Kovács László✧

Kibertér és tudomány

DOI 10.17047/HADTUD.2026.36.2.139

A kibertér meghatározó szerepet játszik a 21. század minden területén, legyen szó gazdaságról, politikáról, kultúráról vagy hadviselésről. A kiberműveletek és a tudomány közötti kapcsolat a 21. század egyik legösszetettebb és legdinamikusabban fejlődő interdiszciplináris kutatási területévé vált. A kibertér intézményes elismerése független működési dimenzióként – amelyet többek között a NATO is kinyilvánított 2016-ban – alapvetően megváltoztatta a biztonságpolitikai gondolkodást és új struktúrákat hozott létre a tudományos együttműködés terén is. A kiberműveletek már nem csupán technológiai vizsgálatokat igényelnek, hanem összetett társadalmi, politikai, jogi és etikai kontextusba ágyazott folyamatok elemzését is, amelyeket csak integrált tudományos megközelítéssel lehet megérteni.

KULCSSZAVAK: kibertér, tudomány, kiberműveletek, digitális társadalom, biztonság

Cyberspace and Science

Cyberspace plays a key role in every aspect of the 21st century, whether in economics, politics, culture, or warfare. The relationship between cyber operations and science has become one of the most complex and rapidly evolving interdisciplinary research fields of the 21st century. The institutional recognition of cyberspace as an independent domain of operations – as declared by NATO, among others, in 2016 – has fundamentally changed security policy thinking and created new structures in the field of scientific cooperation as well. Cyber operations no longer require mere technological analysis, but also the analysis of processes embedded in complex social, political, legal, and ethical contexts, which can only be understood through an integrated scientific approach.

KEYWORDS: cyberspace, science, cyber operations, digital society, security

Bevezetés

Az 1990-es évek második felében, az akkori Zrínyi Miklós Nemzetvédelmi Egyetemen olyan tudományos kutatások indultak, amelyek valódi paradigmaváltást eredményeztek a hadviselés hazai kutatásában. Persze ezek nem egyedülálló kutatások

✧ Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék egyetemi tanár, tudományos rektorhelyettes, a Hadtudományi Bizottság elnöke – *Ludovika University of Public Service Faculty of Military Science and Officer Training Department of Electronic Warfare professor, Vice Rector for Academic Affairs, Head of Military Science Committee*; e-mail:kovacs.laszlo@uni-nke.hu; https://orcid.org/0000-0002-6403-065

voltak, hiszen a nyugati, elsősorban az amerikai hadsereg és a köré szerveződő kutatóintézetek már több éve kutatták a hadviselés 20. század végének és az akkor még csak nagyon halványan körvonalazódó 21. század elejének és az abban várható katonai műveletek lehetséges jellemzőit. Az egyetemen jelen sorok szerzőjeként abban a szerencsés helyzetben voltam, hogy előbb egyetemi hallgatóként, majd doktoranduszként, ezt követően pedig kutatóként ezeknek a kutatásoknak az egyik legnagyobb gravitációs terébe, az Elektronikai Hadviselés tanszék munkájába kapcsolódhattam be. Ebben az inspiráló tudományos közegben, a tanszék és a hozzá szorosan, illetve kevésbé szorosan kapcsolódó kutatók hazánkban először kezdtek el a technikai, ezen belül is az információtechnológiai fejlődés, valamint ennek társadalomra és nem utolsó sorban a hadviselésre gyakorolt hatásaival is magas tudományos szinten foglalkozni.

Ez a munka elsőként a NATO és az amerikai doktrínák felkutatásával és azok magyarra történő fordításával kezdődött. Ne felejtsük el, hogy mindez évekkel hazánk 1999-es NATO csatlakozása előtt történt. Így nem csak a nyugati doktrínákat és szabályzatokat, hanem azokat a nyugati kutatásokat is meg kellett ismerni, amelyek tudományos módszerekkel az említett technológiai, elsősorban információtechnológiai – nyugodtan mondhatjuk forradalmi – fejlődés jelenkori és legfőképp jövőre gyakorolt hatásait vizsgálták.

