УДК 355.40

ИНФОРМАЦИОНО РАТОВАЊЕ У САВРЕМЕНОЈ ВОЈНОЈ ТЕОРИЈИ И ПРАКСИ

Милан Миљковић
Министарство одбране Републике Србије

Информација ће и у будућности имати критички значај за војни успех. Да би САД доминирале у глобалном информационом спектру извршиће се трансформација и сврставања информационих операција у централне и главне по важности војне операције које изводе ОС САД, заједно са копненим, ваздушним, поморским и специјалним операцијама. Информационе операције дефинишу се као координисана примена активности које се предузимају против информација и информационих система непријатеља, уз чување властитих. Основни циљеви су: утицај, прекидање или наношење неисправности противничком „људском“ или аутоматизованом систему за руковођење. Централне активности информационих операција су: психолошке операције, војно обмањивање, заштита операција, електронско ратовање и рачунарско-мрежне операције.

Крајњи циљ информационог ратовања је информациона супериорност, која је дефинисана као оперативна предност добијена из могућности прикупљања, обраде и дистрибуције непрекидног тока информација при експлоатисању или онемогућавању противника да има те исте могућности. Утицај на процес одлучивања код противничког руководства, процес који се популарно назива „петља – посматрај, оријентиши се, одлучи и делуј“ („*OODA-loop*“; *observe, orient, decide, act-loop*), један је од задатака информационих операција. Смањивањем противничке способности да донесе правовремену и ефикасну одлуку умањиће противнички одговор или иницијативу према војној акцији коју спроводе савезничке снаге.

Кључне речи: *информационо ратовање*, *информационе операције*, *војна теорија и пракса.*

Увод

По наводима америчког теоретичара Тофлера, последња декада двадесетог века била је прелаз из индустријског у ново „треће доба“, информационо доба, чије су основне карактеристике да је „информација“[1] средишњи потенцијал светске производње и војне моћи, да се светска производња темељи на власништву и монополу над информацијама и да се сукоби темеље на геоинформацијским надметањима. Информација постаје стратегијски ресурс. Енглески теоретичар Филип М. Тејлор са Универзитета у Лидсу сматра да комуникације и информације у 21. веку имају такав значај за савремено друштво какав су за развој цивилизације у 20. веку имали нафта и угаљ.

Са друге стране, доминација у информационом спектру је неопходан услов за успех и победу у сукобу. Ставови изнети у Националној стратегији безбедности САД из 2002. године, где се наводи да четири основна стуба америчке међународне моћи представљају дипломатска, војна, економска и информациона моћ (познато као парадигма *DIME – Diplomatic/Political, Informational, Military, Economic*), такође указују да информације постају све важније за националну безбедност уопште, посебно, у оружаним сукобима.

Данашње „информационо доба“ доноси промене и у теоријским разматрањима о елементима националне моћи и националној безбедности држава. Раније је војна моћ била доминантан фактор по којем се упоређивала међусобна моћ појединих земаља. У Националној стратегији за безбедност САД из 2002. године наведено је да четири основна стуба америчке међународне моћи представљају дипломатска, војна, економска и информациона моћ (познато као парадигма *DIME – Diplomatic/Political, Informational, Military, Economic).* Може се приметити да се у западној теорији све више говори о седам елемената националне моћи, у којој се поред четири наведена уводе и три нова елемента: финансије, обавештајна делатност и привржености закону (*Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement – DIMEFIL*). Наведено указује да информативна и обавештајна делатност добијају све значајније место у изградњи националне моћи савремених земаља. Један од разлога за наведено „померање тежишта“ и масовно коришћење информативне сфере као оружја у савременом добу је чињеница да су савремена достигнућа у области технике, медија и комуникације постала доступна и сиромашним земљама. Те нове околности доприносе могућности уједначавања конкурентних, али и јачих и слабијих земаља у међусобном надметању. То може да доведе до „поништавања“ војног принципа масе, тј.

