HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

FEKETE CSANÁD[1]

Az információs hadviselés orosz koncepciójának fejlődése a hidegháború végét követően[2]

The Evolution of Russian Information Warfare Concept after the Cold War

Absztrakt

A globális információs tér megjelenését követő években viszonylag hamar megjelent az információs hadviselés koncepciója, melynek következtében létrejött a nagyhatalmak közötti stratégiai vetélkedés egy újabb terepe. A töretlen fejlődés eredményeképp napjainkra kialakult a béke- és háborús időszakban megszakítás nélkül folyó globális információs küzdelem, melyben az információs erőforrások fegyverként kerülnek felhasználásra a tömegek tudatának manipulálása és a külpolitikai célok elérése céljából. Cikkemben Oroszország információs műveletekkel kapcsolatos koncepcióit vizsgálom meg, mely reményeim szerint hozzájárul a napjainkban folyó információs háború hátterének jobb megértéséhez.

Kulcsszavak: információs hadviselés, új generációs hadviselés, fegyveres konfliktusok, lélektani hadviselés

Abstract

Following the formation of the global informational space the concepts of informational warfare has rapidly developed and it has led to the formation of a new battleground which is an ideal place for the strategic rivalry between the great powers. Nowadays, as a result of continuous development a new global informational confrontation has evolved that ongoing in both peacetime and wartime where informational resources used as weapons to manipulate the consciousness of the masses and to reach foreign policy goals. In my article I will examine Russia's

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, doktorandusz hallgató – National University of Public Service, Doctoral School of Military Sciences, PhD student, E-mail: fekete.csanad@uni-nke.hu, ORCID: 0000-0002-9873-4736

[2] Az Emberi Erőforrások Minisztériuma ÚNKP 17-3-I-NKE-58 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

informational warfare concepts which may contributes to a better understanding of the background of today's informational war.

Keywords: information warfare, new generation warfare, armed conflicts, psychological warfare

BEVEZETÉS

Az elmúlt két év során számos kutató vélekedett úgy, hogy a 2014-es ukrán válság kirobbanásával beköszöntött a hadviselés egy olyan új korszaka, melyben a küzdelem súlypontja áthelyeződött a kognitív hadszíntéren folyó információs és pszichológiai műveletek irányába. Mindez egy folyamatos fejlődési folyamat eredménye, mely szorosan összefügg az információs technológiák forradalmával, az egyre gyorsuló globalizáció jelenségével, valamint a bipoláris világrend felbomlását követő geopolitikai folyamatokkal. Ezek hatására drasztikusan megváltoztak a társadalmi és politikai keretek, mely jelentős mértékben kihatott a fegyveres konfliktusok természetére.

A technológia fejlődése kapcsán egyesek egy új hadügyi forradalom kibontakozására hívták fel a figyelmet, melynek középpontjában olyan koncepciók álltak, mint a hadviselés hálózatközpontú és hatásalapú megközelítése. Az orosz információs hadviselési koncepciókra kezdetben az új hadügyi forradalom kapcsán felmerülő kérdések és a hálózatközpontú hadviselés koncepciója gyakoroltak nagy hatást.

Az oroszok már a kezdetektől figyelemmel kísérték a nyugati országokban zajló fejlődési trendeket, így a szovjet fegyveres erők vezérkari főnöke, Nyikolaj Ogarkov marsall az elsők között foglalkozott az új hadügyi forradalom – vagy más néven katonai technikai forradalom (Military Technical Revolution – MTR) – kérdéseivel az 1970-es és '80-as években. Az 1991-es öböl-háború eseményei igazolták a tábornok meglátásait, és bebizonyították az újonnan kifejlesztett C4I[3] rendszerek hatékonyságát és az információs fölény elérésének fontosságát.[4]

Az információs hadviselés orosz koncepciójának fejlődésében emellett a '90-es évek néhány későbbi konfliktusa és Oroszország politikai átalakulása is nagy szerepet játszott, melyek főbb tanulságait alapul véve röviden megvizsgálom, hogy a jelenleg is zajló orosz információs műveletek milyen koncepciókra épülnek, és azok hogyan illeszkednek az új típusú hadviselésről alkotott elképzelésekbe. Reményeim szerint írásom segít megérteni a napjainkban zajló információs konfrontáció hátterét, mely megvilágíthatja a mögötte meghúzódó orosz szándékok természetét.

[3] Katonai információs rendszerek (Command, Control, Communication, Computer, Intelligence – Vezetés, Irányítás, Híradás, Informatika és Felderítés).
[4] Fitzgerald Mary C.: Marshal Ogarkov on the modern theater operation. *Naval War College Review,* 39 (1986/4).

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

AZ INFORMÁCIÓS HADVISELÉSRŐL ÁLTALÁBAN

Az információs forradalom hatásai megkerülhetetlennek számítanak a téma szempontjából, ezért fontosnak tartottam, hogy elsőként röviden kitérjek az információs hadviselés és a lélektani műveletek főbb jellemzőire. A különböző történeti korszakokon végigtekintve, nehezen vitatható, hogy a különféle információalapú tevékenységek – mint amilyen a katonai megtévesztés, a propagandaterjesztés, valamint a hírszerzés – béke- és háborús időszakban egyaránt meghatározó szerepet játszottak. Ennek ellenére ezen tevékenységeket csak az utóbbi évtizedek folyamatai alakították egy olyan egységes rendszerré, amit a szakirodalom összefoglaló néven információs hadviselésnek nevez.[5] Ehhez elsősorban az infokommunikációs technológiák terén bekövetkezett robbanásszerű fejlődés járult hozzá, melynek köszönhetően létrejött a kibertér, és kialakultak az információs társadalmak.

Mindez azzal járt, hogy a szárazföldi, tengeri, légi és kozmikus hadszíntér mellett létrejött a hadviselés egy újabb, információs tartománya,[6] mely magába foglalja az összes valós és virtuális teret, helyet, eszközt és rendszert, amely az információ megszerzésével, előállításával, feldolgozásával, felhasználásával, tárolásával és védelmével foglalkozik. Az információs hadszíntér a globális információs környezet része, mely a valódi hadszíntéren túlnőve magában foglalja a hátországban működő katonai és polgári szervek infokommunikációs rendszereit és szervezeteit, melyek támogatják, biztosítják vagy jelentősen befolyásolják a katonai műveleteket.[7]

Az e hadszíntéren folyó műveletek legfőbb célja az információs fölény és uralom elérése, melyek kevesebb erőforrás bevonásával és a veszteségek csökkentésével teszik lehetővé a győzelem kivívását. Az információs műveletek számos, egymást kiegészítő területet fognak össze, amiket a stratégiai kommunikáció foglal egyfajta keretbe, megteremtve az összhangot a különböző információalapú tevékenységek között.

