Csutak Zsolt:

ÚJ IDŐK ÚJ HADVISELÉSE – KOGNITÍV BIZTONSÁG AZ INFORMÁCIÓS ÉS A KIBERHADVISELÉS KORÁBAN

ÖSSZEFOGLALÓ: *A 21. század posztmodern, globalizált és a számítógépes rendszerek uralta korában radikálisan megváltoztak az információszerzés, a kommunikáció, a társas interakció s így a hadviselés viszonyrendszerei is. A politikai és a gazdasági érdekérvényesítés súlypontja áttevődik a kibertérbe, az elektronikus online média hadszíntérré változik, és az információ fegyverré alakul. Állami és nem állami szereplők használják a propagandisztikus online médiabefolyásolás puha erőkifejtő eszközeit, amelyek ellen nagyon nehéz hatékonyan védekezni. A stratégia és a módszer tulajdonképpen évtizedek óta ismert, csupán a kibertechnológiai megoldások és forradalmi változások teszik újszerűvé az információs műveleteket, illetve a hibrid hadviselés megnyilvánulási formáit. Az emberek és a társadalmak kognitív sérülékenysége a puha erőhatások és a hibrid befolyásoló hadműveletek célpontjában új stratégiai elemző megközelítést és alternatív hadviselési, szociálpszichológiai megoldásokat tesz szükségessé.*

KULCSSZAVAK: *kibertér, információs és pszichológiai műveletek, hibrid, információs és elektronikai hadviselés, kognitív biztonság, médiabefolyásolás, puha erőhatás, propaganda*

„A képzelet sokkal fontosabb, mint a tudás." Albert Einstein[1]

BEVEZETÉS

Közhelyszerűnek tűnő, ellenben igaz megállapítás, miszerint a 21. század elején új idők új szele fúj a társadalmi, technológiai és politikai, következésképp a katonai interakciók és viszonyrendszerek területén is. Az újszerű kihívások újszerű stratégiát és megoldási alternatívákat kívánnak, olyan új paradigmát, gondolkodásmódot, amellyel talán még nem is találkoztak sem a döntéshozók, sem digitális világunk hétköznapi polgárai. Posztmodern korunk meghatározó hívószavai lettek és az utóbbi évtized során alapfogalmakká váltak olyan kifejezések, mint *információ, digitális, elektronikai, kiber,* továbbá a velük szoros összefüggésben használt és értelmezett tág fogalmak, mint *társadalom, biztonság,* valamint a számunkra – a dolgozat témájánál fogva – különösen fontos *hadviselés*.

Mindezen változások hátterében fellelhetőek a széles körű globális politikai és technikai átalakulások, trendek, amelyekre reagálni kénytelenek mind a katonai stratégiaalkotók, mind pedig az elhárításban, információszerzésben és -feldolgozásban érintett biztonsági szolgálatok.

A dolgozat témáját, alapkérdéskörét tekintve a korlátozott formai és tartalmi keretek között kísérletet teszek a viszonylag új stílusú és koncepciójú pszichológiai, illetve informá-

[1] https://www.citatum.hu/idezet/15580 (Letöltés időpontja: 2018. 05. 05.)

ciós műveletek főbb karakterjegyeinek bemutatására és jellemzőinek rövid ismertetésére. Továbbá szeretnék rávilágítani a számítógépes rendszerek uralta kibertér és a vele szoros összefüggésben kibontakozó elektronikai, kiber- és információs hadviselés jellemzőire, annak társadalmi, politikai és szociálpszichológiai vonatkozásaira.

A KIBERVILÁG HÁLÓJÁBAN

Az első öbölháború legendás amerikai parancsnoka, Norman Schwarzkopf tábornok elhíresült *bon mot*-ja volt 1991-ből, hogy nyavalyás számítógépekkel nem lehet csatát vívni,[2] ellenben 2018-ban kis túlzással kijelenthetjük, hogy a mai posztmodern korban már nem lehet – vagy csupán nagyon korlátozott módon – számítógépek igénybevétele nélkül komoly és korszerű hadviselést folytatni. Az amerikai tudományos-fantasztikus irodalom világából 1982 óta kölcsönvett *kibertér* fogalom[3] és a rövidesen hozzákapcsolódó *kiberhadviselés* ma már érzékelhető valóság és új alkalmazott hadviselési forma. Ebben a tekintetben viszonylag gyakran találkozhatunk a kiberhadviselés és -háború *(cyber warfare and war)* egyik névadójának, Richard A. Clarke professzor veterán amerikai nemzetbiztonsági elnöki tanácsadó gondolataival, akárcsak neves washingtoni kiberbiztonsági szakértő munkatársai, Robert Knake és Paul Kurtz meghatározó véleményével. Az említett befolyásos tanácsadók, szakértők az ezredforduló körül bekövetkezett forradalmi technikai és egyéb változások nyomán határozottan úgy vélekednek, hogy a 21. század fő konfliktusai – állami és nem állami szereplők között egyaránt – elsősorban az ún. *kibertérben* fognak lezajlani, pontosabban már évek óta zajlanak.[4]

A kibertér fogalmának filozófiai, irodalmi és technikai tartalmakkal is terhelt használata igencsak szerteágazó, különféle kontextusokban megjelenített posztmodern eszme. Ezért a tisztánlátás, illetve a fogalmi zűrzavar elkerülése érdekében a dolgozatban az amerikai és más mérvadó NATO-tagállamok haderőiben alkalmazott – és a Magyar Honvédségben is elterjedt – szóhasználatot és kontextust tartom követendőnek. Tehát ebben a vonatkozásban elsősorban fizikai, elektronikai jellemzőkkel bíró mesterséges környezetről, továbbá katonai és polgári számítógépes alkalmazások és rendszerek elleni támadások előkészítéséről, kivitelezéséről vagy ezek elhárításáról beszélhetünk.

Ugyancsak említésre méltó tény, hogy a fizikai, mérhető és érzékelhető hálózati környezeten, kibertéren túl létezik egy kvázi megfoghatatlan, virtuális másodlagos tér, avagy környezet is, ahol a kibervilág rejtőzködő, többes identitású szereplői tevékenykednek. Ha az összekapcsolódott számítógépes hálózatok, alkalmazások és mindennemű okoseszközök rendszerét egy nagy globális komplex egységnek tekintjük, nevezetesen a *dolgok internetének (Internet of Things)* a 21. századi világban, akkor egy igazán megdöbbentő és szinte felfoghatatlan méretű és bonyolultságú másodlagos valósághoz jutunk. Ez a kibervilág – illetve mondhatnánk, mesterséges hibrid, fizikai és ugyanakkor virtuálisan létező univerzum – napjainkban közel 30 milliárd eszközt és felhasználót számlál, és exponenciálisan

[2] Richard A. Clarke – Robert Knake: Cyber War: *The Next Threat to National Security and What to do about it*. Harper & Collins, e-könyv, 2010, 12.