[1] Информација (лат. *informatio*) – поучавање, упућивање, упутство, обавештавање, обавештење, распитивање, обавештеност, обавест, извештај, извешће, судско извиђање, истрага; Вујаклија, Лексикон страних речи и израза, Просвета, Београд, 1980, стр. 363.

до тога да војна моћ више није пресудна у одмеравању укупне моћи између две или више држава. Оружја информационог доба помажу малим нацијама против великих и фаворизирају „слабе“ у односу на „јаке“. На наведено посебно указују такозвани сајбер напади неформалних група на значајне војне и индустријске информационе системе „великих земаља“, као што су САД, В. Британија, Немачка. Зато, на уласку у ново информационо доба осмишљавање правилне националне стратегије безбедности може имати велики утицај на коначни исход савремених сукоба.[2]

У уводу доктринарног документа који је издало Министарство одбране САД 2003. године, под називом „Путоказ за информационе операције“ (*Information Operation Roadmap*), изнето је неколико смерница које указују на значај информационих активности у оквиру будућих војних операција које ће изводити америчка војска. Почиње се са прогнозом да ће „информација“, која је увек била од велике важности у ратној вештини, данас и у будућности имати критичку важност за војни успех.[3] Наглашава се будући циљ САД да извођење информационих операција постане централна надлежност америчког министарства одбране, где ће министарство централизовано руководити извођењем тих активности. Основни циљ је будућа доминација САД у глобалном информационом спектру, због чега је потребно да се изврши трансформација и сврставање информационих операција у централне и главне по важности војне операције које изводе ОС САД, заједно са копненим, ваздушним, поморским и специјалним операцијама. Такође, способност брзог дистрибуирања „убедљивих информација“ противничком јавном мњењу којим се директно утиче на надлежне особе противничке стране, представља знатно увећану способност одвраћајуће агресије.

[2] Добар пример је различитост француског и немачког приступа у војној доктрини после Првог светског рата. У периоду између два рата, од 1919. до 1939. године, Француска је дефинисала стратегију предње одбране вођена својом идејом већ познате технике ратовања усавршене на крају Првог светског рата. Међутим, 10. маја 1940. године свет је гледао како је Немачка, с пуно мање ресурса, успешно вршила инвазију на Бенелукс и северну Француску. Немачка је имала добре стратешке одлуке, њен концепт блицкрига (муњевитог рата) у потпуности је искористио предности тадашње „механизације ратовања“. Док је Француска остала у старој стратегији, заснованој на искуствима из „прошлих ратова“, Немачка је, оснажена новом технологијом, развила нову, храбру офанзивну стратегију. Данас се начин на који се ратује поново мења, због нове технологије информацијског доба, па, с тим у вези, треба разумети циљеве, начине и средства концепције информацијског доба.

[3] *Information Operation Roadmap*, Пентангонов документ из 2003. године претходно је класификован као „*noforn*“, што значи – забрањено за дистрибуцију страним представницима, укључујући савезнике. Тај документ представља доктринарну визију развоја информационих операција у надлежности Министарства одбране САД. У њему се говори о психолошким операцијама, електронском ратовању, као и о „ангажовању у извештавању страних новинара“. Документ, иако са прикривеним појединостима, објавио је Архив националне безбедности САД 26. јануара 2006. године, а доступан је на сајту: www.gww.edu/nsarchiv/NSAEBB/NSAEBB/infoopsroaddmap. pdf.

Амерички поглед на информациону и националну безбедност

Основе новог погледа на теорију националне безбедности постављене су у САД почетком осамдесетих година. Проблему националне безбедности Сједињене Државе приступају из једног новог угла – са становишта заштите своје инфраструктуре. Још од деведесетих година руководећи кругови у САД су показивали забринутост због појаве нових претњи националној безбедности. После Првог заливског рата, због све чешће употребе појмова „информационо ратовање“ и „информационо оружје“, Министарство одбране издало је директиву ТС3600.1 од 21. децембра 1992. године под називом „Информациона противодбрана“ у којој је указано на неопходност вођења рачуна о информационим ресурсима при организацији планирања и функционисања система управљања ради повећања ефективности дејстава војних снага у условима противдејстава противника. Од тог времена интензивно се ради на задацима истраживања и развоја „борбе са системима управљања“ са основним циљем – остваривање информационе супериорности.