A modern értelemben vett információs műveletek összehangolt alkalmazására többek között a ’91-es öböl-háború, a 2003-as iraki háború vagy a 2014-es ukrán válság során került sor, melyek egyebek mellett rámutattak a lélektani tevékenységek konfliktusokban játszott szerepének felértékelődésére.

[5] Az információs hadviselés első definícióját Thomas P. Rona, az Egyesült Államok védelmi minisztériumának magyar származású kutatója alkotta meg 1976-ban. Rona definíciójában az információs eszközök és módszerek béke- és háborús időszakban történő koordinált alkalmazásáról ír, melyek stratégiai, hadműveleti és harcászati szinten egyaránt folyhatnak, segítve a kitűzött célok elérését. Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése. *Hadtudomány,* 21. (2011/1–2).

[6] Szakértők szerint a modern értelemben vett információs hadviselés korai alkalmazására elsőként az 1991-es Öböl-háború ideje alatt került sor. Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.

[7] Uo. 157.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

AZ INFORMÁCIÓS HADVISELÉS OROSZ KONCEPCIÓJÁNAK MEGALKOTÁSA A HIDEGHÁBORÚ UTÁN

A világban végbemenő geopolitikai átalakulás – a bipoláris világrend és a Szovjetunió összeomlását, valamint a délszláv háború kitörését kísérő folyamatok – hatására az újonnan létrejövő Oroszországi Föderáció kereste helyét az új nemzetközi rendszerben. A beilleszkedést nehezítette, hogy az egykori szuperhatalom szinte minden területen jelentős visszaesést élt át, az egykori befolyási övezetből a csapatok fokozatos kivonásával jelentősen csökkent Moszkva nemzetközi befolyása, amit komoly presztízsveszteségként élt meg az orosz politikai elit és társadalom. A helyzetet tovább súlyosbította, hogy az újonnan létrejött állam gazdasága romokban hevert, így képtelen volt eltartani a megörökölt katonai struktúrát, ami a katonai képességek erodálódásához és számos félresikerült katonai reformkísérlethez vezetett.[8] Emellett a társadalom is hatalmas nehézségekkel nézett szembe, így nem csoda, hogy az átalakulással járó folyamatok hamar politikai válságokba torkolltak.

Az Oroszországot körülvevő régióban sem volt jobb a helyzet, a posztszovjet térség szinte minden állama hasonló nehézségekkel volt kénytelen szembe nézni. Ennek köszönhetően számos helyen – többek között Hegyi-Karabahban Örményország és Azerbajdzsán között, Dél-Oszétia és Abházia hovatartozása kapcsán Grúziában, a Dnyeszter Menti Köztársaság kikiáltását követően Moldovában, majd később a Csecsenföldön – fegyveres konfliktusok robbantak ki. A fegyveres harcok ugyan elcsitultak, de a problémák továbbra is fennmaradtak, így a posztszovjet térség úgynevezett befagyott konfliktusai máig tartó feszültségforrásként rontják a régió biztonságát és tovább mérgezik az országok közötti

[8] Az Anatolij Szergyukov védelmi miniszter által fémjelzett átfogó modernizációs program előtt három haderőreform-kísérlet is zajlott Oroszországban. A Szovjetuniótól megörökölt nagy létszámú haderő szervezetének strukturális átalakítása a szűkülő források függvényében elsősorban létszámleépítések formájában jelentkezett az 1990-es években. Vlagyimir Putyin hatalomra kerülése és a növekvő energiaárakból származó bevételek folytán később lehetővé vált az orosz fegyveres erők átfogó modernizációs programjának megvalósítása. Mindez főként Szergej Ivanov védelmi miniszter nevéhez fűződik, aki a 2000-es orosz katonai doktrína után 2003-ban kiadta „Az Oroszországi Föderáció fegyveres erői fejlesztésének aktuális feladatai" nevet viselő dokumentumot, majd erre építve 2005-ben meghirdette a gyökeres reform programját. A 2008-ban kirobbant orosz–grúz háború a reformfolyamat szempontjából is fontos állomásnak számít, ami felhívta a figyelmet az orosz fegyveres erők jelentős hiányosságaira és problémáira. Ezek megoldására az új védelmi miniszter, Anatolij Szergyukov 2008 szeptemberében egy újabb, több lépcsős fejlesztési programot dolgozott ki, amely tartalmazta: a fegyveres erők szerkezeti és személyügyi átalakítását, az állomány szociális kérdéseinek megoldását, a diszlokáció és a hadrafoghatóság fejlesztését, valamint a technikai eszközök modernizációját. A tábornoki kar ellenállásába is ütköző ambiciózus reformprogram számos eredményt hozott, de részben a megváltozott politikai és gazdasági helyzet miatt időközben menesztették Szergyukovot, akit 2012-ben Szergej Sojgu váltott a védelmi miniszteri poszton. Nyikolaj Makarov vezérkari főnök helyébe pedig Valerij Geraszimov vezérezredes lépett. A változások ellenére – ami együtt járt a reformfolyamat ütemének mérséklésével és kiigazításával – tovább folytatódott az orosz fegyveres erők modernizációja. Négyesi Áron: Az orosz haderőreformok eredményei a haderő-szervezet és a személyi állomány tekintetében. Biztonsagpolitika.hu, 2013; Rácz András: Az orosz haderőreform rövid áttekintése. MKI-tanulmányok T-2008/31.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

kapcsolatokat. Mindez jelentősen behatárolta az orosz fegyveres erők helyzetét és lehetőségeit, ami kihatott a jövő hadviseléséről alkotott orosz koncepciók jellegzetességeire.[9]

Az orosz teoretikusok korán felismerték, hogy az új hadviselési formákhoz történő alkalmazkodás megköveteli, hogy a hidegháború ipari háborúinak tömeghadseregekre épülő korábbi szovjet doktrínáit és harceljárásait felülvizsgálják. Az új koncepciók megalkotása során figyelembe vették Oroszország politikai és katonai lehetőségeit, melynek tükrében aggódva figyelték az 1991-es öbölháború és az 1999-es koszovói beavatkozás eseményeit, valamint az Egyesült Államok által megalkotott új hálózatközpontú hadviselés koncepcióját, ami a világban zajló tudományos-technológiai forradalomra épült.[10] Az orosz kutatók elsősorban a Nyugat által megalkotott új hadviselési formára adható válaszokat keresték, továbbá megoldással akartak szolgálni arra, hogy hogyan lehetne ebben az Oroszország számára kedvezőtlen nemzetközi helyzetben érvényre juttatni az orosz nemzeti érdekeket és külpolitikai törekvéseket.