[3] Gibson 1982-ben megjelent Burning Chrome c. novellájában utal a kibertérre (cyber space) mint metaforára, habár a sci-fi brit nagymestere, Arthur C. Clarke 1956-os, a Város és a Csillagok című regényében már használt teljesen hasonló leírást, de nem ezzel a kifejezéssel, hanem „virtuális mátrix", illetve a „virtuális valóság" használatával. http://www.technovelgy.com/ct/content.asp?Bnum53 (Letöltés időpontja: 2018. 04. 25.)

[4] Clarke–Knake: i. m. 13–18.

bővülő tendenciát mutat, amelyet ugyanakkor korunkra tipikusan jellemző posztmodern és aszimmetrikus módon csak a világ lakosságának fele ér el és használhat.[5]

A katonai hadszínterek hagyományos hármas földrajzi tipológiáján, kiterjesztésén túl a fenti jelenségek megjelenésével létrejött egy újabb, nem konvencionális, atipikus hadszíntértípus, amely leginkább a *kiberdimenzió* szóval írható le.

Az amerikai és a NATO katonai terminológiában a számítástechnikából átvett és átlényegített kibertér, kibertartomány *(cyber domain)*, illetve információs környezet *(information environment)* is gyakran előforduló fogalom, amely elsősorban mint a klasszikus négy fő hadműveleti tartomány *(operational domain)*, azaz a szárazföldi, légi, tengeri és űr műveleti tartományok mellett megjelenő kiber-, illetve információs – és pszichológiai – tartományra történő utalásként használatos a szakirodalomban.[6] Az amerikai Védelmi Minisztérium (Pentagon) Kiberhadviselési Parancsnoksága *(CYBERCOM)* által 2010-ben összeállított korszerű hadműveleti fogalomtár meghatározása szerint a kibertér egy összetett, vélt, illetve empirikus valóságot lefedő fogalom, hiszen megkülönböztethető a virtuális, névleges *(notional)* entitás a fizikai hálózati, a logikai hálózati és a rejtőzködő, nehezen beazonosítható virtuális kiberszemélyiségek *(cyber-persona)* hálózata mellett.[7]

A kibertér hadtudományi vonatkozású megfogalmazására és tudományos igényű leírására a magyar szakirodalomban elsősorban a Haig Zsolt és Kovács László által használt definíciót és leírást érdemes megjegyezni, amely amerikai mintára szintén az elektronikus hálózati rendszerű adatszerzésre és különösképp támogató műveletekre, továbbá az információs, illetve kiberhadszíntéren történő katonai és biztonsági jellegű műveletek összességére utal.[8]

Az amerikai terminológiában, elsősorban a RAND[9] agytröszt kutatóinak megfogalmazásában az *információs hadviselés (information warfare)* definíciója közérthetően minimalista, miszerint minden konfliktus, amely az információs, illetve digitális információs kibertérben zajlik két vagy több szemben álló fél között, az az információs hadviselés fogalmába és műfajába tartozik.[10] Az elektronikai és az információs hadviselés[11] sok tekintetben átfedést mutat, habár katonai doktrína szintjén például az amerikai haderő az utóbbit még nem nevesítette, csak alkalmazza. Kétségtelen, hogy napjaink digitalizált világában az információs tér a világ lakossága több mint felének egyben elektronikusan hozzáférhető, digitális adatot vagy információs teret, dimenziót jelent, amelyben élen járnak például a digitális médiafelületek, a közösségi hálózatok vagy akár a tömeges online szerepjátékok (MOBA RPG[12]) is.

---

[5] A Statista globális statisztika portál szerint 2017-ben a világ lakosságának csak kb. 51%-a rendelkezett internet-hozzáféréssel. https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/ (Letöltés időpontja: 2018. 05. 10.)

[6] Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány, 2018/1. szám, 116. http://real.mtak.hu/77921/1/HT20181_115_133_u.pdf (Letöltés időpontja: 2018. 07. 28.)

[7] Uo. 117.

[8] Haig Zsolt – Kovács László: Fenyegetések a cybertérből. Nemzet és Biztonság, 2008/5. szám, 61–69. http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf (Letöltés időpontja: 2018. 07. 28.)

[9] Research ANd Development – kutatás és fejlesztés.

[10] Isaac R. Porche III. et al.: Redefining information warfare boundaries for an army in a wireless world. RAND Corp. – Arroyo Center, 2013, XV. https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf (Letöltés időpontja: 2018. 06. 10.)

[11] Uo. XVI.

[12] Massive Online Battle Arena Role Play Games, vagyis tömeges harctéri szerepjátékok, amelyeket szimultán online akár több tízmillióan is játszanak világszerte belső titkosított kommunikációs csatornával, mint pl. World of Warcraft, League of Legends, World of Tanks, Hunger Games stb.

A hazai és az amerikai szakértők elgondolása szerint az információs műveletek és a kiberhadviselés formái tulajdonképpen a tágabb kontextusú és tartalmú *elektronikai hadviselés (electronic warfare)* keretében nyilvánulnak meg. Napjaink technikai és hálózatalapú társadalmainak kitettsége és függősége az elektronikai rendszerek, hálózatok világától polgári és katonai vonatkozásban egyaránt egyre nagyobb jelentőséggel és befolyással bír a politikai döntés-előkészítési és a stratégiai, hadműveleti folyamatok tervezésekor. A különféle elektronikai technológiát alkalmazó megnyilvánulási formái egymást kiegészítő, erősítő eszközök lehetnek katonai és polgári célpontok elleni támadások végrehajtásában, amire minden állami és nem állami szervnek vagy akár multinacionális szervezetnek fel kell készülnie napjaink információs, digitális társadalmában.[13]