Појам информационе безбедности изведен је и заснован, пре свега, на теорији информационог ратовања, где информациона безбедност представља један од елемената подршке информационих операција. Извори претњи су: хакери, инсајдери, активисти противдржавних организација, терористи, инострани учесници информационих операција, итд.

Информациона безбедност јавља се не само као један од видова националне безбедности, већ и као пресек свих других облика безбедности у којима информационе технологије заузимају важно место. Информациона безбедност је неодвојиви део националне безбедности,[4] а дефинисана је као: заштита информационих система против неауторизованог приступа или модификација информација, било у складиштењу, обради или преносу и против лишавања услуга ауторизованих корисника, укључујући неопходне мере детекције, документовања и отклањања таквих претњи.

Елементи информационе безбедности, у контексту националне безбедности, јесу: информационо право као правна основа информационог друштва, информациони аспект управљања војним снагама и оружјем, информационо ратовање и информациона противодбрана, електронско ратовање као борба за доминацију у електромагнетном спектру, информациона без-

[4] Бошко Родић и Стеван Сикорски, „Информациона безбедност у сфери одбране, иностраних послова и унутрашњих послова“, Академија за безбедност и дипломатију, Београд 2007. године, страна 6.

бедност информационих система и заштита информација, заштита државне тајне, извиђање и служба извиђања, информационо-психолошка противодбрана и психолошко ратовање, информационо-психолошка безбедност и морално-психолошко обезбеђење становништва, оружаних снага и других војних организација.[5]

Информациона супериорност

Америчка теорија информационог ратовања (*information warfare – IW*) подразумева концепт информационе превласти, односно информационе супериорности. Крајњи циљ информационог ратовања је, у ствари, информациона супериорност (*IS – information superiority*), која је дефинисана као оперативна предност добијена из могућности прикупљања, обраде и дистрибуције непрекидног тока информација при експлоатисању или онемогућавању противника да има те исте могућности.

Информациона супериорност постиже се путем неколико активности. То су: информациони менаџмент (ИМ), обавештајна делатност, осматрање и извиђање и информационе операције.

Информационо окружење

Све информационе операције реализују се у оквиру много ширег контекста који се назива *информационо окружење*. Наведено окружење препознаје критичну улогу феномена информације и информационих система у данашњем друштву информационог доба. То окружење прожима и превазилази границе копна, мора, ваздуха, свемира и сајбер простора. У оквиру информационог окружења постоје три концептуалне димензије: физичка, информациона и сазнајна.

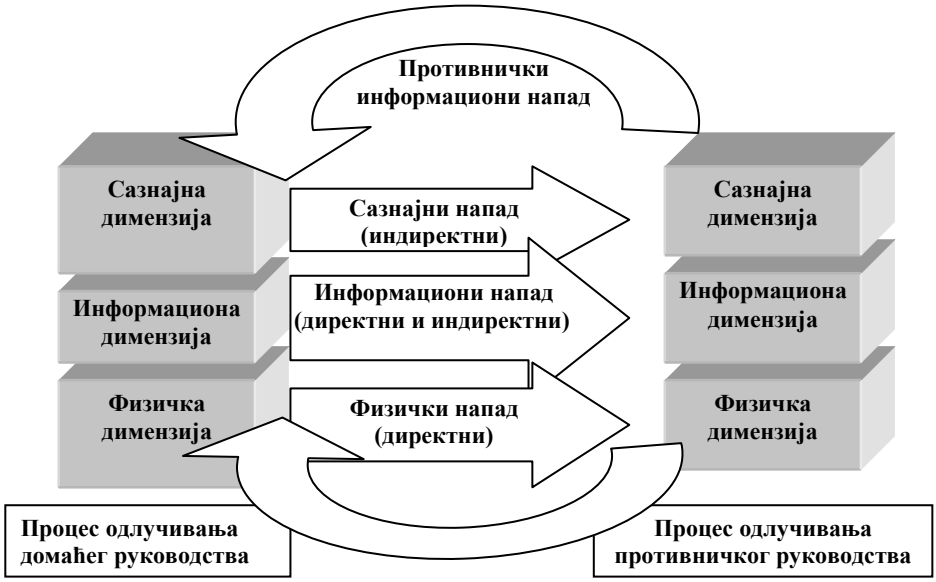
Информационо окружење је и скуп појединаца, организација или система за прикупљање, обраду или дистрибуцију информација.[6] Употреба информација експоненцијално расте са развојем друштва. Савремено информационо окружење се манифестује кроз информациону инфраструктуру, која може бити глобална, национална и војна.[7]