Az ország gazdasági lehetőségei nem tették lehetővé, hogy a konvencionális katonai képességek téren felvegyék a versenyt a nyugati országokkal, azonban felfigyeltek arra a folyamatra, ahogy a nem katonai– politikai, gazdasági, diplomáciai, információs – eszközök jelentősége megnőtt a konfliktusok során, és a stratégiai célok elérésének fontos részeivé váltak. Az oroszok rájöttek, hogy külpolitikai céljaikhoz új aszimmetrikus – indirekt – eszközök kellenek, melyek közül a ’90-es években kialakuló globális információs térben fedezték fel a stratégiai rivalizálás egy újabb, döntő fontossággal bíró tartományát. Az orosz teoretikusok egy része amellett érvelt, hogy a technológiai fejlődés olyan szakaszába lépett a világ, amikor az információs fegyverekkel vívott küzdelem stratégiai jelentőségre tett szert, melyek alkalmazásával elérhetőek a kitűzött stratégiai és politikai célok.[11]

Az olyan teoretikusok, mint Vlagyimir Pirumov vagy S. A. Komov amellett érveltek, hogy az orosz érdekek információs térben való biztosítása érdekében tudományos módszerekkel le kell fektetni az információs hadviselés elveit és törvényszerűségeit.[12] Pirumov szerint az információs konfliktusokban ugyanúgy érvényesek és használhatóak a hagyományos fegyverekkel vívott harc általános törvényszerűségei. Az általa vizsgált trendek közül érdemes néhányat kiemelni, mivel a mai napig ezeken alapul az információs hadviselés orosz koncepciója:

1. az információs hadviselés egyre növekvő szerepet fog játszani a harcoló csapatok támogatása terén, amely összefügg az információs technológiák széleskörű rendszerbe állításával;
2. az információs hadviselés egyaránt zajlik béke és háborús időszakban;

[9] Geers Kenneth: Cyberspace and the Changing Nature of Warfare. *SC Magazine,* Black Hat, 2008.
[10] Armistead Edwin L.: Information Operations: The Hard Reality of Soft Power. Potomac Books, 2004.
[11] Chekinov, S. G., Bogdanov, S. A.: “Влияние непрямых действий на характер современнойвойны” (The influence of the indirect approach on the nature of modern warfare). *Voyennaya mysl,* No. 62011. sz. 2011.
[12] Fitzgerald Mary C.: Russian Views on Electronic and Information Warfare. Hudson Institute, 1996.

3. a fegyveres erők és kormányzati szervek információs rendszereinek növekvő száma miatt az információs hadviselés a fegyveres harc különálló formájává fog válni.

Ezen trendek erősödését elősegíti a hagyományos fegyveres agresszió tiltása a nemzetközi érintkezések terén, illetve az információs hadviselést szabályozó nemzetközi jogi keretek hiánya – ez utóbbi még a mai napig problémát jelent, habár az utóbbi időben történtek előrelépések e téren.[13]

Pirumov és más orosz szerzők megállapításai nagyban támaszkodtak az 1994–1996 között zajlott első csecsen háború tapasztalataira, ahol a csecsen felkelők kreatívan használták ki a modern információs környezet és a média által nyújtott lehetőségeket, ami felhívta az orosz vezetés figyelmét az információs tér konfliktusokban játszott növekvő szerepére. A csecsen konfliktus továbbá ráirányította az orosz vezetés figyelmét az információs fölény korai kivívásának fontosságára, mely elengedhetetlen a stratégiai célok gyors elérése szempontjából.

A konfliktus során Moszkva a „saját kárán" tapasztalta meg, hogy a siker érdekében kulcsfontosságú a megjelenő információk fölötti kontroll biztosítása. A harctérről szóló hírek – vagy a szemben álló fél által folytatott információs műveletek – ugyanis képesek befolyásolni a hazai és nemzetközi közvéleményt, rombolni a katonák morálját, nyomás alá helyezni a döntéshozókat, melyek kulminált hatásai végül jelentősen kihathatnak a harcok kimenetelére, eldöntve az adott konfliktus kimenetelét.

A csecsenek és más felkelő – vagy terrorista – szervezetek sokszor gyorsabban alkalmazkodnak a megváltozott körülményekhez, feltérképezik a szemben álló fél gyenge pontjait, kihasználják a modern információs technológiák és a globalizált világ nyújtotta lehetőségeket. Ezen tényezőknek köszönhetően a bürokratikus, lassú állami szerveknél rugalmasabban tudnak reagálni a konfliktusok folyamatosan változó eseményeire, melyről tudósításokat, képeket és videókat tesznek közzé a világhálón, megnyerve a helyi lakosság – vagy akár a nemzetközi közvélemény – támogatását, és képesek hatást gyakorolni a szemben álló fél politikai és katonai döntéshozatalára.[14]

AZ OROSZOK ÁLTAL FOLYTATOTT INFORMÁCIÓS HADVISELÉS NÉHÁNY JELLEMZŐ VONÁSA

Az amerikai elnökválasztási kampány eseményei és a választási folyamatok befolyásolására indult információs műveletek minden korábbinál nagyobb mértékben világítottak rá a Nyugat és Oroszország között egyre inkább eszkalálódó információs konfrontáció veszélyeire. Az oroszok által kiépített támadó jellegű információs képességek hatékonyságára már a 2007-es észtországi kibertámadások, a 2008-as orosz–grúz háború vagy a 2014-es

[13] Heickerö Roland: Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. FOI Swedish Defence Research Agency Defence Analysis, 2010.
[14] Thomas Timothy L.: Manipulating The Mass Consciousness: Russian And Chechen "Information War" Tactics In The 2nd Chechen-Russian Conflict. Fort Leavenworth, KS., Foreign Military Studies Office, 2000.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

ukrán válság alatt zajló információs műveletek is rámutattak, azonban a nyugati politikai elit és a közvélemény csak az elmúlt hónapok eseményei során szembesült annak közvetlen hatásaival és valódi természetével. Az események sokként érték a nyugati országokat, egyesek félelmei szerint fennáll annak a veszélye, hogy a tovább eszkalálódó információs konfliktus befolyásolhatja az Európa számos országában megrendezendő idei választások kimenetelét.[15]