Ezek a kutatások természetesen nem lettek volna eredményesek csak hazai szakemberek és vizsgálódásaik keretében, ezért nagy szükség volt az olyan nemzetközi együttműködésben végzett kutatásokra, amelyek során komoly kutatási hálózat is kialakult. Ennek egyik legjobb példája az egyik, mai szóhasználattal élve drón kutatási projekt, amely az Európai Unió támogatásával számos európai országból, illetve Izraelből ipari szereplőket, kutatóintézeteket és egyetemeket, egyetemi szakembereket fogott össze. Ez volt az úgynevezett UAVNET, amely a drónok polgári célú európai felhasználásának kérdéseit vizsgálta.[1]

Ugyanakkor ezeknek a kutatásoknak egyik iránya a 2000-es évek kezdetén egyre inkább az információs tér és az abban zajló információs műveletek felé fordult. Ebből az irányból, illetve annak egyik ágából pedig az évek során megszülettettek a kibertérrel kapcsolatos kutatások. Mivel maga a kibertér és a kibertérben használt eszközök és szolgáltatások egész sora fejlődött ki robbanásszerűen az élet minden területén, így ez a kutatási irány hamarosan nagyon népszerű lett a fiatal doktoranduszok körében is. Számos doktori kutatási téma született ezeken a területeken, amelyek sok esetben már nem csak elméleti eredményekkel, hanem valódi, kézzelfogható gyakorlati hasznosulással is jártak. Ezek az eredmények számos esetben a hadseregben, a rendőrség munkájában vagy akár a civil gazdasági szereplők esetében is nagyon jól hasznosíthatóak voltak.

Ugyanakkor ezen kutatások legfontosabb eredménye mégis az volt, hogy olyan iskolát, vagy ha tetszik kutatói közösséget teremtettek, amely közösség gondolkodása kihatással volt a kibertéri védelem és a kiberműveletek hazai alakítására és megvalósítására is.

1 Kovács,Ványa 2005.

Jelen írás ezeket a tudományos kutatásokat kívánja nagyon röviden, azok egyes elemeinek – azokat is teljesen szubjektív módon, a teljesség igénye nélkül – kiemelésével bemutatni az 1990-es évek közepétől egészen napjainkig. Mindezt teszi úgy, hogy a nemzetközi kutatások felvillantása mellett a hazai kutatásokba is bepillantást enged.

Jelen írás azonban terjedelmi korlátok miatt nem vizsgálja a kibertéri bűnözés különböző kérdéseit, és nem vizsgálja részletesen azt a technológiát sem, amely révén a kibertér létrejön.

A kibertér megjelenése a tudományos kutatásokban

A kibertérrel kapcsolatos tudományos kutatások kezdetéig a nem is olyan régmúltra kell visszamennünk. Az 1940-es és 50-es években indultak el azok a kutatások, amelyek közvetettt módon a kibertér[2] kialakulásához vezettek. Ezek a kutatások kezdetben az információelmélet, a kriptográfia és a számítástudomány kérdéseit és összefüggéseit vizsgálták, amelyek egyben – akkor persze még nem sejtett módon – a kibertéri kutatások hajnalát is jelentették. Így a kibertérben vagy az azon keresztül végzett műveletek tudományos megalapozottsága már a 20. század közepére megjelent.

Az 1940-es évek végén és az 1950-es évek elején komoly információ- és számítástudományi forradalom kezdődött. Ez a forradalom természetszerűleg párhuzamosan zajlott azzal a robbanásszerű technikai és technológiai fejlődéssel, amelyet abban a korban az elektronika, majd a mikroelektronika, ma pedig az informatika forradalma szavakkal tudunk a legjobban leírni. Claude Shannon 1948-as munkája, A *Mathematical Theory of Communication,* azaz a Kommunikáció matematikai elmélete nemcsak az információelmélet alapjait teremtette meg, hanem a modern kriptográfia elméleti hátterét is biztosította.[3]

Shannon munkássága bizonyította, hogy a titkosítás matematikailag formalizálható, és az entrópia fogalmán keresztül mérhető a kommunikáció biztonsága. E gondolatmenet a mai napig meghatározza a titkosítási rendszerek fejlesztését, és sokáig egyik legfontosabb alapja volt a kibervédelmi stratégiák kialakításának is.[4]

---

2 A kibertér meghatározására számos többé-kevésbé hivatalos definíció született. Ezek elemzése helyett most mégis a kibertér tágabb értelmezését adjuk meg. Ennek megfelelően, a kibertér az információs környezet részeként értelmezhető, amely egy folyamatosan változó, ember által létrehozott globális működési tér. A kibertér összekapcsolt kommunikációs, informatikai és egyéb elektronikus rendszerekből, valamint hálózatokból épül fel. Ide tartoznak az önálló vagy független rendszerek is, amelyek adatokat gyűjtenek, dolgoznak fel, tárolnak vagy továbbítanak. Nagyon sok elmélet eligazítást és modellt is ad a kibertér felépítésére, amelyek egyetértenek abban, hogy a kibertér három, egymással szorosan összefüggő rétegre bontható: fizikai, logikai és kiber-személyiség rétegre.