[5] Бошко Родић и Стеван Сикорски, „Информациона безбедност у сфери одбране, иностраних послова и унутрашњих послова“, Академија за безбедност и дипломатију, Београд, 2007, страна 7.

[6] Правило: ФМ-100-6, FM 100-6 *Information operations, Department of the Army*, Washington, DC, 1996. године.

[7] (GII, NII, DII – global, national, defense information infrastructure, Правило JP 3-13, 1998).

Слика 1 – *шема „Информационог окружења“*
(извор: Joint Publication 3–13 „Information Operations“, 13. фебруар 2006, страна I–2)



Слика 2 – *шема информационог окружења*
(извор: „Information Operations Primer“, U. S. Army War College, Dept. of Military Strategy, Planning, and Operations & Center for Strategic Leadership, децембар 2007)

Појам и намена информационих операција

Информације постају све важније за националну безбедност уопште, посебно у оружаним сукобима. Иако се још увек, гледано кроз застарелу призму, региструју само војни сукоби, свакодневно се воде технолошки, економски, информациони, обавештајни, верски, психолошки, дипломатски, спортски и други ратови, на различитим нивоима. Тиме се врши померање тежиште рата са војне на друге сфере и делатности, као што су информативна и обавештајна. Савремени сукоб је незамислив без великог броја информација о противнику, сопственим снагама, простору и времену. Савремене оружане снаге се врло много ослањају на најновија технолошка достигнућа на пољу информационе технологије. Међутим, информације су постале и важан циљ за противника. Лишити противника предности које му оне пружају, обманути га лажним информацијама, пласирањем убедљивих информација умањити његову спремност на отпор, уз истовремено обезбеђење потребних информација за сопствене потребе, значи остварити знатну предност у реализацији циља на одређеном простору и за одређено време уз минимално ангажовање снага и минималне губитке. Сагласно томе, савремени сукоби су наглашено окарактерисани и као борба у сфери информација. Они који су савладали технике информационог ратовања у предности су над својим противницима.

Информациона револуција трансформише ратовање, тј. изазива промене у томе како друштва долазе у сукоб, како њихове оружане снаге воде оружани сукоб и друго. Више се не сукобљавају масивне, укопане војске у крвавим исцрпљујућим борбама. Уместо тога, мале и изузетно мобилне снаге, „наоружане“ информацијама у реалном времену добијених са сателита и сензора, обавештајних служби, ударају великом брзином на неочекиваним местима. Победник је она страна која може брже да експлоатише информације, односно, она страна која брже анализира, процењује ситуацију и реагује. Победник је и она страна која успе да противнику пласира убедљиве информације или дезинформације на основу којих ће противничко руководство донети погрешне закључке и одлуке.

Са војног гледишта, информациони простор већ дуже време се цени као борбено поље савременог глобалног друштва.[8] За разлику од индустријског доба, где су земље које су имале превласт на мору и ваздуху „владале“ светом, у информационом добу земље које доминирају информационим простором имају доминацију у свету. Основна специфичност информационог ратовања јесте да бојиште није физички, већ виртуелни свет, а потенцијални ратници на том бојишту могу бити државни органи, војне организације, терористи, индустријски конкуренти, хакери и други. Сваки од тих противника мотивисан је различитим циљевима, ограничен различитим нивоима ресурса,

[8] Дејан Вулетић, „Шта је Информационо ратовање“, Безбедност 3/'05 стр. 491, 2005.

