

SLRG Research Paper – Nr. 2022/3.



SmartLaw Research Group

**Gondolatok az információs műveletek
következő generációjának stratégiai
kérdéseiről**

*Meglátások Jack Kiesler „A Next Generation
National Information Operations Strategy and
Architecture” című munkája kapcsán*

Spitzer Jenő

Jack Kiesler az információs műveletek következő generációjának stratégiai kérdéseiről pragmatikus, határozott és direkt megoldásokkal szolgáló gondolatokat mutat fel írásában. Hitelessége szakmai múltjából és a tanulmány rendezettségéből is fakad, amit tovább erősít az ágazati szakértők széleskörű bevonása. A jelen írás mindezek mentén közvetít stratégiai szintű meglátásokat az információs műveletek tárgyi és adaptív irányairól, az új típusú hadviselésről, az ágazatokon átnyúló kérdésekről és ezekben a védelmi-biztonsági reform kiemelt szerepéről.

Kulcsszavak: *információs művelet, hibrid hadviselés, kibertér, összágazatiság, védelmi-biztonsági reform, új típusú hadviselés, stratégia*

Jack Kiesler offers pragmatic, decisive and direct thinking on strategic issues for the next generation of information operations. His credibility stems from his professional background and the rigour of the paper, which is further enhanced by the extensive involvement of industry experts. In this context, the present paper provides strategic insights on the material and adaptive directions of information operations, new generation of warfare, cross-sectoral issues and the prominent role of defence-security regulation reform in these.

Keywords: *information operations, hybrid warfare, cyberspace, cross-sectoral solutions, defence-security regulation reform, new generation of warfare, strategy*

Jack¹ Kiesler² az információs műveletek következő generációjának stratégiai és szerkezeti kérdéseit vizsgáló munkáját³ úgy vezeti be, hogy az érintett területet, kiváltképpen magát az információt a hatalom gyakorlásának az egyik alapvető, ám mégis sokszor háttérbe szoruló eszközeként azonosítja. Mindezt a diplomáciai, a katonai és a gazdasági aspektusokkal helyezi egy szintre, mint az országnak a más országok

vagy nemzetközi szervezetek, de akár nem állami szereplők⁴ befolyásolásához szükséges eszközét. A szerző paradoxonként látatja, hogy habár az Egyesült Államok kitűnően teljesít az információs hatalom legtöbb elemében – a diplomácia, közügyek, az ún. „puha hatalom” (soft power), a kommunikációs erőforrások (média és közösségi média) és a nemzetközi fórumok területén – azonban úgy tűnik, nem képes

¹ Jelen mű a Nemzeti Közzolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék keretében működő Katonai Nemzetbiztonsági Kibertér Művelési Szakcsoport keretében végzett kutatás részeként született.

² Jack Kiesler a Védelmi Hírszerző Ügynökség (Defense Intelligence Agency) nemzetbiztonsági szakértője, aki a védelmi és katonai hírszerzés területén szerzett tapasztalatokkal rendelkezik, pályáját javarészt a kiber-, technikai és információs műveletekkel kapcsolatos kémelhárítási tevékenységeknek szenteli.

³ Jack KIESLER: *A Next Generation National Information Operations Strategy and Architecture*. Cambridge, Belfer

Center for Science and International Affairs Harvard Kennedy School, National Security Fellowship Program, Research Paper.. 2021.

⁴ Nem állami szereplőkről lásd bővebben: KAJTÁR Gábor: *A nem állami szereplők elleni önvédelem a nemzetközi jogban*. Budapest, ELTE Eötvös Kiadó, 2015.; 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.; SPITZER Jenő: *Önvédelem versus terrorizmus: Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2019.



mindezt minden esetben a stratégiai nemzeti célok elérésére is felhasználni.⁵ A nemzetközi trendekre figyelemmel megkerülhetetlennek tartja, hogy az információs hatalom elemeinek szinkronizálása olyan kérdésekben is erősödjön, mint a kritikus infrastruktúra, az ellátási láncok, a közbiztonság vagy a közegészségügy.⁶