A közelmúlt történései kapcsán le kell szögezni, hogy az oroszok által folytatott információs hadviselés nem számít új jelenségnek, elméleti alapjait a Szovjetunió időszakában fektették le. Az olyan, hidegháborús időkben kifejlesztett és alkalmazott technikákat, mint a maszkirovka és reflexív kontroll[16] hozzáigazították a 20. század végének megváltozott információs körülményeihez, és szervesen beépítették a hadviselés új típusú orosz megközelítésébe. Az információs eszközök felértékelődése kapcsán számtalan tanulmány és cikk jelent meg az évek során az orosz katonai folyóiratok, a *Voennaja Miszl,* a *Nezavisimoye Voyennoye Obozreniye,* a *Zarubezhnoe Voennoe Obozrenie*, a *Voyenno Promyshlennyy Kuryer* vagy a *Krasnaya Zvezda* lapjain.

A trendek megfigyelhetőek továbbá az Oroszországi Föderáció által kiadott stratégiai dokumentumokban, vagy a témával foglalkozó olyan szerzők munkáiban, mint Sz. A. Bogdanov, Sz. G. Csekinov, Vlagyimir Szlipcsenko, Timothy L. Thomas vagy Keir Giles. A következő fejezetben részletesebben kifejtem az orosz szerzők által tett főbb megállapításokat, és megvizsgálom azt a folyamatot, hogyan vált az információs hadviselés az orosz külpolitikai eszköztár egyik legfőbb elemévé.

Az információs hadviselésről alkotott nyugati koncepciókkal szemben az orosz teoretikusok már ezen időszakban is nagy hangsúlyt fektettek a pszichológiai hadviselés és hatások szerepére. Az orosz elképzelésekben nem a technikai központú kibertér kifejezés, sokkal inkább a szélesebb körű információs tér megjelölést használják, mutatva ezzel a nyugati és orosz felfogás közötti különbségeket: az oroszban az információ áll a középpontban.[17]

Az orosz elképzelésekben az információs hadviselésnek két fő – egymást kiegészítő oldala – létezik: az információs-technikai és az információs-pszichológiai hadviselés. Az információs-technikai hadviselés döntően a nyugati terminológia szerinti számítógép-hálózati hadviselést és az elektronikai hadviselést foglalja magában, beleértve az információs rendszerek technikai eszközökkel történő támadását vagy védelmét.

---

[15] Mansfield Katie: Europe ready for CYBERWAR over fears Russia will hack Germany, France and Netherlands vote, express.co.uk, 2016.

[16] A reflexív kontroll technikájának kidolgozása V. A. Lefebrve nevéhez fűződik, aki az 1960-as években egy, a percepciók megváltoztatására irányuló új eljárást dolgozott ki, melynek segítségével anélkül lehet befolyásolni a célba vett egyének vagy csoportok döntési folyamatait, hogy azok tudatában lennének ennek. Kramer, X.H., Kaiser T.B., Schmidt S. E., Lefebvre V. A.: From Prediction to Reflexive Control, Reflexive processes and control. *International Interdisciplinary Scientific and Practical Journal,* 2 (2003/1).

[17] GILES Keir: Handbook of Russian Information Warfare, Research Division NATO Defense College, 2016.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

Az információs-pszichológiai hadviselés pedig a közvélemény és a tömegek tudatának befolyásolását, a kognitív folyamatok manipulálását, a politikai és katonai döntéshozatali folyamatok lassítását és bénítását, végül a kedvező politikai hatások kiváltását célozza.[18]

A cikk további részében elsősorban az információs-pszichológiai hadviselés tükrében fogom megvizsgálni az orosz koncepciókat, ami az orosz értelmezés szerint további két fő területre osztható: a belföldön és a külföldön folytatott tevékenységekre.

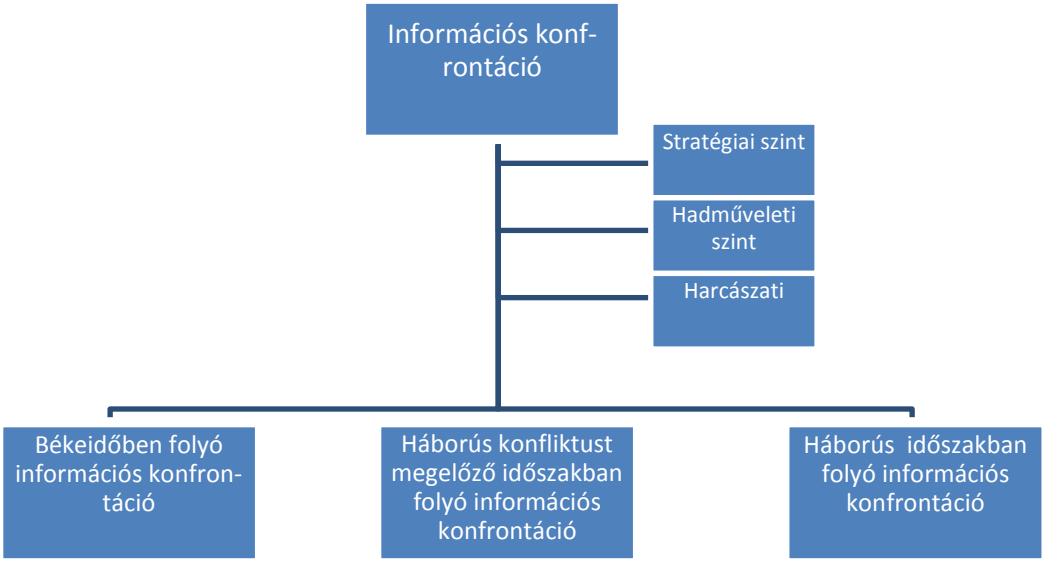
Közülük az előbbi a hazai lakosság információs tevékenységeinek ellenőrzését és irányítását fogja össze, kiemelt helyen kezelve az információ áramlása feletti kontroll kérdését – történjen az akár a nyomtatott vagy online sajtón, rádiós vagy televíziós műsorokon keresztül. Mindez kulcsfontosságú arra nézve, hogy biztosítsák a politikai rendszer stabilitását, irányítás alatt tartsák a társadalmi folyamatokat, elhárítsák az ellenérdekelt információs tevékenységeket és befolyásolási kísérleteket.

