nehézkes kontrollálhatóság, az egyéni és társadalmi szintű kapcsolatokra és pszichére gyakorolt jelentős hatás, illetve a gazdasági élet dinamikáját érintő változtató képesség.

Magától értetődő, hogy egy ilyen széles körű hatásmechanizmusban vagy inkább – mátrixban a biztonsági tényezők és jelentős súllyal a katonai vonatkozások is megjelennek. Az információs tér egyértelműen a nem kinetikus erőkifejtésen alapuló hadviselési módozatok forradalmi fejlődését hozta magával, aminek talán a teljes horizontját még át sem látjuk, különösen akkor nem, ha a hadviselés sok tekintetben megszorítónak tekinthető fogalmán túl a komplex biztonság egészére tekintünk ki.

Látni kell azonban azt is, hogy az információs tér és vele az információs társadalom olyan sokrétű és összetett, hogy annak vizsgálata számos szak- és tudomány terület metszeteként ragadható csak meg helyesen. Ennek megfelelően fontosnak láttuk, hogy jelen írásban is hasonló megközelítést alkalmazva tekintsünk ki az információs korszak kapcsolódásaira, különösen az állam védelmi és biztonsági vonatkozásai terén, figyelmet fordítva a talán hagyományosnak mondható katonai-hadtudományi megközelítéseken túl az állam- és jogtudományi, szociológiai és részint kormányzástani vonatkozásokra is.

E körben az információs korszak talán legkiemelkedő újdonsága az, hogy a biztonság szavatolása kapcsán az állam hagyományos feladatainak fennmaradása mellett soha nem látott súlyra tesz szert a társadalmi közeg. Kiemelendő, hogy a társadalmi környezet mindig is fontos volt a hadviselésben és az ennél tágabb rend- és biztonságszavatolásban is, de jelen korunk technológiai változásai és ezeknek a társadalom szövetébe való természetes beszivárgása miatt már nem, vagy nagyon nehezen – és biztos nem jogállami módon – képzelhető el egy „csak állami” vagy „csak társadalmi” súlyozottságú biztonsági szisztéma. Ebben a megközelítésben tehát az információs korszak és az információs társdalom nem csak az állam védelmi és biztonsági struktúrájának, eszköz- és szabályrendszerének korszerűsödését, hálózatosodását és mégis komplexebbé válását kell magával hoznia, hanem a nemzeti ellenállóképesség, a rezíliencia jelentős megerősítését is ebben a dimenzióban. A biztonság és vele a stabilitás, szabadság és fejlődés megalapozásában tehát új korszakba lép az állami-társadalmi kooperáció, aminek kulcsa az ellenállóképesség, és amelynek átfogó jellegét legjobban talán pont az információs korszak, az információs fölény és az információs hadviselés és befolyásolás vonatkozásain keresztül ragadhatjuk meg.

[43] Ennek kapcsán lásd: KÁDÁR Pál: A védelmi-biztonsági szabályozás reformjának egyes kérdései az Alaptörvényen túl. Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021 : 11 1-17. o.

Felhasznált irodalom

AIKEN, Mary: Cyber-csapda – Hogyan változtatja meg az online tér az emberi viselkedést, Budapest, Harmat – Új Ember Kiadó, 2020.

ALBERTS, David S., GARSTKA, John J., HAYES, Richard E., SIGNORI, David A.: Understanding Information Age Warfare, Washington, DC, DoD CCRP, 2001. 35-53. o.

ALBERTS, David S.: Information Age Transformation: Getting to a 21st Century Military. Washington DC, DoD CCRP, 2002.

ANSAH, Tawia: Lawfare: A Rhetorical Analysis. Case Western Reserve Journal of International Law, Vol. 43, 2010, 87–119. o.

ARQUILLA, John; RONFELDT, David: Cyberwar is Coming! Comparative Strategy, 12. évfolyam 2. szám 1993. 141–165. o.