Az említett kibervonatkozású katonai és biztonságpolitikai kihívások és lehetőségek mellett fontos fogalom és tartalmilag releváns tényező a dolgozat címében is szereplő *kognitív biztonság* és *információs tér*, *környezet*, illetve *hadszíntér*. Ez utóbbi kifejezés első hallásra talán túlzó eufemizmusnak tűnhet, különösen a laikus nagyközönség számára, ellenben Rand Waltzman professzornak, a neves RAND Corporation világhíres kutatójának és a Pentagon Fejlett Védelmi Kutatási Projektek Ügynöksége (*DARPA*[14]) egykori projektvezetőjének határozott véleménye szerint e két fogalompár nagyon jellemző vonása és meghatározó tényezője napjaink társadalmi, védelmi és biztonsági környezetének. Waltzman professzornak az amerikai Szenátus Védelmi és Kiberbiztonsági Albizottsága általi meghallgatásán tett 2017. április 27-i tanúvallomása[15] globális hatásúnak bizonyult nemcsak a biztonság- és védelempolitikai szakma, hanem a kibervilág hétköznapi szereplői számára is. Dr. Waltzman – aki 2018 májusában két nagy sikerű előadást is tartott budapesti egyetemeken – nyilvános kongresszusi beszámolójában ugyanis nem állított mást, mint hogy az internethasználók és különösképpen a közösségi hálózatok ügyfelei folyamatos információs támadás és kártékony külső befolyásolás alatt állnak vagy állhatnak. A *Facebook* és a *Cambridge Analytica* IT-cégek illegális adathasználatai és a 2016-os amerikai elnökválasztás orosz befolyásolási botrányai révén az ilyen információs és pszichológiai jellegű befolyásoló tevékenység újra a hírek és a figyelem középpontjába került – a 2007-es észtországi[16] kibertámadás, illetve a 2008-as grúziai háborús események izgalmai[17] után.

Érzékelhető módon megjelent egy újabb burkolt hadviselési forma, a Waltzman által csak *információs fegyverkezésnek* is nevezhető *(the weaponization of information)*[18] jelen-

[13] Haig Zsolt: Az információs társadalmat fenyegető információalapú veszélyforrások. Hadtudomány, XVII. évf. 2007/3. szám, 50–55. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2201/hadtud_2007_3_haig.pdf?sequence=1&isAllowed=y (Letöltés időpontja: 2018. 07. 28.)

[14] Defense Advanced Research Projects Agency.

[15] Rand Waltzman: The Weaponization of Information – the need for cognitive security. RAND Corp., 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf (Letöltés időpontja: 2018. 05. 10.)

[16] Az első webháború (Web War I) néven is emlegetett összehangolt, többnapos DDOS jellegű kibertámadás sorozat az észt állami és üzleti infrastruktúrák, szolgáltatók ellen a 2007. április 26-i „bronzkatona éjszakája" után. A kevés visszakövethető forrás moszkvai szerverekhez vezetett. http://infowar.cepa.org/Briefs/Est/10-years-after-Web-War-I-in-Estonia (Letöltés időpontja: 2018. 05. 10.)

[17] 2008 augusztusában a dél-oszét–grúz (georgiai) fegyveres konfliktus okán az orosz hadsereg támadást indított a grúz hadsereg egységei ellen, és a megelőző kibertámadásban részlegesen, illetve teljesen ellehetetlenítette az ország katonai és polgári irányítására szolgáló kritikus infrastruktúra üzemeltetését. Daniel Hollis: Cyberwar case study: Georgia 2008. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (Letöltés időpontja: 2018. 05. 09.)

[18] Waltzman: i. m. 1.

ség, amelyet a fent említett műveleti opciók és az elektronikai hadszínterek sajátosságai hívtak életre az utóbbi évtizedek során. Az aszimmetrikus és a kiberhadviselés könnyen megjegyezhető szabályai érvényesülnek ezen a sajátos hadszíntéren is: tudniillik nincsenek kinyilvánított hadviselő felek egy elismert hadszíntéren, ahogy hadüzenet és uniformis viselete sem jellemző a harcban részt vevő felekre. Ez utóbbiak nagyon változatos skálája és széles körű penetrációja jelenti az egyik legnagyobb biztonsági kihívást és problémahalmazt. Waltzman és számos más szakértő megállapítása szerint manapság az előrehaladott technikai lehetőségek révén a kiberhadviselésben az „információs, pszichológiai műveleteket is alkalmazó szereplők (hadviselő felek) száma és jellege teljesen demokratizálódott".[19] Megtalálhatóak közöttük a különösképpen nagy és befolyásos állami szereplők (gondoljunk csak elsősorban olyan államokra, mint az Amerikai Egyesült Államok, Oroszország, Kína, Észak-Korea, Irán, Izrael), de akár tehetséges és globális befolyással bíró magánszemélyek (pl. Ed Snowden, George Soros, Mark Zuckerberg és sokan mások), valamint természetesen terrorszervezetek (ISIS, al-Kaida) is.[20]

A hadtudomány legújabb hadviselés-tipológiája szerint a 4.,[21] illetve akár a 21. századi 5. generációs hadviseléshez is sorolható kiber- vagy információs hadviselési műveletek módszerei és célpontjai nagyon változatosak lehetnek. Számos katonai gondolkodó és hadtudós meglátása szerint a jövő konfliktusai és háborúi a levegő és az információs, illetve kiberhadszíntereken fognak elsősorban lezajlani és eldőlni. Ezen a véleményen van Peter Layton professzor is, az ausztrál légierő tartalékos századosa és az amerikai védelmi akadémia, a tekintélyes Eisenhower College oktatója, valamint az *5. generációs,* hálózatalapú – *elsősorban légi – hadviselés* egyik fő propagálója.[22] Layton százados szerint érdemes a nagy NATO-rivális hatalmi erőterekre is figyelni, tudniillik a kínaiak és az oroszok is felismerték ezt az új trendet, hiszen nyilatkozataik, döntéseik, katonai gondolkodásuk stratégiai irányvonalai mind ebbe az irányba mutatnak.[23]

Ezekhez a katonai fogalmi rendszerekhez kapcsolható a manapság sokszor hivatkozott *hibrid hadviselés* típusa is, amely hatékonyan ötvözi az aszimmetrikus, az irreguláris, az információs és a kiber jellegű műveletek jellemző tulajdonságait. A fősodorbeli globális hírügynökségek meghatározó tevékenysége, illetve az újabb hidegháborúnak is címkézett amerikai–orosz szembenállás révén a 2013-ban megjelent, és a nyugati szakírók által némi túlzással csak *Geraszimov-doktrínaként*[24] is köztudatba került újszerű orosz hadviselési stratégia mondhatni slágertémává tette a hibrid és az információs műveletek fontosságát.

Ez azonban természetesen nem kizárólag orosz sajátosság, hiszen ezeket a módszereket, művelettípusokat hasonlóképpen már hatékonyan alkalmazták az amerikai erők a második öbölháború idején 2003-ban, a libanoni Hezbollah gerilla-terrorista propagandistái 2006-ban

[19] Uo. 3.