сопственим могућностима и могућностима система да се брани. Они који су савладали технике информационог ратовања у предности су над својим противницима. Победник је она страна која може брже да експлоатише информације, односно, она која брже анализира, процењује ситуацију и реагује.

Нови начин ангажовања држава у сукобу условио је појаву нових средстава, а са њима и нових начина вођења сукоба. Један од њих је и информационо ратовање. Захваљујући ефикасности примене оно заузима све значајније место у савременим сукобима. Информационо ратовање није, дакле, нова појава. Назив се мењао временом и еволуирао да би усвојио нове технологије које представљају стратешке изазове нашим националним интересима и вредностима.

Информационе операције (*Information Operation – IO*) су дефинисане, како од цивилних стручњака за наведену област, тако и у оквиру доктринарних докумената оружаних снага западних земаља. Према Арквили и Ронфелду, информационо ратовање обухвата: 1) настојање да се о противнику сазна све и спречавање противника да зна много о вама; 2) окретање „баланса информација и знања" у сопствену корист, посебно ако не постоји баланс снаге; 3) коришћење знања тако да мањи капитал и рад могу бити увећани.[9] Сматра се да је најпотпунија и најприхватљивија дефиниција Ричарда Шафранског, према којој је „информационо ратовање активност уперена против било којег дела система знања и веровања противника. Без обзира на то да ли се води против спољњег противника или унутрашњих група, информационо ратовање има крајњи циљ да употреби информациона оружја ради промене (утицаја, манипулације, напада) система знања и веровања неког спољњег противника."

Са друге стране, документ Министарства одбране САД „*Information Operation Roadmap*" из 2003. године дефинише информационе операције као заједничке активности електронског ратовања, рачунарских мрежних операција, психолошких операција, војног обмањивања и „заштите операција" ради утицаја, прекидања или наношења неисправности противничком „људском" или аутоматизованом систему за руковођење. Слична дефиниција налази се и у нешто старијој војној доктрини ОС САД из 1998. године – *Joint Pub 3–13, Joint Doctrine for Information Operations*. Информационе операције дефинишу се као активности које се предузимају против информација и информативних система противника, уз чување властитих информација и информативних система. Оне захтевају сталну интеграцију офанзивних и одбрамбених потенцијала и активности, као и делотворно осмишљавање, обједињавање и интеракцију командовања са обавештајном подршком.

[9] Дејан Вулетић, „Шта је Информационо ратовање", Безбедност 3/'05 str. 496, 2005. година (Arquilla J., Ronfeldt D., „Мрежни рат и кибер рат", РАНД корпорација, извод из студије објављене у „Comparative Strategy", Volume 12, 1995).

Намена информационих операција јесте да се, коришћењем „информација“[10] и информационог система, утиче на понашање руководеће структуре, пре свега на надлежне особе код противника, али и на противничко јавно мњење. Супротно наведеном, информационе операције, такође, имају намену да одбране надлежне особе пријатељских земаља и пријатељско јавно мњење од прекомерног утицаја циљаних информација и информационих система противничке стране.