A belföldön folytatott tevékenységek kiemelt fontossággal bírnak az orosz koncepciókban, a téma szempontjából mégis az információs hadviselés külföldre irányuló tevékenységei számítanak lényegesebbnek. Ezzel kapcsolatban az orosz teoretikusok és geopolitikusok azt állítják, hogy a béke és háború közötti határvonal megszűnt, az információs hadviselés pedig többé már nemcsak a fegyveres konfliktusokra és a műveleteket előkészítő bevezető szakaszra korlátozódik.[19] Az információs konfrontáció intenzitását tekintve három lehetséges szinten – stratégiai, hadműveleti és harcászati –, valamint három különböző időszakban – békeidőben, háborút megelőző és háborús helyzetekben – folyhat:

[18] Thomas Timothy L.: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies,* 2014.
[19] Giles Keir: Handbook of Russian Information Warfare. Research Division NATO Defense College, 2016, 4.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám



1. ábra: Az információs konfrontáció időszakai és szintjei
(Készítette a szerző)

1. Békeidőszakban az információs konfrontációra történő folyamatos felkészülés zajlik:
   - a titkosszolgálatok a hírszerzési és felderítési tevékenységeken túl a célországban kiépítik a szükséges hálózatokat és infrastruktúrát;
   - felveszik a kapcsolatot és támogatják az érdekeiknek megfelelő politikai pártokat, civil szervezeteket és gazdasági szereplőket;
   - igyekeznek befolyás alá vonni a különböző médiafelületeket, vagy újakat hoznak létre;
   - behatolnak az állami szervek, politikai pártok és egyéb szervezetek számítógépes hálózataiba, ahol kémprogramokat telepítenek, és titkos adatgyűjtést végeznek;
   - a hivatalos álláspontnak ellentmondó összeesküvés elméletekkel és egyéb narratívákkal megkezdődik egy alternatív valóság megteremtése és a percepciók megváltoztatása.

A békeidőben folyó tevékenységek tehát a stratégiai szinten megvalósuló maszkirovka (*megtévesztés, rejtés, álcázás – camouflage, concealment, deception, CC&D*) és a társadalom percepcióinak megváltoztatására irányuló reflexív kontroll jegyében kerülnek végrehajtásra – ez utóbbit a közelmúltban felcserélték a percepció menedzsment fogalmával.[20]

[20] Uo.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

Ezen tevékenységek lényegi elemét képezi, hogy a valós helyzetről, a saját erők helyzetéről, erejéről és tevékenységeiről álhírek, hamis információk és az információkkal történő manipulációk által hamis képet alakítanak ki annak érdekében, hogy a szemben álló fél politikai és katonai vezetése olyan kiszámítható döntéseket hozzon, melyek kedvezőtlenek számára. A percepciók ilyen irányba történő megváltoztatása – az elérni kívánt stratégiai céloktól függően – célozhatják a széles tömegeket vagy akár a döntéshozók szűk körét is.

2. A háborús állapotokat megelőzően induló információs konfrontáció fő célja, hogy a szemben álló fél tudta nélkül és még a konfliktus aktív szakaszának kezdete előtt a lehető legnagyobb mértékben megbénítsa:
   - a szemben álló fél kritikus információs infrastruktúráját;
   - a politikai és katonai döntéshozatalát;
   - ezen keresztül pedig: belső feszültséget keltsen, befolyásolja és destabilizálja annak társadalmát.

S. A. Bogdanov, S. G. Csekinov szerint már ebben az időszakban meg kell ragadni a kezdeményezést, és meg kell szerezni az információs fölényt. Összességében elmondható, hogy a háborús állapotokat megelőző időszakban folytatott tevékenységek intenzitását jelentősen növelik, az előkészítés után az erőfeszítések arra irányulnak, hogy a célpontot gyengítve ideális állapotok álljanak elő egy fegyveres konfliktus sikeres és gyors megvívásához.[21]

3. A háborús időszakban folyó információs konfrontáció a szemben álló fél feletti információs fölény elérését célozza, melynek segítségével megbéníthatóvá válnak az ellenség információs rendszerei és biztosítani lehet a saját információs infrastruktúra védelmét. Az első két fázisban folyó maszkirovka ezen időszakban már stratégiai, hadműveleti és harcászati szinten egyaránt folyik annak érdekében, hogy megtévesszék a szemben álló fél hírszerző szolgálatait, politikai és katonai vezetését. A háborús konfliktusok alatti tevékenységek elsősorban a katonai műveletek támogatása érdekében folynak, beleértve az ellenség vezetési irányítási és katonai információs rendszereinek pusztítását – ahogy ez Ukrajnában is történt –, az elektromágneses spektrumban folytatott támadó és védelmi jellegű tevékenységeket, a számítógépes hálózatok elleni támadásokat és a tömegek tudatának befolyásolása érdekében folyó lélektani műveleteket.

A stratégiai szinten folyó információs konfrontáció alatt az egy vagy több hadszíntéren folyó műveletek végrehajtásáért az állam legfelsőbb szintjén álló minisztériumok és ügynökségek felelősek, a hadműveleti szinten folyó tevékenységeket egy hadsereg vagy hadtest fogja össze, míg a harcászati szinten folyó tevékenységek végrehajtása a közvetlen harcérintkezésben álló alárendelt alakulatokra hárul.[22]

---

[21] Chekinov S. G., Bogdanov S. A: The Nature and Content of a New-Generation War. Military Thought: *A Russian Journal of Military Theory and Strategy,* 2015.