[20] Uo. 2.

[21] Resperger István – Kis Álmos Péter – Somkuti Bálint: Aszimmetrikus hadviselés a modern korban. Zrínyi Kiadó, Budapest, 2015, 60–65.

[22] Peter Layton: Working Paper on Fifth Generation Air Warfare. 2017. http://airpower.airforce.gov.au/APDC/media/PDF-Files/Working%20Papers/WP43-Fifth-Generation-Air-Warfare.pdf (Letöltés időpontja: 2018. 05. 10.)

[23] Waltzman: i. m. 3–5.

[24] Valerij Geraszimov tábornok orosz vezérkari főnök rövid (12 oldalas), ámde annál hatásosabb tanulmánya a nemlineáris, hibrid hadviselés fontosságáról. A 2013. 02. 27-én kiadott orosz nyelvű szöveg Az előrelátás értéke a tudományban címmel: https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf (Letöltés időpontja: 2018. 05. 10.)

az Izrael elleni háborúban, valamint az iraki „Mahdi Hadserege" műveleti főnökei is a bagdadi peremkerületek harcai során az amerikai különleges erők ellen. Ez utóbbi emlékezetes és példaértékű esetnek bizonyult, különösképpen az amerikai fegyveres erők döntéshozói és a kiber-, illetve információs hadviselés tervezői, elemzői számára. Nagyon kis ráfordítással óriási médiahatást és pszichológiai, kommunikációs és egyben katonai ellenreakciót váltott ki a „Mahdi Hadserege" 2007. márciusi újszerű akciója az amerikai különleges erők megtévesztésével a hatásos elterelő információs műveletének eredményeként.[25] Erre az esetre is vonatkoztathatnánk Mark Twain sokat idézett, klasszikussá vált bölcsességét, amely a mai posztmodern korban aktuálisabb és mélyrehatóbb, mint valaha: „Egy hazugság már rég körbejárta a világot, miközben az igazság még csak a cipőjét húzza."[26]

A fenti regionális katonai konfliktusok politikai fontossága és médiahatása hosszú távon természetesen eltörpült a 2014-ben kezdődött – és a sokat emlegetett Geraszimov-doktrína gyakorlati mesterműveként is értelmezhető – ukrajnai események európai biztonságpolitikai jelentősége és kihatása mellett. Ez az eseménysorozat az orosz hibrid hadviselés és az azonosítatlan „udvarias zöld emberek" – az orosz különleges fegyveres erők tagjai – jelenségének reneszánszát eredményezte.

Mindazonáltal a posztmodern hadviselés kategóriájába sorolható kiber-, információs és hibrid hadviselés különféle megnyilvánulási formáiban a stratégiai és a taktikai célok többnyire leszűkíthetőek a következő kategóriákra:[27] biztonsági zavarkeltés, álhír- és tévhitterjesztés, propaganda; technikai és szociálpszichológiai jellegű terepfelmérés; társadalmi káosz és pánikkeltés; gazdasági, katonai, következésképp politikai előnyszerzés. E műveletsorozat, illetve folyamat végén a végső harcba lendülés jele a gerinchálózatok és az életfontosságú szolgáltatások leállítása, illetve irányításának megszerzése a harcoló egységek, a kinetikus[28] katonai erők bevetése előtt. Ugyanakkor még ilyen megváltozott körülmények, hadászati és hadviselési feltételek mellett is érvényesnek tűnik a háború célját leíró klasszikus clausewitzi értelmezés, miszerint az ellenséges akaratérvényesítés/befolyásolás bonyolult folyamatát látjuk kiteljesedni még a kibertérben is, csupán teljesen új kifinomult technológiák és felettébb heterogén szemben álló felek révén.

KOGNITÍV SÉRÜLÉKENYSÉG ÉS HADMŰVELET A KIBERTÉRBEN

Számos kiberbiztonsági szakértő és a nagy globális holisztikus folyamatokat is érzékenyen megfigyelő gondolkodó megállapításai szerint az emberiség által alkotott legkomplexebb és leggyorsabban fejlődő tudásbázis és hálózati rendszer, vagyis az internet és a rajta futó programok, alkalmazások összessége már nem az, aminek eredetileg kitalálták. Ezzel a lehangoló ténymegállapítással egyetért és a drámai társadalmi és technikai átalakulási folyamatokat is egyaránt elismeri az internetes kiberhálózat atyja, illetve a legnépszerűbb netes kezelőprogram, a világháló *(world wide web)* létrehozója, nevezetesen Vinton Cerf és Sir Tim Berners-Lee. Véleményük szerint ők sokáig megvalósulni látták nagy álmukat, hogy létrejöhet a gondolatok és a tudásmegosztás világméretű, szabad, semleges és korlátlan

[25] Waltzman: i. m. 5.

[26] https://kelgyo.blog.hu/2017/12/18/mark_twain_idezetek (Letöltés időpontja: 2018. 07. 28.)

[27] Roger C. Molander – Andrew Riddile – Peter A. Wilson: Strategic Information Warfare: The New Face of War. RAND Corp., 1995, 18–20. www.rand.org/pubs/monograph_reports/MR661.html (Letöltés időpontja: 2018. 05. 02.)

[28] Valódi fizikai katonai erő bevetése az amerikai szakzsargonban (kinetic military force).

fóruma: az internet világa. Ám a 21. század elején bekövetkezett radikális webes átalakulások, a közösségi hálózatok mindent elsöprő ereje, a hamis hírek, áltudományos sarlatánságok és a multifunkcionális propaganda özöne – nem beszélve az általunk is gyakran említett és vizsgált kiberhadseregek, kiberbűnözés, fizetett médiatrollok és zsarolóvírusok elterjedéséről – csúnyán szétzúzták az alapító atyák jóhiszemű, idealista elképeléseit.[29]

A kibertér fokozódó militarizálódása és az információs fegyverkezés mellett érdemes szót ejtenünk az ezekkel a folyamatokkal párhuzamba állítható globális szociálpszichológiai jelenségekkel (kognitív kitettség, sérülékenység, fenyegetettség és disszonancia, illetve információs buborék) az ál- és hamis hírek gyártása korában. Ezekről a jelenségekről nyugodtan kijelenthetjük, hogy a hibrid és az új generációs információs hadviselés puha *(soft)* fegyver formái, amelyet számos „szemben álló harcoló fél" alkalmaz, legyen az állami vagy nem állami, akár globális hatású multinacionális üzleti szereplő is.