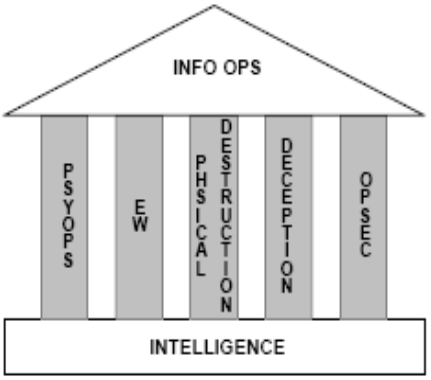
Примарни циљ информационих операција јесте противничко руководство, као и „процес одлучивања“ противничког руководства. Мете напада су: руководство противника (политичко, војно, социјално, културно), војна инфраструктура (комуникациони системи, обавештајне структуре, логистика и операције које изводи), цивилне инфраструктуре (телекомуникације, транспорт, енергетски систем, финансијски систем, производни систем) и оружани системи (авијација, бродови, артиљерија, прецизно-вођена муниција и ПВО систем). Коришћење информационих операција на домаће јавно мњење је по законима САД забрањено. Утицај на циклус одлучивања код противничког руководства, процес који се популарно назива „петља – посматрај, оријентиши се, одлучи и делуј“ (*OODA-loop; observe, orient, decide, act – loop*) такође утиче и на понашање циљних група. Смањивањем противничке способности да донесе правовремену и ефикасну одлуку умањиће противнички одговор или иницијативу према војној акцији савезника САД.

Садржај информационих операција

Америчка војна теорија, када говори о садржају информационих операција, наводи да оне представљају координиране активности пет централних и пет подржавајућих активности (способности) ради подршке командантових борбених циљева или спречавања постизања циљева противника. Те централне способности су: психолошке операције (*Psychological Operations – PSYOP*), војно обмањивање (*Military Deception – MILDEC*), безбедност операција (*Operations security – OPSEC*), електронско ратовање (*Electronic Warfare – EW*) и рачунарске мрежне операције (*Computer Network Operations – CNO*). Постоје и додатне активности које подржавају информационе операције и три повезане активности. Све заједно, те способности омогућавају командантима да утичу на ситуацију у зони своје одговорности. Да би се избегла могућност да дође до несклада између наведених активности,

[10] Под информацијама се подразумевају чињенице, подаци или инструкције у било каквом медију или облику. Човек је тај који подацима, користећи се прихваћеним конвенцима, даје одређена значења. Иста информација за друге кориснике може имати сасвим друго значење, тј. различитим прикупљачима и корисницима даје „вишезначне сигнале“.

потребна је њихова координација, синхронизација и интегрисана примена. Информационе операције се деле на две главне врсте: офанзивне и одбрамбене.[11]



Слика 3 – *НАТО правило: AJP 2.1 INTELLIGENCE PROCEDURES, март 2002., страна 3–9*

Главне активности информационих операција

Од наведених пет централних способности *ИО*, психолошке операције, војно обмањивање и безбедност операција имале су тежишну улогу у војним операцијама вековима уназад. У савременом добу, тим активностима су придодате, прво, електронско ратовање, а затим и рачунарске мрежне операције. Када се свих пет способности примене заједно са подржавајућим и повезујућим активностима, добија се основно средство команданта којим он утиче на противничку страну и друге циљне групе, чиме се омогућава слободно деловање здружених снага у „информативном окружењу".

[11] Офанзивне информационе операције подразумевају обједињену употребу формацијских и подржавајућих потенцијала и активности уз подршку обавештајног фактора, са циљем да се на противничкој страни онемогући рад особама које доносе битне одлуке и да се постигну или промовишу неки специфични циљеви. Формацијски и подржавајући потенцијали и активности обухватају: оперативну безбедност, војно обмањивање, психолошке операције, електронски рат, физички напад/уништење и специјалне информационе операције, а могу обухватити и напад на рачунарску мрежу.

Одбрамбене информационе операције обједињују и координирају политику и процедуре, операције, људство и технологију са циљем да заштите и одбране информације и информативне системе. Одбрамбене информативне операције изводе се и потпомажу кроз заштиту информација, безбедност информација, физичку безбедност, контраобмањивање, контрапропаганду, контраобавештајну делатност, електронски рат и специјалне информационе операције. Одбрамбене информационе операције обезбеђују благовремени приступ тачним и релевантним информацијама и, истовремено, противнику онемогућавају да се користи савезничким информацијама и информационим системима.