A Kiesler által tett összehasonlítás a hatalomgyakorlás eszközeinek egyik legnépszerűbb

tudományos és gyakorlati felosztásából indul ki, az úgynevezett „DIME” modellből. A „DIME” rövidítést (diplomatic, informational, military, economic, azaz diplomáciai, információs, katonai és gazdasági) hosszú évek óta használatos a nemzeti hatalomgyakorlás eszközeinek a leírására, ugyanakkor az azokra gyakorolt hatások és az eszközök komplexitása okán napjainkra erősen meghaladottá vált. Érthető ez alatt többek között a globalizáció áthálózó lenyomata is,⁷ de még inkább a civil kompetenciák állami szektorba való befecskendezése és az átalakuló katonai dimenziók állandósulása is. A döntéshozók és alapvetően a stratégiai szint jó ideje ezek okán egy szélesebb kört határoz

„...az elmúlt évtizedek technológiai fejlődése, a társadalom széles rétegei felé felmutatható és elérhető eredményei, mint a jóformán határtalan kommunikációs lehetőségek, az információáramlás folyamatosága és gyorsasága, továbbá a globalizáltság paradigmaváltást hoztak. Kihívás ez az egyénnek, a társadalomnak, és még inkább az államhatalom stabilitását biztosító mechanizmusoknak...”

meg a nemzeti hatalomgyakorlás instrumentumainál, a „MIDFIELD” akronimmal jelölt (military, informational, diplomatic, financial, intelligence, economic, law, development, tehát katonai, információs, diplomáciai, pénzügyi, hírszerzési, gazdasági, jogi és fejlesztési) modellt használva. Egyes elgondolások⁸ a „PMESII” (political, military, economic, social, informational, infrastructure) akronimmal operálnak, ami a

téma tekintetében továbbra is fókuszban tartja az információs tényezőket, de külön társítja mellé a társadalmi aspektusokat is. Mindez nemcsak egy szélesebb látásmódot jelent, hanem azt is, hogy a diplomáciai, információs, katonai és gazdasági tényezők ne mutassanak átfedést a pénzügyi, a hírszerzési, a jogi és a fejlesztési, politikai, vagy adott esetben társadalmi elemekkel. Mindez persze nem egy vegytiszta izoláltságot jelent, hanem egy erős definiáltságot, ami az elemek közötti viszonyrendszert is láttatja.⁹

Általános jelenségként mutatkozik, hogy az elmúlt évtizedek technológiai fejlődése, a társadalom széles rétegei felé felmutatható és elérhető eredményei, mint a

⁵ Ezzel szemben: „West Point-i katonai szakértők hangsúlyozzák, hogy az oroszok szinte példa nélküli módon egymást kiegészítve, kombinálva alkalmazzák a kiberhadviselés, az elektronikus hadviselés (EW) és az információs műveletek (IO) eszközparkját.” – KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődésében*. In: *Hadtudományi Szemle*, 2020/4. szám, 76. o.

⁶ Jack KIESLER i.m. (2021) 4. o. A téma kapcsán lásd még: *Instruments of National Power*. In: *The Lightning Press SMARTbooks*. Online: <https://www.thelightingpress.com/the-instruments-of-national-power/> (Elérés dátuma: 2022. február 19.)

⁷ PONGRÁCZ Alex: *Nemzetállamok és új szabályozó hatalmak a globális erőterben – avagy megszelídíthető-e a globalizáció?* Budapest, Dialóg Campus, 2019.; SZIGETI

Péter: *Világrendszernézőben. Globális „szabad verseny” – a világgazdaság jelenlegi stádiuma*. Budapest, Napvilág Kiadó, 2005.

⁸ Így a NATO művelettervezési módszertana, a COPD (NATO Comprehensive Operations Planning Directive) is. Ennek kapcsán lásd: VIKMAN László: *A művelettervezés jogi feladatai*. In: *Honvédségi Szemle* 2021/2. szám, 44-56. o.;

⁹ A hatalomgyakorlás fent tárgyalt eszközei tekintetében lásd még: Jack D. KEM: *Understanding the operational environment: the expansion of DIME*. In: *The Free Library, U.S. Army Intelligence Center and School 2007.*; Joint Doctrine Note 1-18 of Joint Chiefs of Staff, azaz Vezérkari Főnökök Egyesített Bizottságának 1-18. sz. doktrínája; Robert KOZLOSKI: *The Information Domain as an Element of National Power*. Washington, Strategic Insights of Center for Contemporary Conflict, 2008.