BACHMANN, Sascha Dov– MOSQUERA, Andres B. Munoz: Lawfare and hybrid warfare – how Russia is using the law as a weapon. Amicus Curiae, Journal of the Society for Advanced Legal Studies, Summer 2015, 25–28. o.

BALOGH Gábor: Egy túlterhelt fogalom. Információs Társadalom, Infonia Alapítvány, 1. 2006.

BALOGH Péter: A magyar katonai rádiófelderítés története. Rendvédelem-történeti Füzetek XXIII. évf. (2013) 31-34. szám. 15-16. o.

BÁNYÁSZ Péter – KRASZNAY Csaba – TÓTH András: A NATO kibervédelmi szakpolitikája, In: SZENES Zoltán (szerk.) A mai NATO: A szövetség helyzete és feladatai, Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 2021, 130-149. o.

BÁNYÁSZ Péter: a közösségi média, mint az információs hadszíntér speciális tartománya. Hadmérnök XII. Évfolyam „KÖFOP" szám – 2017. október. 108-121. o.

BÉRZINA, Ieva: Total defence as a comprehensive approach to national security. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 71-89. o.

BUCHANAN, Ben: The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics. Cambridge – London, Harvard Univeristy Press, 2020.

CASTELLS, Manuel: Az évezred vége – Az információ kora. Budapest, Gondolat Kiadói Kör, 2007.

CATTARUZZA, Amaël: A digitális adatok geopolitikája. Hatalom és konfliktusok a big data korában. Budapest, Pallas Athéné Books, 2020.

DESSEWFFY Tibor: Digitális szociológia. Szociológiai képzelet a digitális korban. Budapest, Typotex Kiadó, 2019.

DUNLAP, Charles J. JR.: Law and Military Interventions: Preserving Humanitarian Values in 21 st Conflicts. (letöltve: 2021.06.10., https://people.duke.edu/~pfeaver/dunlap.pdf)

FARKAS Ádám – RESPERGER István: Az úgynevezett "hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai. In: FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020., 132-149. o.

FARKAS Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei. In: SLRG Working Paper 2021/1.

FARKAS Ádám: Komplex biztonság, hibrid konfliktusok, összetett válaszok. In Honvédségi Szemle 2020/4. szám, 11-23. o.

FODOR István: Merre megy a világ gazdasága, merre mehetünk mi? In: GLATZ Ferenc (szerk.): Az információs társadalom. Magyarország az ezredfordulón, Stratégiai kutatások a Magyar Tudományos Akadémián VI., MTA, Budapest. 2000. 95-113. o.

FREDERICKS, BRIAN: Information Warfare: The Organizational Dimension. Institute for National Strategic Studies, 1996.

HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest. 2018. 158-167. o.

HAMILTON, Daniel S. (eds.): Forward Resilience. Protecting Society in an Interconnected World. Washington, Center for Transatlantic Relations – Johns Hopkins University, 2016.

HEEKS, Richard: Do information and communication technologies (ICTs) contribute to development? 2010. Journal of International Development, 22(5), 625–640. o

HÓDOS László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai. In: Honvédségi Szemle 2020/4. szám, 49-64. o.

HÓDOS László: A nemzetbiztonsági szolgálatok közelmúltbeli tevékenységét befolyásoló mérföldkövek,avagy az új típusú biztonsági kihívások jelentette veszélyek és az azokra adott kormányzati, illetve jogalkotói válaszok 2010 és 2020 között. In Szakmai Szemle 2021/1. szám 134-149. o.

IGNATOW, Gabe: Sociological Theory in the Digital Age. London – New York, Routledge, 2020.

JANELIŪNAS, Tomas: The deterrence strategy of Lithuania: in search of the rigth combination. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 180-198. o.

JOBBÁGY Szabolcs: A negyedik generációs hadviselés infokommunikációs aspektusai – fogalmi kitekintő. In: Hadmérnök 2017/1. szám, 203-213. o.