Психолошке операције (PSYOP) јесу акције чији је задатак да страном аудиторијуму пренесу одабране информације и индиције. Циљ им је да утичу на емоције, мотиве, начин размишљања и, коначно, на понашање страних влада, организација, група и појединаца.[12] *PSYOP* имају стратегијску, оперативну и тактичку примену, укључујући и активности пројектовања истине као подршку операцијама војног обмањивања. На стратегијском нивоу *PSYOP* често има облик политичких или дипломатских ставова, саопштења и комуникеа. На оперативном нивоу психолошке операције могу обухватати дистрибуцију летака, емитовање садржаја помоћу разгласа, радио и ТВ емитовање и остале облике преношења информација које подстичу противничке снаге на бежање, дезертирање или предају. Стални напади могу деловати синергички са *PSYOP*, убрзавајући осипање морала и додатно подстичући дезертерство. На тактичком нивоу, психолошке операције обухватају коришћење разгласа и осталих средстава, како би се изазвао страх и неслога у противничким редовима. Снаге *PSYOP* могу на ставове и понашање утицати и путем непосредних контаката, а могу подржавати и операције војног обмањивања.

Војно обмањивање (MILDEC) у рукама команданта здружених снага „напада на људе" који одлучују на противничкој страни и утичу на систем прикупљања, анализирања и дистрибуције информација противника.[13] Обмањивање захтева добро познавање противника и његовог процеса одлучивања. У процесу креирања концепта обмањивања посебна пажња се поклања команданту здружених снага и његовим идејама о томе како би волео да се противник понаша. Наведене идеје о жељеном понашању противника постају циљ операција обмањивања, а то је да противнички команданти стекну погрешне представе о потенцијалима и намерама савезничких снага, да се поремете противникове могућности за прикупљање обавештајних података или противникове снаге омету у коришћењу најадекватнијих борбених јединица или јединица подршке. Операције војног обмањивања саставни су део здружених операција. Планови операција војног обмањивања могу обухватати употребу јединица нижег нивоа, иако подређени команданти при том не морају знати целину операције обмањивања. Стога је изузетно важно да команданти своје планове у вези са операцијама обмањивања координирају са надређеним командантом и при том обезбеде јединство акције. Операције војног обмањивања зависе од обавештајних операција у смислу идентификације одговарајућих мета обмањивања, помоћи у развијању уверљиве приче, идентификације и нападања на праву мету и процене ефикасности плана војног обмањивања. Операције војног обмањивања су веома моћно оружје, али имају и своју цену. Ради уверљивости акције обмањивања неке снаге и ресурси морају се потпуно посветити тој операцији, занемарујући за краће време остале аспек-

[12] „Доктрина здружених психолошких операција", ЈП 3-53.

[13] „Здружена доктрина за војно обмањивање", ЈП 3-58.

те похода или операције. Операциона безбедност може налагати да у случају операција војног обмањивања само изабрана група виших команданата и штабних официра у здруженим снагама зна које су акције искључиво обмањивачког карактера. Та ситуација могла би да изазове конфузију, па је командант здружених снага и његов штаб морају непосредно пратити.

Електронски рат (*EW*) дели се на три основна елемента: електронски напад (*EA*), електронску заштиту (*EP*) електронску ратну подршку (ЕС). Сва три елемента доприносе офанзивним и одбрамбеним информационим операцијама. Електронско ратовање је свака војна акција која подразумева употребу електромагнетне и усмерене енергије ради управљања електромагнетним спектром или ради напада на противника. Електронски напад подразумева акције предузете ради напада на непријатеља са намером да се наруши, неутралише или уништи непријатељски борбени потенцијал и спречи или умањи ефикасна употреба електромагнетног спектра непријатеља.[14] Електронска заштита подразумева акције као што су самозаштитно ометање и контрола емисије ради заштите употребе савезничког електронског спектра минимизирањем ефеката савезничког или непријатељског коришћења електронског рата помоћу којег се нарушава, неутралише или уништава савезнички борбени потенцијал. Електронска подршка доприноси свести команданта здружених снага о актуелној ситуацији детектовањем, идентификовањем и лоцирањем извора намерно или ненамерно емитоване електромагнетне енергије ради моменталног откривања претње. Електронски напад требало би да се користи у складу са утврђеним принципима ратовања. Одлука о извођењу напада требало би да се доноси не само на основу укупних циљева здружене кампање или операције, већ и имајући у виду ризике од могућег одговора непријатеља и остале потенцијалне ефекте на кампању или операцију. Електронска заштита и електронска подршка се, по природи ствари, примењују, како у мирнодопско, тако и у време криза и конфликата. У име постизања максималног ефекта и смањења опасности од ометања сопствених снага и савезника, командант здружених снага требало би да обезбеди најбољу могућу координацију између електронског рата и осталих активности обавештајне и комуникацијске подршке информационе операције. Та координација је неопходна како би се добили максимални ефекти размене информација, елиминисања нежењеног дуплирања активности и обезбедила узајамна подршка.