A sokat említett Waltzman professzor, a RAND Corporation és DARPA kutatója szerint a kognitív sérülékenység napjaink multimédiás, képközpontú kibervilágának fő és egyedi sajátossága.[30] Az emberiség történelmében előzmények nélküli egyedüli módján manapság felfoghatatlan mennyiségű és értelmezhetetlenül sokszínű, ugyanakkor mégis homogén jegyeket hordozó felületes és torzított információdömping zúdul az emberekre, amelyekre sajnálatos módon nincsenek felkészülve sem intellektuálisan, pszichológiailag, sem politikai vagy biztonsági szempontból. A Waltzman professzor által elterjesztett *kognitív sérülékenység, kitettség (cognitive vulnerability and exposure)* is erre a folyamatra, jelenségcsoportra utal, kiegészítve a szintén általa meghonosított másik fontos fogalommal, amely a webalapú multimédiás technológiák és a híranyaggyártás demokratizálódására *(democratization of online and news-making technologies)* fókuszál – annak számos pozitív és még több negatív következményével. Manapság tulajdonképpen szinte bárki képes minimális digitális készséggel és alapismeretekkel jó minőségű, hihető és reálisnak tűnő hang- és videóhíranyagot szerkeszteni és azonnal közzétenni, terjeszteni a világhálón. Erre számtalan példa van az utóbbi évtizedekből, mint a puha erő *(soft power)* alkalmazása az iraki, afgán és egyéb felkelőkkel, illetve terrorista csoportok ellen vívott aszimmetrikus összecsapások során.

A többnyire tájékozatlan és felületes, azonnal véleményt alkotó polgárok és társadalmi, politikai, gazdasági csoportosulások annak a híranyagnak hisznek, amelyik elsősorban érzelmileg hat rájuk és közelebb áll a *kognitív disszonancia*[31] által befolyásolt világnézetükhöz. Ez a nagyon leegyszerűsített és hihető képvilágú, ellenben hamis vagy torzított valóságtartalmú propagandisztikus médiabefolyásolás csak a technikáját és a gyors, globális tömeghatását tekintve újszerű jelenség. Módszerét és filozófiáját tekintve azonban egyáltalán nem új keletű médiahatalomról és -befolyásolásról beszélünk, elég, ha csak a 20. század legnagyobb hatású amerikai újságírójának – Walter Lippmann – munkásságára gondolunk. Az amerikai szocialista párt egyik alapító ideológusa és Wilson elnök szövegírója, főtanácsadója az 1922-ben, illetve 1925-ben megjelent *Public Opinion* (Közvélemény) és *The Phantom Public* (A nyilvánosság fantomja) címet viselő két fő művében befolyásos baloldali újságíróként

[29] Tim Berners-Lee: The system is failing. The Guardian, 2017. 11. 15. https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality (Letöltés időpontja: 2018. 01. 15.)

[30] Waltzman: i. m. 3.

[31] Szociálpszichológiai tudati, érzelmi feszültségi állapot, amelyre jellemző, hogy önmagunk véleményével, meggyőződésével egyetértő és azt megerősítő módon viselkedünk, paradox módon akár az ennek ellentmondó, zavaró tények ellenében is kitartva álláspontunk mellett. https://www.mimi.hu/pszichologia/kognitiv_disszonancia.html (Letöltés időpontja: 2018. 05. 15.)

és demokrata politikusként – igencsak paradox, elitista módon – megkérdőjelezi a modern tömegtársadalmak megbízhatóságát, a tömegember képességét tárgyilagos, észszerű értékítélet meghozására. Sarkalatos és hatalmas vitákat gerjesztő véleménye szerint – amelyet a későbbiekben a náci, fasiszta és a kommunista diktatúrák propagandistái is nagyon jól ismertek és alkalmaztak – az érzelemvezérelt, ösztönös és sekélyes tájékozottságú, mélyreható médiabefolyásolás hatása alatt álló személyek, vagyis tömegemberek nem képesek elfogulatlan, önálló véleményalkotásra és ítélkezésre országos vagy különösképpen globális vonatkozású témákban.[32] Waltzman professzor hasonló felismerése szerint a Lippmann által leírtak alapján a média által kreált *pszeudo-* vagy *álvalóság*, hamis áligazságok, alternatív tények *(post-truth, alterantive facts)* és összeesküvés-elméletek *(konteók)* uralta álkörnyezet *(pseudo media environment of con-theos)* igencsak kísérteties módon hasonlít napjaink virtuális, túlmediatizált másodlagos valóságára.[33]

Kijelenthetjük, hogy az újabban sokat emlegetett *befolyásoló,* illetve *pszichológiai* műveletek (*PSYOPS*[34]) a 21. századi médiavezérelt posztmodern társadalmainkban egyfajta technikai erőkifejtésként, érdekérvényesítő eszközrendszerként jelennek meg az állami és a nem állami szereplők fegyvertárában. Természetes – és sajnálatos módon – a pszichológiai befolyásolás politikai, katonai és félkatonai alkalmazására számos tragikus példa létezik a történelemben, amikor közvetett vagy közvetlen módon ártó, gonosz szándékból egy pusztító fegyveres konfliktust megelőzőleg – vagy akár háborút kirobbantó tömeges érzelmi túlfűtöttség elérése érdekében – alkalmaztak országos szinten pszichológiai befolyásolási műveleteket. Ez történt például a délszláv háború idején vagy a ruandai népirtás előidézésekor az 1990-es években. A teljesen vagy csak részben hamis hírek, alternatív valóságtartalmak propagandisztikus terjesztése, a háttérhatalmak uralta világ *konteóinak* sejtelmes sugallata nemcsak a globális médiakonglomerátumok, hanem a politikai és a katonai vezetők eszköztárában is előkelő helyet foglal el akár a saját lakosság, de természetesen legfőképp az ellenséges ország polgárainak pszichológiai, mentális gyengítése, összezavarása érdekében.[35]

A propaganda, a meggyőzés és a befolyásszerzés évtizedek óta az orosz (szovjet) és a kínai politika és hadviselés szerves része, következésképp Szergej Sojgu orosz védelmi miniszter ez irányú, 2017. februári nyilatkozata az orosz információs hadsereg felállításának fontosságáról leplezetlen nyíltsággal erősíti ezt a trendet.[36] A nyíltan felvállalt és nem túl kifinomult, ellenben annál hatékonyabb orosz média és az információs hadviselési formák mellett szükséges megemlíteni a nagyságrendekkel nagyobb és hatékonyabb kínai állami információs műveleteket, a kiberhadviselési egységeket és a befolyásolási gyakorlatot, amelyet akár több millió fizetett, illetve önkéntes hazafi végez politikai és hadászati előnyszerzési célokból. A közismert és híres/hírhedt kínai „50 centes párt" fizetett, illetve párthűség alapján önkéntes online médiaszűrői és kommentelő trolljai, egyes vizsgálatok szerint kb. 450 millió közösségi médiaoldalt és hírfolyamot befolyásoltak vagy tettek tönkre a legna-