3 Shannon 1948. Elérés: https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf (Letöltve: 2026. 03. 31.)

4 Meg kell jegyezni, hogy a kriptográfia mai is kiemelten fontos a kiberbiztonságban, ugyanakkor emellett számos technikai és eljárásbeli, nem utolsó sorban szabályozási kérdés hasonló súllyal jelentkezik a biztonságos rendszerek megteremtése esetében. Ma a kriptográfia esetében már inkább az a kérdés, hogy a jelenleg használatos titkosítási algoritmusok kiállják-e a kvantumfizikai alapokon működő kvantumszámítógépek jelentette kihívások próbáit. Ez ma már a posztkvantum-titkosítás igen komoly kérdése.

A nyilvános kulcsú kriptográfia áttörése – amely Whitfield Diffie és Martin Hellman nevéhez köthető – radikálisan új dimenziót nyitott a digitális rendszerek biztonságában. A Diffie–Hellman kulcscsere protokoll, amelyet a szerzők 1976-ban publikáltak, lehetővé tette a biztonságos kommunikációt előzetes kulcscsere nélkül, ami a globális hálózati infrastruktúra egyik alapfeltétele lett.[5]

A számítógép-hálózatok megjelenésével és széleskörű elterjedésével számos elméleti és gyakorlati kutatás indult el a témában, amelyek eredményeként egyrészt megjelent a kibertér, mint fogalom, másrészt megjelentek a kibertéri tevékenységeket vizsgáló tudományos kutatások is. A tudományos publikációk gyorsan adaptálódtak a katonai és kormányzati igényekhez, miközben a polgári szféra – különösen az elektronikus kereskedelem – is profitált az eredményekből.

A kibertéri biztonság, vagy az akkori terminológiával élve, számítógépes biztonság (*Computer Security*) önálló tudományterületté válása a 1990-es évek közepétől, végétől figyelhető meg. A szakirodalom – például Ross Anderson *Security Engineering* című műve, amelyet leginkább „A biztonság mérnöki alapja" magyar címre lehetne lefordítani – hangsúlyozza, hogy a biztonság nem pusztán technikai, hanem rendszerelméleti probléma. A támadási felületek növekedése, a hálózati topológiák komplexitása és az emberi tényező együttesen alakítják a sebezhetőséget.[6]

A tudományos diskurzusok így a formális verifikáció, a kockázatelemzés és a biztonsági architektúrák tervezése felé mozdultak el.

Már az 1990-es évek elején megjelentek az olyan kutatások, amelyek a kibertéri műveletek katonai, illetve hadviselésben betöltött szerepét vizsgálták. Az egyik első kutatás, illetve a kutatások összefoglalásaként megjelent tanulmány John Arquilla és David Ronfeldt, a RAND kutatóintézet munkatársai nevéhez fűződik. Arquilla és Ronfeldt a *Cyberwar is coming!* (Kiberháború közeledik!) című tanulmányukban először hangsúlyozták, hogy a jövő konfliktusait egyre inkább a hálózati alapú hadviselés és a kibertér fogja dominálni. A kiberháború, vagy ahogy ma egyre inkább hívjuk, kiberhadviselés nemcsak technológiai támadásokat jelent, hanem az információs fölényért folyó küzdelmet is. A decentralizált, rugalmas hálózatok hatékonyabbak a hagyományos hierarchiáknál, így az államok és nem állami szereplők is alkalmazkodnak ehhez az új hadviselési formához.[7]

Az információért és az információs fölényért folytatott – és azóta is tartó – küzdelem egyik elméleti megalapozója Martin Libicki és Jeremy Shapiro amerikai kutatók. *The Changing Role of Information in Warfare* (Az információ hadviselésben játszott változó szerepe) című elemzésükben megállapítják, hogy az információs forradalom alapjaiban alakítja át a hadviselést, hiszen az információ, a kommunikáció és a hálózatok válnak kulcsfontosságúvá a katonai műveletekben. A jövő fegyveres konfliktusaiban az fog előnyre szert tenni, és végső soron nyerni, aki jobban kezeli az információt, és kihasználja a (számítógép)hálózatok nyújtotta előnyöket. Az új fenyegetések

5 Diffie, Hellman 1976. Elérése: https://ee.stanford.edu/~hellman/publications/24.pdf (Letöltve: 2026. 03. 31.)

6 Anderson 2001. Elérés: https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Security_Engineering_A_Guide_to_Building_Dependable_Distributed.pdf. (Letöltve: 2026. 03. 31.)