JOHANSSON, Per: Total defence demands new types of collaborations (letöltve: 2021.07.30., https://soff.se/en/our-focus/total-defense/)

KÁDÁR Pál: A hibrid kihívások és a működő államszervezet: Gondolatok egy konferencia margójára. Honvédségi Szemle: a Magyar Honvédség központi folyóirata 148: 4; 3-10. o., 2020.;

KÁDÁR Pál: A nemzeti ellenállóképesség és a kormányzás folytonossága – Rendvédelmi összefüggések. Pécsi Határőr Tudományos Közlemények 2021: 23. 19-28. o.

KÁDÁR Pál: A védelmi-biztonsági szabályozás reformjának egyes kérdései az Alaptörvényen túl. Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021 : 11 1-17. o.

KAPLAN, A.- HAENLEIN, M.: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010.

KATZ, Eian: Information Operations in International Humanitarian and Criminal Law: Reflections on the Oxford Statement (letöltve: 2021.11.24., http://opiniojuris.org/2021/07/22/information-operations-in-international-humanitarian-and-criminal-law-reflections-on-the-oxford-statement/)

KEARNEY, Michael: Lawfare, Legitimacy and Resistance: The Weak and the Law. In: Ardi IMSEIS (ed.): The Palestine Yearbook of International Law. Martinus Nijhoff Publishers, Leiden, 2010, 79–129. o.

KELEMEN Roland – NÉMETH Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése, In: FARKAS Ádám (szerk.): Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében, Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, 147-170. o.

KELEMEN Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése, Honvédségi Szemle, 2020/4 szám, 65-81. o.

KELEMEN Roland: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban, In: SmartLaw Research Group Working Paper, 2021/2. szám, 1-17. o.

KELTON, Kari: Learning from the Enemy: Approaches to Identifying and Modelling the Hidden Enemy Organization In KOTT, Alexander (szerk.): Information Warfare and Organizational Decisionmaking, Norwood, MA: Artech House, 2007, 29-63. o.

KESZELY László: A nemzeti ellenállóképesség fejlesztésének trendjei. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/6. (letöltve: 2021.11.28.; https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20M%C5%B1helytanulm%C3%A1nyok%202021_6_Keszely%20L%C3%A1szl%C3%B3_A%20nemzeti%20ellen%C3%A1ll%C3%B3k%C3%A9pess%C3%A9g%20fejleszt%C3%A9s%C3%A9nek%20trendjei.pdf)

KESZELY László: A védelmi igazgatás szerepe a nemzeti szintű átfogó megközelítés megvalósításában. Budapest, Nemzeti Közszolgálati Egyetem, doktori értekezés, 2017.

KHADER, Majeed– NEO, Loo Seng– CHAI, Whistine Xiau Ting: Introduction to Cyber Forensic Psychology. Singapore, World Scientific Publishing Co. Pte. Ltd.; 2021.

KISS Álmos Péter: A hibrid hadviselés természetrajza Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata 147:4. 2019. 17-37. o.

KISS Tibor – PARTI Katalin – PRAZSÁK Gergő: Cyberdeviancia. Budapest, Dialóg Campus Kiadó, 2019.

KITTRIE, Rode F.: Lawfare. Law as a Weapon of War. New York, Oxford University Press, 2016.

KLEIN Tamás – TÓTH András: Technológia jog – Robotjog – Cyberjog, Budapest, Wolters Kluwer, 2018.

KOLIN Péter: Evolúció és kultúra. Budapest, Információs Társadalom, Infonia Alapítvány, 3. 58-78. o.; MÉSZÁROS Rezső: A kibertér és a globalizáció. 2004, eVilág, 4-9. o.;

LAURENCE, Janice H.; MATTHEWS, Michael D.: The Oxford Handbook of Military Psychology. Oxford University Press, 2012.

LIBICKI, Martin: What is Information Warfare? US National Defence University ACIS Paper 3. 1995.

LIND, William S.– THIELE, Gregory A.: 4th Generation Warfare Handbook. Kouvola, Castalia House, 2015.