[32] Walter Lippmann: A külvilág az elménkben. In: Angelusz Róbert – Tardos Róbert – Terestyéni Tamás (szerk.): Média – nyilvánosság – közvélemény. Gondolat Kiadó, Budapest, 2007.
[33] Waltzman: i. m. 3.
[34] Psychological Operations.
[35] Lásd Krekó Péter szociológus idevágó doktori kutatásaiból született könyvét: Tömegparanoia, az összeesküvés-elméletek és álhírek szociálpszichológiája. Athenaeum, Budapest, 2018, 210–220.
[36] Waltzman: i. m. 3–4.

gyobb kínai, amerikai és ázsiai webportálokon.[37] A Waltzman professzor által kidolgozott és szorgalmazott ún. *kognitív biztonság*[38] *(cognitive security)* fogalma és rendszere erre a jelenségre próbál hatékony választ, stratégiai ellenlépést nyújtani az érintett kormányok és szervezetek, valamint a tudatosabb, kritikusabb internethasználó polgárok számára.

A fenti releváns orosz és kínai példákon túl az amerikai intézkedések és technológiák jelentős lépéselőnyben vannak, hiszen szinte minden jelentős, az online, kibervilághoz kapcsolható szellemi termék, technikai megoldás, alkalmazás amerikai eredetű vagy az Amerikai Egyesült Államokban látott először napvilágot.

A 19. század közepén az amerikai elnöki hivatal – James Polk, majd Zachary Taylor elnökök idején – katonai információkat kezelő parányi titkársága már az 1847-es mexikói háborúban is hasonló jellegű felderítő, elemző, hírszerző, dezinformáló tevékenységtípusokat alkalmazott az expanziós háborús sikerek érdekében.[39] Ugyanakkor mintegy másfél évszázadnak kellett eltelnie, hogy a Pentagon Bill Clinton elnöksége idején, 1999-ben intézményesítse a különféle védelmi és biztonsági információkat kezelő ügynökségek munkáját, és azokat információs műveletek néven és struktúrában egységesítse.[40] Ezt megelőzően már 1996 januárjában a befolyásos RAND Corporation agytröszt javaslatára létrehozták az Információs Műveletek Irodáját *(Information Operations Office)* a Pentagonban, különösképpen az elektronikai hadviselés *(electronic warfare)*[41] keretein belül, elsősorban a számítástechnikai és az egyre növekvő fontosságú digitális információs térbe, online környezetbe történő hangsúlyeltolódás miatt. A RAND Corp. szakértői 1994–96 között készült elemzésükben elsősorban politikai és nemzetbiztonsági, másrészt katonai stratégiai fontosságú témának értékelték az információs műveleteket a hidegháborút követő időszakban.[42]

A világháló megállíthatatlan bővülésével, a kibertér fontosságának növekedésével, valamint az ott sokasodó események potenciális hadszíntérszerű kibontakozása révén[43] először az amerikai légierő hozta létre saját kiberhadműveleti központját 2007-ben. Ezt rövidesen követte az amerikai összhaderőnemi kiberparancsnokság *(CYBERCOM)*, valamint a globális fontosságú NATO Kibervédelmi Kiválósági Központ (*CCDCOE*[44]) felállítása is 2008-ban. Ez utóbbi szimbolikus módon nem máshol, mint a számos kibertámadást átélt észt fővárosban, Tallinnban kapott helyet. 2018-ban itt rendezik a világ legnagyobb nemzetközi kiberbiztonsági interdiszciplináris konferenciáját a NATO kiberközpont 10 éves és az internet használatának 50 éves évfordulója előtt tisztelegve.[45] Ez a nagyszabású és különösképpen fontos esemény a nemzetközi kiberbiztonsági tapasztalatcsere egyik fóruma, hiszen a posztmodern, hibrid

[37] Henry Farrell: The Chinese government fakes nearly 450 million social media comments a year. This is why. The Washington Post, 2016. 05. 19. https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/?noredirect=on&utm_term=.bc3e3e8f7890 (Letöltés időpontja: 2018. 05. 15.)

[38] Waltzman: i. m. 7–8.

[39] U.S. Army War College: Information Operations Primer: Fundamentals of Information Operations. Carlisle, PA, 2006, 2–8. http://www.csl.army.mil/usacsl/publications/IO-Primer-AY07.pdf (Letöltés időpontja: 2018. 05. 16.)

[40] Uo. 10.

[41] C2W (Command and Control Warfare), illetve EW (Electronic Warfare – az ellenséges erők vezetési és irányítási, illetve elektronikai rendszerei ellen irányuló hadviselés. Molander–Riddile–Wilson (1995): i. m. 26.

[42] Uo. 4–6.

[43] Roger C. Molander – Andrew Riddile – Peter A. Wilson: Strategic War… in Cyberspace. RAND Corp., 1996. https://www.rand.org/pubs/research_briefs/RB7106.html (Letöltés időpontja: 2018. 05. 02.)

[44] Cooperative Cyber Defence Centre of Excellence.

[45] NATO Kibervédelmi Kíválósági Központja. https://www.ccdcoe.org/ (Letöltés időpontja: 2018. 05. 18.)

hadviselés fő hadszíntere a globális határok feletti kibertérben zajlik. Abban a furcsa közegben, amelyről Norton Schwartz tábornok, az amerikai légierő első kiberparancsnoka találóan megjegyezte, hogy „még egy egyszerű áramszünet sem lehet többé csak sima áramszünet, hanem akár egy összehangolt kibertámadás részének is tekinthető”.[46]

KONKLÚZIÓ

Közel egy évszázad távlatából a globális média és a közösségi oldalak hírfolyamának korában Walter Lippmann szavait aposztrofálva újra kijelenthetjük, hogy az emberek azt hiszik el, amit a média és a politikusok el akarnak hitetni velük.[47] A puha erő és a propagandisztikus befolyásolás alkalmazása annak szubtilis, burkolt jellege és nehezen felderíthető volta révén népszerű és hatékony módja egy célcsoport – ellenséges vagy akár saját ország, társadalom – dezinformálására, szétzilálására és pszichológiai, mentális, politikai, következésképp fegyveres ellenállásának felbomlasztására még a hagyományos fegyveres erők bevetése előtt vagy akár azok helyett. A média mint sokszor emlegetett hatalmi tényező évtizedek óta hatékonyan műveli a katonai terminológiában információs és pszichológiai műveletek néven ismertté vált tevékenységi formákat a mindenkori politikum elvárásai, illetve saját érdekei mentén.