7 Arquilla, Ronfeldt 1993. Elérés: https://www.rand.org/pubs/reprints/RP223.html (Letöltve: 2026. 03. 31.)

– például az információs támadások és társadalmi befolyásolás – sebezhetővé teszik az államokat, ezért új stratégiák és új védelem filozófia kialakítása szükséges.[8]

Az információs műveletek (illetve az akkori kifejezéssel élve információs hadviselés) egyik legtöbbet olvasott és idézett szerzője Winn Schwartau amerikai számítógépbiztonsági szakértő, aki az *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age* (Információs háború: Kiberterrorizmus: Az egyéni biztonság védelme a digitális korban) című, először 1994-ben[9] megjelent könyvében valóban látnoki módon foglalta össze mindazokat a kihívásokat, amelyek az információtechnológia és a digitalizáció révén ma a mindennapjaink részei.[10]

Nagyon fontos kérdéskört járt körbe a NATO Kooperatív Kiberbiztonsági Kiválósági Központja a *Tallinn Manual* kézikönyv összeállításakor. A tudományos kutatásokra épülő tanulmánycsokor a nemzetközi jog kibertéri alkalmazhatóságát vizsgálta. A kiválósági központ kezdeményezte annak a tanulmánykötetnek a létrehozását is, amely a kiberhadviselés nemzetközi jogi szabályozását elemzi. A *Tallinn Manual* első kiadása 2013-ban jelent meg, fő célja pedig az volt, hogy feltárja a kibertérben alkalmazható nemzetközi jogi és hadijogi kereteket. A kutatás több egyetem és intézet együttműködésével készült, eredményeit két fő részben ismertették. A kötet 7 fejezetben 95 szabályt határozott meg a kibertérben alkalmazható nemzetközi jogi szabályokra.[11] A kibővített Tallinni Kézikönyv, azaz a *Tallinn Manual 2.0*[12] 2016-ban látott napvilágot, és már 154, kiberműveletekre alkalmazható jogi szabályt elemzett. A két kötet megjelenése között eltelt három év is rávilágított arra a problémára, amely az első és a második kötet címében érhető tetten talán a leglátványosabban. Az első kötet címe „A nemzetközi jog alkalmazhatósága a *kiberhadviselésben"*, míg a második kötet címében a hadviselés helyett már *kiberműveletek* szerepel. Ez arra a – nem csak terminológiai – bizonytalanságra is nagyon jó példa, amely azóta is tart a tudományos diskurzusokban és a gyakorlatban is: mikortól beszélhetünk kiberháborúról, és melyek azok az attribútumok, amelyek megkülönböztetik az olyan kiberműveleteket, mint a kibertéri hírszerzés a valódi – már-már a fizikai háborúval egyenértékű – kiberhadviselést jelentő kiberműveletektől?

A 2022 óta folyó orosz–ukrán háború és annak kiberműveleti tapasztalatai szintén tudományos alaposságú elemzést igényelnek, hiszen ez a háború az első olyan teljes skálájú fegyveres konfliktus, amelyben a kiberműveletek szervesen és folyamatosan kiegészítik a kinetikus műveleteket. Az így nyert tapasztalatok, bár alapjaiban nem írják felül a korábbi elméleti várakozásokat, de az ezek alapján megfogalmazható

8 Libicki, Shapiro 1999. Elérés: https://www.rand.org/pubs/monograph_reports/MR1016.html (Letöltve: 2026. 03. 31.)

9 A könyv először 1994-ben jelent meg, de 1996-ban a második kiadása révén lett világszerte elérhető. Schwartau 1996.

10 Schwartau más munkái is nagy hullámokat keltettek. Ilyen munkája például az *Analóg hálózati biztonság: idő, meghibásodások, mérnöki munka, rendszerek, az én audio-pályafutásom és egyéb gondolatok hat évtizednyi elmélkedésről* című 2018-ban megjelent könyve, amely egyik legfontosabb mondanivalója az, hogy nem létezik teljes digitális biztonság, így az analóg értelemben vett biztonsághoz kell visszanyúlnunk Schwartau 2018.