jóformán határtalan kommunikációs lehetőségek, az információáramlás folyamatossága és gyorsasága, továbbá a globalizáltság paradigmaváltást hoztak. Kihívás ez az egyénnek, a társadalomnak, és még inkább az államhatalom stabilitását biztosító mechanizmusoknak, ami a végrehajtó és a jogalkotó hatalmat is új rugalmas keretek kimunkálására kényszeríti. Katonai szempontból megközelítve látható, hogy a hadviselés negyedik generációja¹⁰ ehhez a felgyorsult és globalizált szisztémához szervesen kapcsolódik, ami a technológiai szinten tartás és az államköziség dimenzióján túl a nem állami szereplők térnyerésével szintén számolni kényszerül. A biztonságot fenyegető hibrid szcenáriókban az infokommunikációs környezet és abban a társadalmi, gazdasági, politika, valamint biztonsági tényezők fúziója mutatja az érdemi kihívást, ami a komplex biztonság tág értelmezésének pályájára kényszeríti a döntéshozókat. Ahogyan a perspektíva kiszélesedik, akképpen figyelhető meg az is, hogy a hagyományos, technokrata és konvencionálisan katonai szempontok az adaptív megközelítés, a befolyásolás

közvetett és közvetlen hatásaiban rejlő lehetőségek korszerűsége és hatékonysága intenzív erózió előtt állnak, ami miatt szükségszerű a komplex biztonsághoz alkalmazkodó, átfogó és komplex megközelítés erősítése.¹¹

Az információs műveletek dogmatikai összetétele és gyakorlati vonatkozásai egyfajta „információs művelési robbanásként” szélesednek ki, a befolyásolás és a beavatkozás az állami és a nem állami érdekérvényesítés kiemelt útvonalává avanszál.¹² Az ehhez szükséges információs fölény pedig – utalva a fentebb kifejtett paradigmaváltásra – csak úgy képes érdemi előnyt nyújtani a védekezésben és a támadásban is, ha a tudástöbblet mellett a kellő hatóképesség és befolyásolással szembeni reziliencia is felmutatható. Az információs műveletek aktív és passzív alkotóelemeinek a jogállami keretek között tartása, továbbá a nemzetközi béke és biztonság igényeihez illesztése természetszerűleg igényel olyan stratégiai elgondolásokat és szabályozási koncepciókat, amik – akár csak a hibrid konfliktus természetét¹³ is felismerve – túlmutatnak a

¹⁰ A téma kapcsán lásd: KÁDÁR Pál: *A hibrid kihívások és a működő államszervezet: Gondolatok egy konferencia margójára*. In: Honvédségi Szemle: a Magyar Honvédség központi folyóirata 148: 4; 2020, 3-10. o.; RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: *Negyedik generációs hadviselés*. In: Honvédségi Szemle 2014/1. szám, 4-12. o.; JOBBÁGY Szabolcs: *A negyedik generációs hadviselés infokommunikációs aspektusai – fogalmi kitekintő*. In: Hadmérnök 2017/1. szám, 203-213. o.; WILLIAM S. LIND – GREGORY A. THIELE: *4th Generation Warfare Handbook*. Kouvola, Castalia House, 2015.; 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.

¹¹ Ennek kapcsán lásd: FARKAS Ádám: *Az állam fegyveres védelmének alapvonalai*. Budapest, Katonai Nemzetbiztonsági Szolgálat, 2020; FARKAS Ádám: *A totalitás kora?* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

¹² FARKAS Ádám – SPITZER Jenő: *Az információs korszak és az állam reziliencia egyes kérdései*. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/18. szám 5. o.; Példaként lásd még: Oxford Institute ELAC: *The Oxford Statement on International Law Protections in Cyberspace: The Regulation*

of Information Operations and Activities (letöltve: 2022.02.21., <https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities>); EIAN KATZ: *Information Operations in International Humanitarian and Criminal Law: Reflections on the Oxford Statement*. (letöltve: 2022.02.21., <http://opiniojuris.org/2021/07/22/information-operations-in-international-humanitarian-and-criminal-law-reflections-on-the-oxford-statement/>); WASEEM AHMAD QURESHI: *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.; FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája” című kötetének főbb üzenetei*. In: SLRG Working Paper 2021/1.

¹³ 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., 239 p. pp. 132-149.; RESPERGER



tisztán katonai dimenzióhoz tartozó jogelemzésen. Ez nem csupán a globalizált polgári elemek információs társadalmi jellemzőinek az adaptálását jelenti a kormányzati és a katonai oldalon, hanem a polgári elemek komplex stratégiai érdekek megóvásához alkalmas ellenállóképességének¹⁴ a kidolgozását is.