[22] Fontos megjegyezni, hogy az információs műveletek végrehajtásáért a fegyveres erők információvédelemmel, jel- és rádióelektronikai felderítéssel foglalkozó szakcsapatain és az olyan számítógépes

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

Az orosz megközelítés szerint az információs hadviselés középpontjában az információ áll, amely bárhol tárolható és bármilyen csatornán keresztül továbbítható, így a terjesztési közege sem korlátozódik kizárólagosan a kibertérre. Az információs konfrontációban a harcot az úgynevezett *információs fegyverek* segítségével vívják, melyek S. P. Rasztorgujev orosz teoretikus szerint lehetnek bármely olyan technikai, biológiai vagy társadalmi eredetű eszközök vagy rendszerek, amelyek az információ előállításával, feldolgozásával, továbbításával, tárolásával vagy blokkolásával foglalkoznak.[23]

Az információs fegyver ennek értelmében egy veszélyes, olcsó és univerzális fegyverrendszer, amit bárhol, bármikor és bárki ellen be lehet vetni. A fogalmat olyan széleskörűen értelmezik az orosz kutatók, hogy az általuk leírt információs fegyver túlmutat a technikai értelemben vett számítógépes hálózatokon és kártékony szoftvereken. Vitalij Cigicsko orosz kutató szerint az információs fegyverek tulajdonságaikat tekintve több eltérő kategóriára oszthatóak:

- rendeltetésűeket tekintve lehetnek egy- vagy többfunkciósak, illetve univerzálisak;
- hatótávolságukat tekintve alkalmazhatóak rövid vagy nagy hatótávolságú műveletek során;
- a célcsoportokat tekintve képesek lehetnek egyének, csoportok vagy tömegek elleni pusztításra;
- célba juttatásukat tekintve rendelkezésre állhat többféle hordozóeszköz;
- hatásukat tekintve többféle romboló hatással is rendelkezhetnek.

A szerző részben e tulajdonságokból kiindulva egy későbbi írásában hat eltérő csoportot sorolt fel, melynek értelmében az információs fegyvereket eszközként lehet alkalmazni:

1. az olyan berendezések helyzetének pontos meghatározására és fizikai pusztítására, melyek jeleket sugároznak ki az elektromágneses spektrumban;
2. a különböző elektronikai berendezések zavarására és befolyásolására;
3. az egyes elektronikai berendezések vezérlő rendszereinek befolyásolására;
4. az információ továbbítás folyamatának befolyásolására;
5. a propaganda és dezinformáció terjesztésére
6. az úgynevezett pszichotróp fegyverek[24] használatára.[25]

---

incidensek elhárítására szakosodott szervezeteken túl, mint az orosz Számítástechnikai Sürgősségi Reagáló Egység (*Russian Computer emergency Response Teams* – RU-CERT) elsősorban az Oroszországi Föderáció polgári és katonai nemzetbiztonsági és hírszerző szervezetei: a Szövetségi Biztonsági Szolgálat (*Federalnaja Szluzsba Bezopasznosztyi* – FSZB), a Külföldi Hírszerző Szolgálat (*Szluzsba Vnyesnyej Razvedki* – SZVR), valamint a Katonai Felderítő Főcsoportfőnökség (*Glavnoje Razvedivatyelnoje Upravlenyije* – GRU) felelnek. Bővebben lásd Giles Keir: Handbook of Russian Information Warfare. Research Division NATO Defense College, 2016.

[23] Thomas Timothy L.: Comparing US, Russian, and Chinese Information Operations Concepts, Fort Leavenworth, KS., Foreign Military Studies Office, 2004.

[24] Anatolij Szergyukov orosz védelmi miniszter 2012-ben bejelentette, hogy az új fizikai törvényszerűségeken nyugvó – irányított energiájú, geofizikai, genetikai, pszichotróp – fegyverrendszerek kifejlesztése a 2011–2020 közötti haderő modernizációs program központi elemét képezi. A pszichotróp fegy-

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

Az információs fegyver másik speciális fajtája egyfajta „társadalmi vírusként”, a kognitív tartományban is alkalmazható – akár nyomtatott sajtótermékként, közvetlen agitációval vagy szóbeli pletykaként terjesztve – az egyes társadalmi csoportok vagy a közvélemény gondolkodási folyamatainak manipulálására.

Az orosz kutatók úgy tekintenek az információs erőforrásokra, mint az agresszió célpontjában álló közvélemény és politikai vezetés támadásának egyik legfőbb és egyben a külpolitikai célok elérésének leghatékonyabb eszközére. Amennyiben megfelelően előkészítették a támadást, az alkalmazó fél képes akár napok alatt destabilizálni a célpontként szolgáló társadalmat és elérni a kívánt politikai hatásokat anélkül, hogy a megtámadott fél tudatában lenne a forrásnak.

Az orosz teoretikusok szerint az információs fegyverek hatékonysága olyannyira megnőtt az utóbbi években – köszönhetően a globális kibertér megjelenésének és fejlődésének, a közösségi média kialakulásának és a széles tömegek elérhetővé válásának –, hogy a teljes siker elérhető a fegyveres erők minimális bevetése mellett – vagy egyes esetekben akár anélkül is.[26]

Az elmúlt évek eseményei és az orosz szerzők információs hadviselésre vonatkozó koncepciójában megfogalmazottak szerint jelenleg a háborús állapotokat megelőző és a háborús időszakban folytatott információs konfrontáció egyfajta keverékének lehetünk tanúi. A fejezetben írtak alapján ennek hátteréről és jellegzetességeiről az alábbi megállapítások tehetők – amiket a közelmúlt eseményei a gyakorlatban is igazoltak:

a. Az információs hadviselés orosz koncepciójának megalkotását nagyban meghatározta a Szovjetunió öröksége, az Oroszországi Föderáció ’90-es évekbeli gazdasági, politikai és katonai helyzete, valamint az erőforrások hiánya. E tényezők nagymértékben hozzájárultak ahhoz, hogy az orosz teoretikusok alternatív és „aszimmetrikus” módszereket kerestek a nemzeti érdekek biztosítása érdekében.
b. Az információs hadviselés orosz koncepciójára nagymértékben hatottak a korszak főbb konfliktusai és az azokból levont tapasztalatok, az infokommunikációs technológiákhoz

verek a pszichológiai és a biológiai kutatások tudományos eredményeit hasznosítják az emberek elméjének manipulálása céljából. A szovjet időkig visszanyúló kutatások célja volt, hogy az agy bizonyos területeit tudatmódosító szerek és elektromágneses mezőket létrehozó speciális technikai eszközök segítségével stimulálják, olyan különleges eljárásokat fejlesztve ki, melyek befolyásolhatják a célpont kognitív folyamatait. Bővebben lásd: Billion dollar race: Soviet Union vied with US in ‘mind control research. RT News, 2013.

[25] Thomas Timothy L.: Information Warfare in the Second (1999–) Chechen War: Motivator for Military Reform? 2003.