11 Schmitt 2013.

12 Schmitt 2016.

jövőkép, valamint nem utolsó sorban a felvázolható kibertéri eszköz- és eljárásrendszer be kell, hogy épüljön a jövő hadviseléséről való gondolkodásunkba.

Összességében elmondható, hogy a kezdeti kibertéri kutatások 1990-es évek elején történt megjelenése óta eltelt több mint három évtized kibertéri történései a korai véleményeket és az akkoriban még igencsak merész, de mára nagyon is reális és pontos előrejelzéseket nagyon nagy százalékban igazolták. Az elmúlt három évtizedben tudományos kutatások egész sora, több tucatnyi könyv és tudományos cikk született ezekben a témákban.

Információs műveletek és kiberműveletek a hazai tudományos kutatásokban

A kibertérrel, illetve az abban folyó műveletekkel kapcsolatos hazai kutatások – a nyugati kutatások után – már az 1990-es évek közepén-végén megkezdődtek a hazai hadtudományi kutatások keretében. A munka magyarországi úttörői Makkay Imre és Várhegyi István voltak. Az ő általuk jegyzett *Információs korszak, információs háború, biztonságkultúra* című, 2000-ben megjelent könyv volt az első olyan összefoglaló hazai tudományos munka, amely átfogó és komplex módon elemezte a technikai és technológiai fejlődés – különösen az információtechnológiai forradalom hadügyre és társadalomra gyakorolt – közvetett, illetve közvetlen hatását.[13]

Haig Zsolt és Várhegyi István könyve *Hadviselés az információs hadszíntéren* címmel 2005-ben jelent meg.[14] A könyv a hazai modern hadviselés kutatása egyi alapművének számít. A munkában a szerzők azon kívül, hogy bemutatják az információs társadalom alapvetéseit és azt a technikai hátteret, amely a digitalizációval egyetemben magát a társadalmat is formálja, rendszerezik az információs műveletek elméletét, elválasztva egymástól a technikai – például az informatikai-biztonság vagy elektronikai hadviselés – és a kognitív (például a lélektani műveletek vagy megtévesztés) elemeket. A könyv nagyon jól rávilágít arra, hogy az információ már nemcsak támogató eszköz, hanem önálló fegyver és egy önálló műveleti dimenzió is. A szerzők a munkában részletesen elemzik a hálózatközpontú hadviselés alapjait (amely a 2000-es évek elején még abszolút úttörő vállalkozásnak számított), a kritikus infrastruktúrák védelmét, valamint a döntéshozatali folyamatok befolyásolásának stratégiai jelentőségét.

A hazai kutatások az említett könyvön kívül is külön figyelmet szenteltek a kritikus infrastruktúrák, ezen belül is a kritikus információs infrastruktúrák kitettségének és azok lehetséges védelmének. 2009-ben került kidolgozásra, majd egy évvel később látott napvilágot a *Digitális Mohács* című tanulmány. Ez egy forgatókönyvet vázolt fel a hazai kritikus infrastruktúrák támadásra. Megírását a hazai kritikusinfrastruktúra-védelem akkori hiányosságai motiválták. Mivel 2009-ig ezen a területen nem történt érdemi kormányzati előrelépés, ezért a szerzők egy olyan gondolatkísérletet mutattak be, amely a magyarországi fizikai és információs infrastruktúrák elleni szimultán támadások társadalmi, gazdasági és politikai hatásait elemezte.[15] A forgatókönyv rávilágított arra, hogy központi, állami koordináció nélkül az egyes

13 Várhegyi, Makkay 2000.

14 Haig, Várhegyi 2005.

15 Kovács, Krasznay 2010.

üzemeltetők – az ágazati összefonódások és kölcsönös függőségek miatt – képtelenek hatékonyan reagálni az összetett támadásokra, így csupán a tüneteket kezelik a valódi okok helyett.[16]