LIND, William S.: Understanding Fourth Generation War. In: Military Review 2004/September-October, 12-16. o.

LIND,William S.: The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, Vol. 73, No. 10 1989. 22–26. o.

LUPTON, Deborah: Digital Sociology. London – New York, Routledge, 2015.

MAVOR A. S.; PEW R. W.: Modeling Human and Organizational Behavior: Application to Military Simulations, Washington, D.C.: National Academy Press, 1998.

MOLNÁR Ferenc: A reziliencia kérdése és a NATO. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/15. (letöltve: 2021.11.28., https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20M%C5%B1helytanulm%C3%A1nyok%202021_15_%20Moln%C3%A1r%20Ferenc_A%20reziliencia%20k%C3%A9rd%C3%A9se%20%C3%A9s%20a%20NATO.pdf)

MUNK Sándor: Az információs fölényről. Hadtudomány, 11. évf. 3. sz. 2001. 43–52. o.

MUNK Sándor: Információs színtér, információs környezet, információs infrastruktúra. Nemzetvédelmi Egyetemi Közlemények, 6. évf. 2. sz. 2002. Online http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1083/nek_2002_2_munk.pdf?sequence=1&isAllowed=y (Elérés időpontja: 2021. november. 2.)

NAGY Viktor, ERDÉSZ Viktor: Az információs védelem és az információs műveletek szerepe a nemzetvédelemben. Felderítő Szemle X. évfolyam 3-4. szám . szeptember-december 51. o.

NATO Allied Joint Doctrine for Information Operations (AJP-3.10) LEX-7. 2015. Online: https://info.publicintelligence.net/NATO-IO.pdf (Elérés időpontja: 2021. november 2.)

NATO CDS: Enhancing the Resilience of Allied Societies through Civil Preparedness (letöltve: 202.07.30., https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/011%20CDS%2021%20E-%20RESILIENCE%20THROUGH%20CIVIL%20PREPAREDNESS_0.pdf)

NATO: Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016. (letöltve: 2021.07.30., https://www.nato.int/cps/en/natohq/official_texts_133180.htm)

NATO: Strengthened Resilience Commitment. 14. Juny 2021. (letöltve: 2021.07.30., https://www.nato.int/cps/en/natohq/official_texts_185340.htm)

NYÍRI Kristóf: Globális társadalom, helyi kultúra. IIn: GLATZ Ferenc (szerk.): Az információs társadalom. Magyarország az ezredfordulón, Stratégiai kutatások a Magyar Tudományos Akadémián VI., MTA, Budapest. 2000. 43-64. o.

O'HARA, Kieron– HALL, Wendy: Four Internets: Data, Geopolitics, and the Governance of Cyberspace. Oxford, Oxford Scholarship Online: July 2021.

Oxford Institute ELAC: The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities (letöltve: 2021.11.24., https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities)

PAGANINI, Pierluigi: Data, the New Power in Geopolitics (letöltve: 2021.11.24., https://www.ispionline.it/en/pubblicazione/data-new-power-geopolitics-30657)

PORKOLÁB Imre: Az aszimmetrikus hadviselés adaptációja: A tradicionális és irreguláris hadikultúrák összecsapásainak vizsgálata. Budapest, Magyarország : Ludovika Egyetemi Kiadó, 2020.

PRAKS, Henrik: Estonia's approach to deterrence: cimbining central and extended deterrence. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 146-162. o.

QURESHI, Waseem Ahmad: Information Warfare, International Law, and the Changing Battlefield. In: Forsham International Law Journal 2020/4., 901-937. o.

RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Negyedik generációs hadviselés. In: Honvédségi Szemle 2014/1. szám, 4-12. o.

ROEPKE, Wolf-Diether– THANKEY, Hasit: Resilience: the first line of defence (letöltve: 2021.07.30., https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html)

ROSENBACH, Eric - MANSTED, Katherine: The Geopolitics of Information. Cambridge, Belfer Center for Science and International Affairs Harvard Kennedy School, 2019.