Kiesler mélyrehatóan vizsgálja a rendelkezésre álló forrásokat, vezető információs műveleti szakemberek állásfoglalásait is beépítve annak érdekében, hogy széles körben azonosítsa az amerikai információs műveleti eszköztárat sújtó stratégiai hiányosságokat. A nemzeti információs műveleti közösséghez kapcsolódó kulcs emberekkel készített interjúk és az azt megelőző elemzések szintetizálására építve javaslatot tesz egy új, az ország információs erejét kiaknázó és célkitűzéseit kiszolgáló stratégiára és szerkezetre. Ennek eléréséhez maga a szerző is sarkalatos pontként tekint a közvélemény támogatására, a döntéshozatal politikai érdekek szerinti befolyásolásának megakadályozására szolgáló fékekre és ellensúlyokra, valamint jogszabályi környezetre és kontrollra.

A szerző öt stratégiai hiányosságot jelöl meg neurálgikus pontként. Elsőként kiemeli a nemzeti információs műveleti architektúra vezetéséhez szükséges egyértelmű vezetési-irányítási rendszer hiányát. Meglátása szerint az információs műveletek rendkívül összetett és széttagolt területén nincs kifejezett vezetői szint, amely

feladatrendszert határozna meg, irányítana, erőforrásokat biztosítana. Ennek következtében kiválósági központok sora jött létre, amelyek bár sikeresek, a nemzeti jövőkép vagy a nemzeti erősségeket a célok elérése érdekében hasznosító vezetés ellenére, nem pedig annak köszönhetően valósultak meg. Második pontként Kiesler az össznemzeti védelmi képességeknek a nem állami szereplőkkel szembeni kitettségét és a hazai magánszektor involválódásának fejlesztését, a kellő összhang hiányát emeli ki.

„...azzal kapcsolatban is aggodalmát fejezi ki, hogy egy háborús vagy „szürke zónás” konfliktus esetére az ország jogrendszere ezen a területen nem enged különbséget tenni a béke idős működés és az attól eltérő időszakok között és ragaszkodik a béke idős szűkebb fellépési keretekhez, ami hátrányokhoz vezethet...”

Harmadik kritikai fordulatával a szerző a jogszabályi keretrendszert célozza meg. Meglátása szerint az Egyesült Államoknak jelentős fókuszot kellene helyeznie az erőalkalmazási szabályokkal való összhang megteremtésére, valamint a fegyveres konfliktus küszöbértéke alatt tartott, „szürke zónás” tevékenységekre.

Kiesler azzal kapcsolatban is aggodalmát fejezi ki, hogy egy háborús vagy „szürke zónás” konfliktus esetére az ország jogrendszere ezen a területen nem enged különbséget tenni a béke idős működés és az attól eltérő időszakok között és ragaszkodik a béke idős szűkebb fellépési keretekhez, ami hátrányokhoz vezethet, ami bizonyos fokú optimalizációt igényelhet. A felsorolás negyedik pontja a kémelhárítást célozza: az ilyen tevékenységre felhatalmazott szervek tevékenységének tempóját a „szürke zónás” tevékenységekhez tartja szükségesnek felzárkóztatni, ami leginkább az interoperabilitás¹⁵ fokozásával érhető el.

István: *A válságkezelés és a hibrid hadviselés*. Budapest, Dialóg Campus Kiadó, Nordex Kft, 2018.

¹⁴ Ennek tekintetében lásd: MOLNÁR Ferenc: *A reziliencia kérdése és a NATO*. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/15. szám; HARNISCH-THIES- FRIEDRICH: *The logic of resilience in transatlantic relations*. In: *The Politics of Resilience and Transatlantic Order – Enduring Crisis?* London: Routledge, 2019; KÁDÁR Pál: *A pandémia*

kezelése mint a nemzeti ellenálló képesség „tesztje”. In: Honvédségi Szemle, 149.2. (2021)

¹⁵ E tekintetben a szerző azt világítja meg, hogy az információs műveletekkel kapcsolatos támadás forrása kezdetben ismeretlen és sokszor nagyon kevés idő áll csak rendelkezésre az effektív elhárításhoz és a válaszadásra. A szövetségi jogszabályok és eljárások biztosítják, hogy a hálózati támadásokat a hírszerző közösség ne vizsgálja ki, ha úgy gondolják, hogy azok amerikai személytől származnak és ezáltal hírszerzési



Ötödik pontként a felsorolást az adatvédelmi és adatkezelési szempontok zárják.