Amint szembesülhettünk a RAND Corporation kutatói és különösképpen Waltzman professzor megállapításaival, napjainkban az információ – legyen az valós vagy valótlan tartalmú – fegyverré vált egy globális, virtuálisan mediatizált hadszíntéren, amelynek hatása alól valójában csak akkor lehetne mentesülni, ha valaki kilépne az élet szinte minden területét átható technikai civilizációból. Nyilvánvalóan egy ilyen lépésnek végzetes következményei lennének arra a személyre vagy csoportra nézve napjaink egymásra utalt, kölcsönösen kiszolgáltatott globalizált világkereskedelmi rendszerében. Ez az állapot és befolyásolási trend nem elhanyagolható kihívást jelent a politikai döntéshozók és a katonai, illetve a biztonsági szolgálatok tagjai számára, hiszen a burkolt, puha erőkivetítéssel, az információs, pszichológiai és kiberhadviseléssel szemben nem igazán létezik bevált forgatókönyv, hatékony ellenlépés vagy hierarchikus és agilis eljárásrendszer.

Mindezek ismeretében komoly kihívást jelent a döntéshozók és a társadalom meghatározó szellemi vezetői számára, hogy felkészítsék a polgárokat és a biztonsági, illetve fegyveres erők tagjait az ellenséges médiabefolyás, propaganda, álhírterjesztés felismerésére és semlegesítésére, továbbá az új típusú, technológiaalapú kiber- és hibrid hadviselés fő jegyeinek felismerésére. Ez emberfeletti, mondhatni sziszifuszi feladat össztársadalmi szinten, amit napjaink felgyorsult, képek és felületes élmények vezérelte világában tulajdonképpen csak hosszú távon, a tudatos emberi lét támogatásával, hatékony oktatással lehet kivitelezni. Nyilvánvaló módon a fenti műveletek stratégiai kitervelői és alkalmazói jól ismerhetik a globalizálódott tömegtársadalmak szociálpszichológiáját és fő mozgatórugóit – az emberek biztonságigényét, alapfelfogását –, valamint e tényezők komplex erőhatásainak akár hadászati célú alkalmazásával, befolyásolásával hatékonyan elérhetik céljaikat. Az információs és pszichológiai műveletek elsősorban a hátország civil társadalmát, a lakosságot célozzák, míg a technológiaalapú kibertámadások és -műveletek a célország kritikus infrastruktúrájában próbálnak minél nagyobb kárt és zavart okozni. A sokat használt posztmodern

[46] Clarke–Knake: i. m. 9.
[47] Lippmann: i. m. 28.

világ és mindenható elektronikus és nyomtatott sajtóuniverzum kiváló ismerője, Marshall McLuhan még 1970-ben, az internet és a webalapú közösségi médiaplatformok 21. századi paradigmája előtt megfogalmazta baljóslatú észrevételét, miszerint „a III. világháború már egy gerillainformációs háború lesz, amelyben eltűnik a hadsereg és a civil lakosság közötti különbségtétel".[48]

A 21. században a puha erőbehatások és befolyásoló műveletek fentebb bemutatott változatos formái sokkal hatékonyabb eszközei lesznek a szemben álló felek stratégiai előnyszerzést célzó harcának, mint a nyers, kinetikus (fegyveres) erők alkalmazása, ami eddig végigkísérte az emberiség évezredes küzdelmeit.

A döntéshozóknak tekintetbe kell venniük a megváltozott társadalmi és biztonsági környezetet, technikai körülményeket, hiszen a digitális korban egy nagyszabású és költséges fegyveres konfliktust megelőzhet, sőt kiválthat egy átfogó és pusztító, bénító hatású elektronikai, illetve kibertámadás-sorozat a hátország kritikus infrastruktúrája ellen, kiegészülve a szintén hatásos pszichológiai befolyásoló műveletekkel a lakosság emocionális és kognitív meggyőzésére.

A tanulmányban felvázolt és röviden elemzett társadalmi, politikai jelenségek, illetve az új, 21. századi hadviselési formák fontosságának amerikai elismeréseként, a rivális és a feltörekvő nagyhatalmak (Oroszország, Kína), illetve a „latorállamokként" is emlegetett országok (Irán, Észak-Korea) kiber- és információs hadviselésének ellensúlyozása, elhárítása előkelő helyet és hangsúlyt kapott a Trump elnök vezette amerikai kormányzat által 2017-ben közzétett új Nemzetbiztonsági Stratégiában[49] *(National Security Strategy),* akárcsak a nemrég bemutatott Nemzeti Védelmi Stratégiában[50] *(National Defense Strategy)* is.

Nyilvánvalóan az Amerikai Egyesült Államok stratégiai ellenfelei is tisztában vannak az ország döbbenetes méretű és elrettentő erejű konvencionális és nukleáris haderejével, akárcsak saját korlátaikkal, gyengeségeikkel és erősségeikkel egyaránt. Éppen ezen okból sok rivális állam és nem állami Amerika-ellenes csoportosulás tudatosan alkalmazza a gyengébbek fegyverét, vagyis a bemutatott aszimmetrikus hadviselési formákat, észben tartva Trump elnök nemzetbiztonsági tanácsadójának, az első öbölháború páncélos hadosztályparancsnokának, H. R. McMaster tábornok elhíresült szavait, miszerint „az USA ellen csak kétféleképpen lehet harcolni: aszimmetrikusan vagy bután".[51]

Láthatóan mindezek az átfogó állami szintű stratégiai fenyegetések és kihívások még a sokat emlegetett és mediatizált terrorizmus elleni küzdelmet is háttérbe szorítják a közeljövőben, jelentősen meghatározva a nemzetközi kül- és biztonságpolitikai szereplők mozgásterét és lehetséges forgatókönyveit.

FELHASZNÁLT IRODALOM

Berners-Lee, Tim: *The system is failing.* The Guardian, 2017. 11. 15. https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality

[48] Marshall McLuhan: Culture is our business. Wipf & Stock Publ., New York, 2015, 15.

[49] National Security Strategy of the United States of America. Washington D.C., 2017. december, 32. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (Letöltés időpontja: 2018. 02. 12.)