A kiberműveletek azonban nemcsak technikai, hanem kognitív és társadalmi dimenzióval is rendelkeznek. A 2016. évi amerikai elnökválasztás körüli információs műveletek vizsgálata rámutatott a közösségi média algoritmusainak szerepére a dezinformáció terjedésében. Így az akkori hazai kutatások már a politikatudományi és kommunikációelméleti kérdésekre is kiterjedtek, amelyek az online manipuláció demokratikus intézményekre gyakorolt hatását elemezték.[17]

Ezt követően tovább folytak a kiberműveletek és az információs műveletek hazai kutatásai. Haig Zsolt 2019-ben megjelent *Információs műveletek a kibertérben* című könyve a modern hadviselés technikai és műveleti dimenzióit rendszerezi. A szerző a kiberteret önálló műveleti térként mutatja be, ahol az egyik legfontosabb cél az információs fölény kivívása. A könyv különválasztja a támadó, a védelmi és a támogató jellegű kiberműveleteket, bemutatva azok katonai és nemzetbiztonsági relevanciáját. A munka központi témája a kritikus infrastruktúrák sérülékenysége, a hibrid fenyegetések elleni fellépés, valamint a hálózatközpontú képességek integrálása a hagyományos összfegyvernemi (összhaderőnemi) harcba, elméleti és gyakorlati alapokat adva a védelemhez.[18]

Mindezek mellett számos olyan hazai kutatás is elkezdődött a későbbiekben, amelyek a kibertér és a biztonságpolitika kapcsolatát vizsgálták. Ilyen kutatások történtek például a kiberdiplomácia területén. A kiberdiplomácia a diplomácia egy viszonylag új, de kritikus fontosságú ága, amely a kibertérrel kapcsolatos nemzetközi kapcsolatokat, tárgyalásokat és normákat foglalja magában. Ezen a területen elsősorban nem technikai kérdésekről van szó, hanem arról, hogyan viszonyulnak egymáshoz az államok a digitális térben. A kiberdiplomáciai kutatások azt vizsgálják, hogy a külpolitikai célok elérése miként valósulhat meg a kibertér eszközeivel, illetve a kibertér diplomáciai úton történő szabályozására milyen eszközök alkalmazhatók. Mindezen belül olyan fontos kérdéseket kutattak a hazai szakértők is, mint például a nemzetközi (kiber) normák kialakítása, azaz annak meghatározása, hogy mi számít elfogadható állami magatartásnak a kibertérben; milyen kiberbiztonsági együttműködésekre van szükség az országok között; mit jelent a digitális szuverenitás, vagy az internet-kormányzás; milyen mértékű nemzetközi információmegosztás szükséges a nemzetek között például a nagyszabású kibertámadások és a kiberbűnözés elleni fellépés érdekében. A hazai kiberdiplomácia kutatói között meg kell említeni Molnár Annát és Molnár Dórát, akik szerkesztésében megjelent *Kiberdiplomácia* című könyv remek összefoglalást nyújt a témában.[19]

A hazai kibertéri kutatások elindulásával párhuzamosan már a kezdetekben megjelentek a doktori (PhD) kutatások is, sőt a téma a doktori képzés szerves részét

16 Kovács 2018.

17 Kovács, Krasznay 2017.

18 Haig 2022.

19 Molnár Anna, Molnár Dóra 2022. Elérés: https://webshop.ludovika.hu/wp-content/plugins/olvasoprobak/olvasoproba_1008_Kiberdiplomacia.pdf (Letöltés: 2026. 03. 31.)

képezte a Zrínyi Miklós Nemzetvédelmi Egyetemen, illetve annak jogutódján a Nemzeti Közszolgálati Egyetemen (NKE). Az egyetemen először a két katonai doktori iskolában, a Hadtudományi Doktori Iskolában és a Katonai Műszaki Doktori Iskolában, majd ezt követően már az NKE Közigazgatástudományi Doktori Iskolájában és a Rendészettudományi Doktori Iskolájában is indultak olyan kutatási témák, amelyek a kibertér különböző kérdéseit tudományos igénnyel vizsgálták. A konkrét kiberműveletekkel kapcsolatos kutatások természetesen a két katonai tematikájú doktori iskolában jelentek meg elsősorban, ahol a kiberhadviselés, annak technikai kihívásai, valamint a különböző kiberbiztonsági (elektronikus információbiztonsági) szabályozási kérdések kutatása folyt, és folyik jelenleg is. Ezek mellett az információs műveletek és a hibrid műveletek, illetve az ezekben alkalmazott kiberműveleti megoldások vagy éppen kibervédelmi eljárások kutatása is jelen volt a doktori képzésben. Ezt követően természetesen más hazai egyetemeken is megjelentek a kibertéri kutatások, így például az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában, ahol számos kiberbiztonsági tematikájú kutatási témát hirdetettek meg az elmúlt években.[20]