A tanulmány értelmezése szerint az Egyesült Államok jelenleg lemaradásban van az információs műveletek szempontjából fontos információmegosztást támogató biztonságos, minősített digitális keretrendszer létrehozásában. Egy olyan digitális keretrendszer, adathalmaz, amely elemezni és döntést előkészíteni is képes, továbbá a mai mesterséges intelligencia képességeivel figyelemre méltó hatásokat érhet el, így például a dezinformáció cáfolását is. A probléma gyökere azonban a közvélemény bizalmatlanságában jelenhet meg a kormányzatban és a magánélet védelmére vonatkozó jogszabályok betartásában, különösen a hatalmas adatmennyiségek hasznosítása, akár big data elemzések során.¹⁶

Kiesler a tanulmányban ezután tér ki azokra a lényegi pillérekre, amelyeknek a megvalósulását elengedhetetlennek tartja az információs műveleti stratégia és architektúra következő generációjába történő sikeres átlépéshez. Ezek közül az első egy nemzeti információs műveleti igazgató kijelölése¹⁷, aki egyfelől rendelkezik kiberfelügyeleti hatáskörrel, másfelől képes az információs műveleti közösség minden elemét összehangoltan vezetni, továbbá mindennapi kapcsolódással bír az Elnöki Hivatalhoz. A második pillérhez a szerző meglátása szerint a Kongresszusnak meg kell határoznia és finanszíroznia kell egy közös együttműködési környezetet vagy fúziós központot mind a védelmi, mind a támadási információs műveletek számára. Meglátása szerint egy központi koordinatív szerv nem csupán az interoperabilitást növeli, de a funkcionális

közösségek adatszolgáltatása által komoly helyzeti előnyt teremtő adatbázisokat hozhat létre. A harmadik pillér az össznemzeti jellegre erősítene rá akképpen, hogy a Kongresszus megbízására a belügyi és igazságügyi területek együttműködéséből létrejövő centrum dolgozna ki úgy az információs műveleti stratégiát, hogy abban mind a kibertevékenység,¹⁸ mind a nemzetbiztonsági szolgálatok tevékenysége, mind pedig a magánszektor szerepvállalása fajsúlyosan jelenne meg.¹⁹

A tanulmány következtetéseiben újfent az osztársadalmi reakciók fontosságára mutat rá, a dezinformáció felismerésére²⁰ és a kritikus gondolkodás meglétére. Ennek a szerepét olyannyira jelentősnek látja, hogy azt a mesterséges intelligenciában rejlő azonosítási képességek elé sorolja. Kiesler hangsúlyozza a magánszektornak, mint meglátása szerint a legmagasabb kiberszakmai tudásbázis bevonásának megkerülhetetlenségét, azonban a technológiai fejlődés és fenyegetettségekkel szembeni kiszámítható ellenállóságot úgy tudja elképzelni, ha ezek a piaci szereplők a témakör tekintetében szigorú állami ágazati felügyelet alatt működnének együtt egy jól funkcionáló kiberparancsnoksággal. A szerző szintén kiemelt szerepet szán az egyes fúziós központokba beágyazott nemzetbiztonsági szolgálati elemeknek, amelyek jogszabályi környezetben egy azonnali reakcióra alkalmas képességcsomagot és mechanizmust hivatott biztosítani annak érdekében, hogy egyszerre legyen képes kiszolgálni a háborús harcokat és a szürke zónában felmerülő érdekeket.²¹

és alapjogi elvek sérülnének. Az ellenérdekelt fél pedig kihasználja ezt azáltal, hogy olyan támadásokat hajt végre, amelyek azt a látszatot keltik, hogy az Egyesült Államokból származnak.

¹⁶ KIESLER 13-20. o.

¹⁷ Ennek vonatkozásában lásd: VIKMAN László: *Az amerikai titkosszolgálati rendszer áttekintése*. In: Katonai Jogi és Hadijogi Szemle 2020, 35-68. o.

¹⁸ FARKAS Ádám: *Kibertér művelet: Hírszerző, rendészeti és katonai műveletek elegye?: Gondolatok az angol National Cyber Force kapcsán*. In: Military and Intelligence CyberSecurity Research Paper, 2021/1. szám 1-12. o.; VIKMAN László: *A német kiberbiztonsági szisztéma áttekintése: Szervezeti keretek, különös tekintettel a*

nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására. In: Military and Intelligence CyberSecurity Research Paper, 2021/2. 1-20. o.