[26] Valerij Geraszimov tábornok is hasonló következtetésekre jut a 2000-es évek konfliktusaira és a későbbi eseményekre – főként a 2010-es arab tavaszra – alapozva. A tábornok szerint a Nyugat kifejlesztette a hadviselés egy új hibrid formáját, melyben az információs tér és információs erőforrások széleskörű felhasználására kerül sor annak érdekében, hogy a célpont társadalmát destabilizálják és egy kívánt politikai fordulatot hajtsanak végre. A tábornok az Oroszországi Föderációra leselkedő legnagyobb fenyegetések között említi a színes forradalmakat és a hibrid hadviselést, melynek elhárítására nagy hangsúlyt kell fektetni a jövőben. Geraszimov Valerij: Cennoszty nauki v predvigyenyii. *Vojenno-promislennij kurjer,* 8 (2013/476).

fűződő katonai-technikai forradalom, az orosz politikai és katonai vezetés félelmei a nyugati országok új hálózatközpontú hadviselésétől, valamint a globális információs környezet létrejötte.

c. Az orosz koncepciók némileg eltértek a Nyugaton gyökeret vert technológia-központú megközelítéstől, hangsúlyosabb szerepet szánva a befolyásolási műveletek és a lélektani hadviselés szerepének. Mindez a Szovjetunió időszaka alatt kifejlesztett koncepciókra és hagyományokra épült, amik alapos felülvizsgálaton mentek át, mely során az új információs környezet jelentette lehetőségek kihasználását tűzték ki célul.

d. Az orosz teoretikusok felhasználták és beépítették az információs hadviselésről alkotott koncepciókat az új generációs hadviselésről szóló elméleteikbe. Nézeteik szerint a 21. század konfliktusaiban az információs hadviselés meghatározó jelentőségű lesz. A globális információs közeg részét képező közösségi médiafelületeken és az egyéb hálózatokon folyó küzdelem alapvetően meghatározzák majd a harcok kimenetelét. Mindez azon elképzelésen alapszik, hogy a 21. századi hadviselés legfőbb terepe az emberi elme lesz, ezért az információs műveletek kiemelt szerepet játszanak az új generációs orosz hadviselésben. A siker kulcsát a különböző információalapú tevékenységek összehangolása és az egy cél érdekében történő koordináció megteremtése jelenti.

e. Az utóbbi években stratégiai jelentőségre tettek szert az információs fegyverek. Az információs erőforrások mozgósításával zajló információs konfrontáció egyaránt zajlik a béke és háborús időszakban, melynek legfőbb stratégiai célja a multipoláris világrend kialakítása.

f. A 2000-es években meginduló intenzív fejlesztéseknek köszönhetően az oroszok fokozatosan felzárkóztak a nyugathoz, ledolgozták lemaradásukat és mára képesek maradéktalanul érvényesíteni az orosz érdekeket az információs térben, amit a tavalyi év eseményei is jól mutatnak.

Végül az információs hadviselés orosz koncepciójának kronológiai fejlődését jól szemlélteti a *2. ábra*:

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

A koncepció kidolgozása (1980-1994)

- A hadügyi forradalom és a hálózatközpontú hadviselés megjelenése és az 1991-es öböl háború tapasztalataiból levont következtetések felhasználása
- Ezek alapján megkezdődik az információs hadviselés orosz koncepciójának elméleti kidolgozása

A koncepció első gyakorlati tesztje (1994-1996)

- Az első csecsen háború kitörése, mely rávilágított az információs tér növekvő fontosságára

A koncepció továbbfejlesztése (1996-1999)

- Az információs hadviselés orosz koncepciójának továbbfejlesztése a csecsen háború tükrében
- Az információs hadviseléshez szükséges infrastruktúra kialakítása és az információs rendszerek rendszerbe állításának fokozása
- Az 1999-es koszovói beavatkozás és a második csecsen háború kitörése
- Tanulva az első csecsen háború hiányosságaiból az 1999-ben kitört második csecsen háborúban az oroszok hatékonyan ellenőrizték az információáramlást és felhasználták a médiát

A felkészülés időszaka (1999-2007)

- Az információs hadviselés támadó jellegű, technikai képességeinek gyors ütemű fejlesztése
- Egyesek szerint a 2007-es észtországi kibertámadások során tesztelték az új támadó jellegű kiberképességeket. A támadásokért hivatalosan hazafias orosz hackercsoportok vállalták a felelősséget, ennek ellenére számos nyugati kutató véli úgy, hogy az orosz kormány áll az incidens hátterében

Egy új hadviselési forma születése (2008-2014)

- A 2008-as orosz-grúz háború során az információs hadviselési képességeket elsőként használják háborús időszakban, a katonai műveletekkel összhangban és azok támogatására
- Az orosz-grúz háború tapasztalatainak hatására egy új átfogó modernizációs program veszi kezdetét, melyben kiemelt szerep hárul az információs képességek fejlesztésére
- A 2010-es arab-tavasz és a 2011-es líbiai beavatkozás tapasztalataira építve megszületik az oroszok új generációs hadviselési koncepciója, amit végül 2014-ben az ukrán válság kirobbanásával a gyakorlatban is kipróbáltak

információs konfrontáció fokozódása (2014-)

- Egy globális információs konfrontáció kialakulása a Nyugat és Oroszország között, mely fokozatosan eszkalálódik és és az intenzitása végül 2016-ban meghaladja a békeidőben folyó tevékenységek szintjét

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

KÖVETKEZTETÉSEK

Nehezen vitatható, hogy az utóbbi évek technológiai fejlődése lehetővé tette emberek millióinak valós időben, bármilyen nyelven és országhatártól függetlenül történő célba vételét, mely az információs hadviselés különböző formáinak felhasználásával vált lehetővé. A technikai eszközök folyamatos bővülése által – a kiterjesztett és virtuális valóság technológiájával, a mesterséges intelligencia terén tett fejlesztésekkel, valamint a propagandaterjesztés új automatizált lehetőségeivel, az úgynevezett persona management szoftverek[27] segítségével – az információs technológiák várhatóan egyre nagyobb szerepet fognak játszani a stratégiai célok eléréséért folytatott vetélkedésben. A nyugati országok felismerve a permanens információs konfrontációval kapcsolatban jelentkező veszélyeket, igyekeznek lépéseket tenni az álhírek és a propaganda kiszűrése érdekében. Az ilyen jellegű lépések azonban az esetlegesen felmerülő technikai nehézségek mellett a szólásszabadság terén is komoly aggályokba ütközhetnek a jövőben.