Szubjektív válogatás a hazai információs műveletekkel és kiberműveletekkel kapcsolatos tudományos munkákból

(Szerk. a Szerző)

Szerző	*Mű címe*	*Megjelenés éve*
Makkay Imre, Várhegyi István	Információs korszak, információs háború, biztonságkultúra	2000
Haig Zsolt, Várhegyi István	Hadviselés az információs hadszíntéren	2005
Kovács László, Krasznay Csaba	Digitális Mohács	2010
Kovács László	A kibertér védelme	2018
Kovács László	Kiberbiztonság és -stratégia	2018
Haig Zsolt	Információs műveletek a kibertérben	2019
Molnár Anna, Molnár Dóra (szerk.)	Kiberdiplomácia	2022
Krasznay Csaba (szerk.)	Taktikák és stratégiák a kiberhadviselésben	2023
Kovács László	Hadviselés a 21. században: kiberműveletek	2023

A fenti, alapvetően elméleti kutatások mellett számos kutatás-fejlesztési és innovációs projekt indult hazánkban is az elmúlt években, amelyeknek mindegyike támaszkodott azokra az elért tudományos eredményekre, amelyek a területen korábban születtek. Ezek egy jó része az innováció és a kettős felhasználású technológiák területén folyt, mert a kiberműveletek és a tudomány kapcsolatát erősen meghatározza a kettős

20 Meg kell jegyezni, hogy nagyon érdekes eredményekre vezető külön kutatást vagy kutatásokat lenne célszerű végezni ezeknek a doktori programoknak, illetve a kutatási témáknak összehasonlító elemzésével.

felhasználási cél, azaz az úgynevezett dual-use technológiák problémája. A mesterséges intelligencia, a gépi tanulás és a nagy adatbázisok elemzése egyszerre szolgálhatja a gazdasági fejlődést, de egyben a támadó – akár civil, akár katonai – műveletek hatékonyságát is. A generatív mesterséges intelligencia modellek alkalmazása például automatizált adathalász-kampányokat tehet lehetővé, miközben legitim kutatási és ipari célokat is szolgál.

A kutatások során az etikai diskurzus egyre hangsúlyosabbá válik. A felelős kutatás és innováció elve arra ösztönzi a tudományos közösséget, hogy mérlegelje azok potenciális katonai alkalmazásait. A nyílt tudomány normái és a nemzetbiztonsági érdekek közötti feszültség különösen érzékeny kérdés a kibertéri kutatásokban.

Összegzés, következtetések

A kiberműveletek és a tudomány kapcsolata kölcsönösen konstitutív. A tudomány biztosítja az elméleti és technológiai alapokat, míg a kiberműveleti gyakorlat új kutatási kérdéseket és normatív dilemmákat generál. Az interdiszciplinaritás, az intézményes együttműködés és az etikai reflexió kulcsfontosságú ezen a területen is a jövőbeli fejlődés szempontjából. A kibertér tudományos vizsgálata nem csupán technológiai kérdés, hanem a globális biztonság, a stabilitás és a társadalmi reziliencia alapvető eleme.

Az 1990-es évek elején megkezdett nemzetközi, valamint az 1990-es évek közepén elindult hazai kibertérrel kapcsolatos kutatások, illetve azok eredményei a 2010-es évekre a gyakorlatban nyertek visszaigazolást. Ma már a kiberműveletek a mindennapi katonai tevékenységek integráns részeit képezik, míg a hibrid műveletek részeként egyre fokozódó – főleg civil célpontok ellen irányuló – kiberműveletek és információs műveletek egész sorát láthatjuk nap, mint nap.

Ugyanakkor a kiberműveletek gyakorlata új empirikus adatforrásokat is teremtett a tudomány számára. Az iráni atomlétesítmények ellen intézett 2010-es úgynevezett Stuxnet támadás esete paradigmaváltást is jelentett egyben, hiszen az a kibertámadás a fizikai infrastruktúrát – konkrétan az említett iráni nukleáris létesítményeket – károsította. A tudományos kutatások tehát már nem csak elméleti síkon mozognak, hanem azok részletesen analizálják, hogy miként vált a kiberfegyver a geopolitikai stratégia eszközévé. A 2010-es évek óta számos tanulmány vizsgálta és vizsgálja az államilag támogatott kibertámadások mintázatait. Az empirikus kutatások kiterjedtek a kritikus infrastruktúrák védelmére is. A villamosenergia-hálózatok, egészségügyi rendszerek és pénzügyi infrastruktúrák sérülékenysége a tudományos érdeklődés középpontjába kerültek.