¹⁹ KIESLER 21-35. o.

²⁰ A téma kapcsán lásd még: KELEMEN Roland: *Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben*. In: Jog Állam Politika, 2021/3. szám, 71-85.o. FARKAS Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

²¹ KIESLER 36-38. o.



Jack Kiesler kötetének elgondolásai felismerik az „információs műveleti robbanásnak” a recenzióban is részletezett korszakváltását, aminek eredménye egy az adaptív (befolyásolásra irányuló) direktívákban való elmélyültségről tanúskodó, a negyedik generációs hadviselés hibrid természete okán pedig a magánszektor bevonódását támogató és a társadalmi közeg felértékelődését elismerő stratégiai és szerkezeti koncepció.

Javaslati egyszerűen direkt, aprólékosak és forrásgazdagok, ugyanakkor szigorú keretbe foglaltak. Mindezek ugyanakkor a döntéshozónak szűk mezsgyét mutatnak, amiben éppen a kimunkált koncepció miatt egy-egy kérdésre szinte kizárólag egy-egy megoldási irány rajzolódik ki. Ennek a felvállalása mégis hitelt érdemel, aminek oka a szerző szakmai múltjához is köthető, de azt a tanulmány szerkezete, széleslátása és érvrendszere vitathatatlanul alátámasztja.

Kiesler írása mind témavezetésében, mind gondolatiságában könnyűszerrel alkalmazható. Elsőként megállapítható, hogy akár a DIME rendszert, akár annak kiszélesített változatait vesszük alapul, az érdemi nemzeti hatalomgyakorlás elengedhetetlen velejárója az információs térben való effektív és domináns jelenlét, polgári és katonai megközelítésből is.²² Szintén tapasztalható, hogy az információs közeg és az ott végbemenő műveletek számos hatalmi aspektussal állnak szerves kapcsolatban, amire többek között napjaink égetően megoldásra váró orosz-ukrán konfliktusa is rendszeresen mutat rá. Egy

dezinformációs hullám nem csak társadalmi feszültséget kelt, de fokozott információvédelemre kényszeríti a hírszerző tevékenységet és az államigazgatást is, befolyásolja a katonai műveletek sikerességét és eszkalációját, mindemellett képes megrengetni a tőzsdét, ami bizonytalan pénzügyi és végsősoron globális gazdasági nehézségekhez vezet. Ezeknek a mérlegelése pedig képes bénítólag hatni a világpolitika csaknem egészére.

A körülmények a haderőfejlesztésre és a fegyverkezésre is hatást gyakorolnak, hiszen az információs hadviselés konvencionális, technokrata oldala ezután sem lesz elhanyagolható, ugyanabból az okból kifolyólag, amiért láthatóan tévhitté válik a reguláris hadviselés alkonyának vizionálása és abban egyre inkább a feléledés és a kiszélesedés figyelhető meg. Mindezek mellett pedig, visszautalva a hatalomgyakorlás instrumentumaira, tovább erősödik az információs műveletek

„...az információs közeg és az ott végbemenő műveletek számos hatalmi aspektussal állnak szerves kapcsolatban, amire többek között napjaink égetően megoldásra váró orosz-ukrán konfliktusa is rendszeresen mutat rá. Egy dezinformációs hullám nem csak társadalmi feszültséget kelt, de fokozott információvédelemre kényszeríti a hírszerző tevékenységet és az államigazgatást is, befolyásolja a katonai műveletek sikerességét és eszkalációját, mindemellett képes megrengetni a tőzsdét, ami bizonytalan pénzügyi és végsősoron globális gazdasági nehézségekhez vezet.”

adaptív megközelítésének a szerepe is, ami habár financiálisan látszólag kevésbé erőforrás igényes, komoly kérdéseket szegez az államműködésnek. A konvencionális-adaptív aspektusok közös halmazát a reziliencia képes megadni, amiben az eredményesség kulcsai a preventív képességek, az éber tartott védelmi kapacitások, a támadólagosság képessége, valamint „célponthoz való” a kellő, társadalomban is mutatkozó forráskritika és felkészültség. Mindezek biztosítása olyan feltételek eléérése esetén teljes, mint az állam és a versenypiac közötti konszenzusos együttműködés, továbbá az állam