RÓZSA Tibor: Az információs műveletek vizsgálata, különös tekintettel a befolyásolási képességek alkalmazásának lehetőségeire a magyar honvédség feladatrendszerében. PhD-értekezés kézirata. Budapest, NKE Hadtudományi Doktori Iskola 2006. Online: http://archiv.hhk.uni-nke.hu/uploads/ media_items/rozsa-tibor-ezredes-az-informacios-muveletek-alkalmazasanak-lehetosegei-a-magyar-honvedseg-feladatrendszereben.original.pdf (Elérés időpontja: 2021. november 2.)

S&D MAGAZINE: Resilience: Planning for Sweden's "Total Defence" (letöltve: 2021.07.30., https://sd-magazine.com/avis-experts/resilience-planning-for-swedens-total-defence).

SALONIUS-PASTERNAK, Charly: Finland's ambiguous deterrence: mixing deterrence by denial with ambiguous extended deterrence. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 110-127. o.

SARI, Aurel: Blurred Lines: Hybrid Threats and the Politics of International Law. Helsinki, The European Centre of Excellence for Countering Hybrid Threats, 2018.

SARI, Aurel: Hybrid Warfare, Law and the Fulda Gap (letöltve: 2021.07.30., https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2927773_code957129.pdf?abstractid=2927773.&mirid=1)

SARI, Aurel: Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats. Exeter, Exeter Centre for International Law, 2019.

SOMKUTI Bálint: A 4. generációs hadviselés. In: Hadtudományi Szemle 2009/2. szám, 42-51. o.

SZABÓ András: Az információs hadviselés és hadtudomány. Hadtudomány, 8 évfolyam4. szám 1998. Online: http://www.zmne.hu/kulso/mhtt/hadtudomany/1998/ht-1998-4-5.html (Elérés időpontja: 2021. november 2.)

TOWNSEND, Jim– AGACHI, Anca: Build Resilience for an Era of Schocks. In: Christopher SKABULA (eds.): NATO 20/2020. Twenty Bold Ideas to Reimagine the Alliance after the 2020 US Election. Washington, The Atlantic Council, 2020.

VANAGA, Nora: Latvia's defence strategy: challenges in providing a credible deterrence posture. In: Nora VANAGA – Toms ROSTOKS (eds.): Deterring Russia in Europe. Defence Strategies for Neighbouring States. London – New York, Routledge, 2019., 163-179. o.

VARGA Csaba – UHRIN Emese: Új demokrácia- és államelmélet. Budapest, Századvég Kiadó, 2007. 17-57.o.

VÉGH Károly: Információs és befolyásolási műveletek a nemzetközi jog „szürke zónájában". In: FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020., 191-212. o.

VIKMAN László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságraA közműszolgálatátoks és reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/14. (letöltve: 2021.11.28.; https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK_M%C5%B1helytanulm%C3%A1nyok_2021_14_Vikman%20L%C3%A1szl%C3%B3_A%20k%C3%B6zm%C5%B1szolg%C3%A1ltat%C3%A1sok%20%C3%A9s%20a%20reziliencia%20egyes%20k%C3%A9rd%C3%A9sei,%20k%C3%BCl%C3%B6n%C3%B6s%20tekintettel%20a%20kiberbiztons%C3%A1gra.pdf)

VIKMAN László: A művelettervezés jogi feladatai. In Honvédségi Szemle 2021/2. szám, 44-56. o.

WALTZ, Edward: Information Warfare: Principles and Operations, Artech House, Inc., Norwood, 1998, 108-110.o.

WITHER, James Kennet: Back to the future? Nordic total defence concepts. In: Defence Studies Vol. 20. 2020, 61-81. o.

Z. KARVALICS László: Információ, tudás, társadalom, gazdaság, technológia: egy egységes terminológia felé. Információs Társadalom. Budapest, Infonia Alapítvány, 4., 2005. 7-17. o.