Az utóbbi hetek eseményei alapján úgy tűnhet, hogy a döntéshozók kullognak az események után, és csak lassan reagálnak az információs hadviselés jelentette fenyegetésekre, míg a támadók folyamatosan újabb és újabb módszereket fejlesztenek ki céljaik eléréséhez. Az információs technológiák töretlen fejlődése – és ezzel együtt az e technológiáktól való függés további növekedése – azt vetíti előre, hogy az információs tér feletti kontroll megszerzése, az információ áramlásának ellenőrzése, valamint a különböző információs fegyverek még nagyobb szerepet fognak játszani a jövő konfliktusaiban. Mindezt a 2016-os év eseményei is alátámasztják, akkor ugyanis az információs térben és közösségi médiában folyó tevékenységek minden korábbi mértéket felülmúlóan alakították a politikai folyamatokat – ahogy arra a 2016. július 15-i török puccs kudarca vagy akár az amerikai Demokrata Párt szervereinek feltörése, majd a kompromittáló információk kiszivárogtatása is rávilágít. Az információs térben zajló globális konfrontáció folyamatos fenyegetést jelent, ennek felismerése azonban nem elég az információs agresszió elleni hatékony védelem megteremtéséhez. Ahhoz elsőként nemzetközi összefogásra, a nemzetbiztonsági szolgálatok megerősítésére, valamint a közvélemény bizalmának visszanyerésére lenne szükség.

Ezen túl a tartós védelem elengedhetetlen feltétele a szemben álló fél stratégiai szándékainak és kártékony tevékenységeinek korai feltérképezése, majd az erről szóló hiteles információk megfelelő formában történő továbbítása a közvélemény irányába a hatékony stratégiai kommunikáció részeként. Egyelőre azonban úgy tűnik, hogy néhány technikai jellegű próbálkozáson túl – ezek közé tartozik az álhírek jelenlétét célzó megoldások bevezetése a közösségi oldalakon – a társadalom megosztottsága és a feszültségek csak tovább növekednek a mindent átfogó és egyre erősödő információs konfrontáció árnyékában.

[27] Az utóbbi időszakban – online persona management service néven – olyan automatizált szoftverek is kifejlesztésre kerültek, melyek segítségével egy operátor egyszerre több felhasználói fiókot tud szimultán kezelni, biztosítva a vélemények gyors és hatékony befolyásolását. A témáról részletesebben lásd: Paganini Pierluigi: PsyOps and Socialbots. Infosec Institute, 2013.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

FELHASZNÁLT IRODALOM

1. Armistead, Edwin L.: Information Operations: The Hard Reality of Soft Power. Potomac Books, 2004.
2. Billion dollar race: Soviet Union vied with US in ‘mind control research’. RT News, 2013. https://www.rt.com/news/psychotronic-arms-soviet-weapon-379/ (Letöltés ideje: 2018. 06. 20.)
3. Chekinov, S. G., Bogdanov, S. A.: The Nature and Content of a New-Generation War. *Military Thought: A Russian Journal of Military Theory and Strategy,* 2015.
4. Chekinov, S. G.,Bogdanov, S. A.:“Влияние непрямых действий на характер современнойвойны”(The influence of the indirect approach on the nature of modern warfare). *Voyennaya mysl,* 2011. No. 62011 3.
5. Fitzgerald, Mary C.: Marshal Ogarkov on the modern theater operation. Naval War College Review No. 4, 1986.
6. Fitzgerald, Mary C.: Russian Views on Electronic and Information Warfare, Hudson Institute, 1996. http://www.agentura.ru/text/biblio/view.txt (Letöltés ideje: 2017. 01. 14.)
7. Geers, Kenneth: Cyberspace and the Changing Nature of Warfare. *SC Magazine,* Black Hat, 2008.
8. Geraszimov, Valerij: Cennoszty nauki v predvigyenyi. *Vojenno-promislennij kurjer,* 2013, Vol. 8 No. 476. http://www.vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf (Letöltés ideje: 2015. 11. 25.)
9. Giles, Keir: Handbook of Russian Information Warfare. Research Division NATO Defense College, 2016 https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Letöltés ideje: 2017. 01. 12.)
10. Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése. *Hadtudomány,* 21 (2011/1–2).
11. Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.
12. Heickerö, Roland: Emerging Cyber Threats andRussian Views on Information Warfare and Information Operations. FOI Swedish Defence Research Agency Defence Analysis, 2010.
13. Kramer, X. H., Kaiser T.B., Schmidt S. E, Lefebvre V. A.: From Prediction to Reflexive Control. *Reflexive processes and control International Interdisciplinary Scientific and Practical Journal,* 2003, Vol. 2 No. 1.
14. Mansfield, Katie: Europe ready for CYBERWAR over fears Russia will hack Germany, France and Netherlands vote 2016. express.co.uk. www.express.co.uk/news/world/742875/europe-cyberwar-russia-hack-germany-france-netherlands-elections (Letöltés ideje: 2017. 01. 14.)
15. Négyesi Áron: Az orosz haderőreformok eredményei a haderő-szervezet és a személyi állomány tekintetében. 2013, Biztonsagpolitika.hu. http://old.biztonsagpolitika.hu/documents/1370375838_NEGYESI_Aron_Oroszorszag_haderoreform_-_biztonsagpolitika.hu.pdf (Letöltés ideje: 2017. 01. 14.)
16. Paganini, Pierluigi: PsyOps and Socialbots. Infosec Institute, 2013. resources.infosecinstitute.com/psyops-and-socialbots/ (Letöltés ideje: 2016. 11. 10.)
17. Rácz András: Az orosz haderőreform rövid áttekintése. MKI-tanulmányok T-2008/31.

18. Thomas, Timothy L.: Manipulating The Mass Consciousness: Russian And Chechen "Information War" Tactics In The 2nd Chechen-Russian Conflict. In: Foreign Military Studies Office, Fort Leavenworth, KS., 2000. fmso.leavenworth.army.mil/documents/chechiw.htm (Letöltés ideje: 2018. 01. 15.)
19. Thomas Timothy L.: Information Warfare in the Second (1999–) Chechen War: Motivator for Military Reform? In: Aldis, Anne C. (szerk.), McDermott, Roger N. (Ed.): Russian Military Reform, 1992–2002 (Soviet (Russian) Military Experience). Routledge, 2003.
20. Thomas, Timothy L.: Comparing US, Russian, and Chinese Information Operations Concepts. Fort Leavenworth, KS., Foreign Military Studies Office, 2004.
21. Thomas, Timothy L.: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies*, 2014.