Mindezek mellett a pszichológia és a viselkedéstudomány szintén fontos szerepet játszik a kibertéri tudományos kutatásokban. A kognitív torzítások, a megerősítési torzítás és a csoportpolarizáció jelenségei hozzájárulnak az információs műveletek sikeréhez. A tudományos kutatások így interdiszciplináris keretben vizsgálják a technológiai infrastruktúra és az emberi viselkedés kölcsönhatását. A technika és a technológia tudományos alapon történő vizsgálata mellett a társadalomtudományi dimenziók és az információs műveletek kapcsolatának kutatása kiemelt fontosságú a jövőben.

FELHASZNÁLT IRODALOM

Anderson, Ross 2001. *Security Engineering. A Guide to Building Dependable Distributed Systems. Wiley.* Elérés: https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Security_Engineering_A_Guide_to_Building_Dependable_Distributed.pdf (Letöltve: 2026. 03. 31.)

Arquilla, John; Ronfeldt, David 1993. *Cyberwar is Coming!* Rand Coorporation. Elérés: https://www.rand.org/pubs/reprints/RP223.html (Letöltés: 2026. 03. 31.)

Diffie, Whitfield; Hellman, E. Martin 1976. New Directions in Cryptography. IEEE Transactions on Information Theory, Vol. IT-22, No. 6. Elérés: https://ee.stanford.edu/~hellman/publications/24.pdf (Letöltve: 2026. 03. 31.)

Haig Zsolt 2022. *Információs műveletek a kibertérben.* Budapest: Ludovika Egyetemi Kiadó.

Haig Zsolt, Várhegyi István 2005. *Hadviselés az információs hadszíntéren.* Budapest: Zrínyi.

Information in Warfare. In: Khalilzad, Zalmay M.; White, P. John: *The Changing Role of Information in Warfare*. Rand Coorporation. Elérés: https://www.rand.org/pubs/monograph_reports/MR1016.html (Letöltve: 2026. 03. 31.)

Kovács László, Krasznay Csaba 2010. Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság*, 3 (1): 44–56.

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

Kovács László; Krasznay Csaba 2017. „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Stratégiai Védelmi Kutatási Elemzések*, 9.

Kovács László, Ványa László 2005. Az Európai Unió polgári célú pilóta nélküli repülőgépeinek kutatás-fejlesztési programja: az UAVNET. *Repüléstudományi Közlemények,*17. Különszám.

Libicki, Martin; Shapiro, Jeremy 1999. Conclusion: The Changing Role of Information in Warfare. In: Khalilzad, Zalmay M.; White, P. John: *The Changing Role of Information in Warfare. Rand Coorporation.* Elérés: https://www.rand.org/pubs/monograph_reports/MR1016.html (Letöltés: 2026. 03. 31.)

Molnár Anna, Molnár Dóra (szerk.) 2022. *Kiberdiplomácia.* Budapest: Ludovika Egyetemi Kiadó. Elérés: https://webshop.ludovika.hu/wp-content/plugins/olvasoprobak/olvasoproba_1008_Kiberdiplomacia.pdf (Letöltés: 2026. 03. 21.)

Schmitt, Michael N. ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press.

Schmitt, Michael N. ed. 2016. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* New York: Cambridge University Press.

Schwartau, Winn 1996. *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age.* Thunder's Mouth Press.

Schwartau, Winn 2018. *Analogue Network Security: Time, Broken Stuff, Engineering, Systems, My Audio Career, and Other Musings on Six Decades of Thinking about It All*. SchwartauHaus.

Shannon, E. Claude 1948. A Mathematical Theory of Communication. *The Bell System Technical Journal,* Vol. 27, 379–423, 623–656. Elérés: https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf (Letöltve: 2026. 03. 31.)

Várhegyi István, Makkay Imre 2000. *Információs korszak, információs háború, biztonságkultúra.* Budapest: Országos Műszaki Információs Központ és Könyvtár.