²² Ennek kapcsán lásd: RUSZIN Romulusz: *A Magyar Honvédség feladatrendszere és vállalásai, különös tekintettel a nemzetközi terrorizmus elleni fellépésre és a migrációs válságra*

In: FARKAS Ádám (szerk.): *Az állam katonai védelme az új típusú biztonsági kihívások tükrében*. Budapest, Nemzeti Közszerzői Egyetem, 2019. 60-74. o.



működésének minden ágát egy irányba terelő, interoperabilitást elősegítő és koordináló közeg. Így a megfelelő struktúrával és hatásköri rendszerrel a polgári, katonai és hírszerzési oldalaknak közös alap, célorientált vezetősztál teremődik. Említésre méltó a kérdéskör lélektani, szociológiai és edukációs vizsgálata, amelyben egyik oldalról a lélektani műveletek, és a civil-fegyveres együttműködési képességek erősítésének igénye mutatkozik meg, másfelől pedig – hozzá véve a kritikus gondolkodás legkorábbi, közoktatásban való megjelenését – markánsan szélesedhet a bölcsészettudomány és az állam- és jogtudomány gyakorlati keresztmetszete.

A védelmi-biztonsági reform kiindulási pontja lehet annak, hogy létrejőjön egy technikai bázis, ami egyúttal olyan jogkörökkel felruházott szervezeti egység, aminek a végrehajtó hatalomtól leágazva megfelelő struktúrája és működési mechanizmusa van. A reziliencia ebben a tekintetben nem csak materiális és vezetési-irányítási kérdés, de egy jogszabályrendszert is kell, hogy jelentsen., Olyan normarendszert, ami a közigazgatás egészét hatja át a témakörre nézve, kapcsolatot teremtve a közjog és a civilizisztika társadalmi mindennapokat és hosszútávú kérdéseket egyaránt szabályozó rendelkezései között. A reziliencia egyúttal a társadalmi tudatosságra is hatást hivatott gyakorolni, az információval szembeni kritikusságot és szkepticizmust, amiben az államhatalom arculattal szolgál, ami társadalmi együttműködést indikál és nagymértékben ellenálló a támadónak arculatvesztést célzó befolyásolásával szemben.

FELHASZNÁLT FORRÁSOK

- [1.] 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.
- [2.] 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.
- [3.] FARKAS Ádám – SPITZER Jenő: Az információs korszak és az állami reziliencia egyes kérdései. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/18. szám 5. o.
- [4.] FARKAS Ádám: A totalitás kora? Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.
- [5.] FARKAS Ádám: Az állam fegyveres védelmének alapvonalai. Budapest, Katonai Nemzetbiztonsági Szolgálat, 2020.
- [6.] FARKAS Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amaél Cattaruzza „A digitális adatok geopolitikája” című kötetének főbb üzenetei. In: SLRG Working Paper 2021/1.
- [7.] FARKAS Ádám: Kibertér művelet: Hírszerző, rendészeti és katonai műveletek elege?: Gondolatok az angol National Cyber Force kapcsán. In: Military and Intelligence CyberSecurity Research Paper, 2021/1. szám 1-12. o.
- [8.] HARNISCH-THIES- FRIEDRICH: The logic of resilience in transatlantic relations. In: The Politics of Resilience and Transatlantic Order – Enduring Crisis? London: Routledge, 2019
- [9.] JOBBÁGY Szabolcs: A negyedik generációs hadviselés infokommunikációs aspektusai – fogalmi kitekintő. In: Hadmérnök 2017/1. szám, 203-213. o.
- [10.] Joint Doctrine Note 1-18 of Joint Chiefs of Staff, azaz Vezérkari