[50] Summary of the National Defense Strategy of the United States of America. 2018. március, 2–4. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (Letöltés időpontja: 2018. 05. 20.)

[51] National Geographic TV: Film on American Generals. 2007.

Clarke, Richard A. – Knake, Robert: *Cyber War: The Next Threat to National Security and What to do about it*. New York, Harper & Collins, e-könyv, 2010.

Farrell, Henry: *The Chinese government fakes nearly 450 million social media comments a year. This is why.* The Washington Post, 2016. 05. 19. https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/?noredirect=on&utm_term=.bc3e3e8f7890

Geraszimov, Valerij: *Az előrelátás értéke a tudományban*. VPK, 2013. 02. 27. https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf

Haig Zsolt: *Az információs társadalmat fenyegető információalapú veszélyforrások.* Hadtudomány, XVII. évf. 2007/3. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2201/hadtud_2007_3_haig.pdf?sequence=1&isAllowed=y

Haig Zsolt – Kovács László: *Fenyegetések a cybertérből.* Nemzet és Biztonság, 2008/5. http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf

Hollis, Daniel: *Cyberwar case study: Georgia 2008*. SWJ, 2011. január 6. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Krekó Péter: *Tömegparanoia, az összeesküvés-elméletek és álhírek szociálpszichológiája*. Athenaeum, Budapest, 2018.

Layton, Peter: *Working Paper on Fifth Generation Air Warfare*. RAAF, 43. 2017. http://airpower.airforce.gov.au/APDC/media/PDF-Files/Working%20Papers/WP43-Fifth-Generation-Air-Warfare.pdf

Lippmann, Walter: *A külvilág az elménkben*. In: Angelusz Róbert – Tardos Róbert – Terestyéni Tamás (szerk.): Média – Nyilvánosság – Közvélemény. Gondolat Kiadó, Budapest, 2007.

Lippmann, Walter: *Public Opinion*. New York, Free Press, 1997.

McLuhan, Marshall: *Culture is our business*. Wipf & Stock Publ., New York, 2015.

Molander, Roger C. – Riddile, Andrew – Wilson, Peter A.: *Strategic Information Warfare: The New Face of War.* RAND Corp., 1995. www.rand.org/pubs/monograph_reports/MR661.html

Molander, Roger C. – Riddile, Andrew – Wilson, Peter A.: *Strategic War... in Cyberspace.* RAND Corp., 1996. https://www.rand.org/pubs/research_briefs/RB7106.html

Munk Sándor: *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései*. Hadtudomány, 2018/1. http://real.mtak.hu/77921/1/HT20181_115_133_u.pdf

National Geographic TV: *Film on American Generals.* 2007.

National Security Strategy of the United States of America. Washington D.C., 2017. december. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

NATO Kibervédelmi Kíválósági Központja: https://www.ccdcoe.org/

Porche III., Isaac R. – Paul, Christopher – York, Michael – Serena, Chad C. – Sollinger, Jerry M. – Axelband, Elliot – Min, Endy Y. – Held, Bruce J.: *Redefining information warfare boundaries for an army in a wireless world.* RAND Corp. – Arroyo Center, 2013. https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf

Resperger István – Kis Álmos Péter – Somkuti Bálint: *Aszimmetrikus hadviselés a modern korban*. Zrínyi Kiadó, Budapest, 2015.

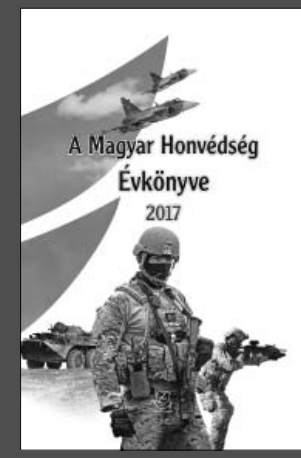
Summary of the National Defense Strategy of the United States of America. 2018. március, 2–4. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

U.S. Army War College: *Information Operations Primer: Fundamentals of Information Operations*, Carlisle, PA, 2006. http://www.csl.army.mil/usacsl/publications/IO-Primer-AY07.pdf

Waltzman, Rand: *The Weaponization of Information – the need for cognitive security.* RAND Corp. 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

http://infowar.cepa.org/Briefs/Est/10-years-after-Web-War-I-in-Estonia
https://www.citatum.hu/idezet/15580
https://kelgyo.blog.hu/2017/12/18/mark_twain_idezetek
https://www.mimi.hu/pszichologia/kognitiv_disszonancia.html
https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/
http://www.technovelgy.com/ct/content.asp?Bnum53

A Magyar Honvédség Évkönyve 2017



A hagyományokhoz hűen a Magyar Honvédség évkönyv formájában összegzi az elmúlt egy év legfontosabb eseményeit, az elért eredményeket és sikereket, mindazon kihívásokat, amelyek meghatározóak voltak a hon védelmének feladatai, történései terén. A 2017-es év is bővelkedett ilyen eseményekben, hiszen lassan megszokjuk, hogy a mindennapi életünk civil szférájában sem lehet a biztonság fogalma üres frázis.

2017-ben fontos feladataink voltak, amelyek közül talán a legnagyobb hangsúllyal a „Zrínyi 2026" Honvédelmi és Haderőfejlesztési Program, ennek részeként a Magyar Honvédség technikai eszközei korszerűsítésének megkezdése, valamint nagy hangsúllyal az Önkéntes Területvédelmi Tartalékos Rendszer bevezetése és annak toborzási feladatai szolgáltatták a legtöbb témát a közvélemény számára is.

Történelmi lehetőség előtt áll a Magyar Honvédség, hiszen a „Zrínyi 2026" Program nyomán, a költségvetési feltételeket is megteremtve valósággá válhat egy korszerű eszközökkel felszerelt, a kor biztonsági kihívásaira adekvát válaszokat adó honvédség létrehozása úgy, hogy biztosítva legyen az a társadalomból építkező hátország is, amely önként, de tudatosan gondolkodik és tesz az ország biztonságáért. Olyan feladatokról beszélünk, amelyek alapjaiban határozzák meg hosszú távon a honvédelmi képességeinket. Az Önkéntes Tartalékos Rendszer területi alapokra helyezése egy olyan kezdeményezés, egy olyan hosszú távú honvédelmi képesség kiépítése, amely közvetlenül is megszólítja a civil társadalmunk tagjait, közvetlenül is lehetőséget biztosítva a hazánk védelmi feladataiban való részvételhez.

Dr. Benkő Tibor vezérezredes
Honvéd Vezérkar főnök
(Részlet a kötethez írt előszóból)