- Főnökök Egyesített Bizottságának 1-18. sz. doktrínája;
- [11.] KÁDÁR Pál: A hibrid kihívások és a működő államszervezet: Gondolatok egy konferencia margójára. In: Honvédségi Szemle: a Magyar Honvédség központi folyóirata 148: 4; 2020, 3-10. o.
- [12.] KÁDÁR Pál: A pandémia kezelése mint a nemzeti ellenálló képesség „tesztje”. In: Honvédségi Szemle, 149.2. (2021)
- [13.] KAJTAR Gábor: A nem állami szereplők elleni önvédelem a nemzetközi jogban. Budapest, ELTE Eötvös Kiadó, 2015.;
- [14.] KATZ, Eian: Information Operations in International Humanitarian and Criminal Law: Reflections on the Oxford Statement. (letöltve: 2022.02.21., <http://opiniojuris.org/2021/07/22/information-operations-in-international-humanitarian-and-criminal-law-reflections-on-the-oxford-statement/>)
- [15.] KELEMEN Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődésében. In: Hadtudományi Szemle, 2020/4. szám, 76. o.
- [16.] 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.
- [17.] KELEMEN Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. In: Jog Állam Politika, 2021/3. szám, 71-85.o. FARKAS Ádám: A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.
- [18.] KEM , Jack D.: Understanding the operational environment: the expansion of DIME. In: The Free Library, U.S. Army Intelligence Center and School 2007.
- [19.] KIESLER, Jack: A Next Generation National Information Operations Strategy and Architecture. Cambridge, Belfer Center for Science and International Affairs Harvard Kennedy School, National Security Fellowship Program, Research Paper.. 2021.
- [20.] KOZLOSKI, Robert: The Information Domain as an Element of National Power. Washington, Strategic Insights of Center for Contemporary Conflict, 2008.
- [21.] LIND, William S.– THIELE, Gregory A.: 4th Generation Warfare Handbook. Kouvola, Castalia House, 2015.
- [22.] MOLNÁR Ferenc: A reziliencia kérdése és a NATO. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/15. szám
- [23.] Oxford Institute ELAC: The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities (letöltve: 2022.02.21., <https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities>)
- [24.] PONGRÁCZ Alex: Nemzetállamok és új szabályozó hatalmak a globális erőterben – avagy megszelídíthető-e a globalizáció? Budapest, Dialóg Campus, 2019.
- [25.] QURESHI, Waseem Ahmad: Information Warfare, International Law, and the Changing Battlefield. In: Forsham International Law Journal 2020/4., 901-937. o.
- [26.] RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Negyedik generációs hadviselés. In: Honvédségi Szemle 2014/1. szám, 4-12. o.
- [27.] RESPERGER István: A válságkezelés és a hibrid hadviselés. Budapest, Dialóg Campus Kiadó, Nordex Kft, 2018.
- [28.] RUSZIN Romulusz: A Magyar Honvédség feladatrendszere és vállalásai, különös tekintettel a nemzetközi terrorizmus elleni fellépésre és a migrációs válságra In:



- FARKAS Ádám (szerk.): Az állam katonai védelme az új típusú biztonsági kihívások tükrében. Budapest, Nemzeti Közszerzői Társaság, 2019. 60-74. o.
- [29.] SPITZER Jenő: Önvédelem versus terrorizmus: Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2019.
- [30.] SZIGETI Péter: Világrendszernézőben. Globális „szabad verseny” – a világkapitalizmus jelenlegi stádiuma. Budapest, Napvilág Kiadó, 2005.
- [31.] 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.
- [32.] VIKMAN László: A művelettervezés jogi feladatai. In: Honvédségi Szemle 2021/2. szám, 44-56. o.;
- [33.] VIKMAN László: A német kiberbiztonsági szisztéma áttekintése: Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására. In: Military and Intelligence CyberSecurity Research Paper, 2021/2. 1-20. o.
- [34.] VIKMAN László: Az amerikai titkosszolgálati rendszer áttekintése. In: Katonai Jogi és Hadijogi Szemle 2020, 35-68. o.



IMPRESSZUM

Szerző(k):

Dr. Spitzer Jenő

Kézirat lezárásának ideje:

2022. Március 11.

Szerkesztők:

Dr. Farkas Ádám PhD
Dr. Glavanits Judit PhD
Dr. Karácsony Gergely PhD
Dr. Kelemen Roland

Dr. Keserű Barna Arnold PhD
Dr. Király Péter Bálint
Dr. Spitzer Jenő
Németh Richárd

Kiadó:

Smart Law Research Group

Elérhetőségek:

<http://smartlawresearch.hu/>

ISSN:

2732-3846

A borító a <https://wallpaperaccess.com/download/iot-3246253> címen elérhető ingyenes háttérkép felhasználásával 2021. február 15-én készült.

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.

A sorozat célja a SmartLaw Reseach Group, illetve annak tagjai és esetleges külső együttműködők által végzett kutatások részeredményeinek közzététele a szakmai, tudományos megvitathatóság érdekében, illetve a későbbi publikációk előkészítésének támogatása érdekében.