Оперативна безбедност (*OPSEC*) доприноси офанзивним информативним операцијама тако што успорава циклус доношења одлуке на непријатељској страни и ствара прилику за лакше и брже постизање циљева на савезничкој страни. За оперативну безбедност веома је важно добро разумевање могућности којима непријатељ располаже у погледу благовременог прикупљања поузданих и адекватних обавештајних података. У комбинаци-

[14] „Електронски рат у здруженим војним операцијама“, ЈП 3-51.

ји са другим потенцијалима, *OPSEC*, када је то могуће, прикупља веома корисне информације о противниковим сазнањима и проценама у вези са нашим операцијама. *OPSEC* противнику ускраћује критичне информације о пријатељским потенцијалима и намерама које су му неопходне за ефикасно и благовремено одлучивање и тиме га чини рањивим у односу на друге офанзивне потенцијале. Од кључног значаја је што раније укључивање *OPSEC*-а у процес планирања мисије, јер се на тај начин на минимум своде показатељи који откривају пријатељске намере у вези са операцијом и, у исто време, лакше напада процес одлучивања на противничкој страни. Оперативна безбедност је процес којим се идентификују критичне информације и анализирају акције сопствених или пријатељских оружаних снага ради одређивања: које су сопствене информације потребне противнику да би супротна страна имала тачне податке о стварним намерама пријатељских снага, лишавање противничких командних структура критичних информација о намерама савезника и довођење противничког руководства до погрешне процене о стварним намерама, обезбеђујући тајност и безбедност таквих информација. С тим у вези, *OPSEC* остварује тесну координацију активности са војним обмањивањем, у лишавању противниковог стварног плана и оповргавајући обмањивачки план.

Рачунарске мрежне операције (*CNO*) једне су од најсавременијих и најмодернијих способности развијених за потребе подршке војних операција. Значај тих операција порастао је са наглим порастом коришћења умрежених рачунарских система и телекомуникационе инфраструктуре од стране војних и цивилних структура и организација. Рачунарске мрежне операције, заједно са електронским ратовањем, користе се за напад, ометање, прекид и уништење противничких информационих и рачунарских система. У војним операцијама, рачунарске мрежне операције деле се на нападне (*CAN*) и одбрамбене (*CND*) и повезане рачунарске операције за експлоатацију (*CNE*). Рачунарске операције за експлоатацију омогућавају извођење операција и обавештајно прикупљање података преко рачунарских мрежа, са циљем да се из противничких база података прикупљају подаци.

Операције за подршку информационе операције

Активности које подржавају информационе операције су: информациона поузданост, физичка безбедност, физички напад, контраобавештајне активности и активности „борбених камера“.

Информациона поузданост (*Information Assurance – IA*) дефинише се као мера која се спроводи ради заштите и одбране информација и информационог система, обезбеђујући њихову расположивост, интегритет, аутентичност, поверљивост и неодрицљивост.

Физичка безбедност је онај део безбедности који се односи на примену физичких мера везаних за обезбеђење људства, спречавање неодобреног приступа опреми, инсталацији, материјалима и документима и мера везаних за обезбеђење од шпијунирања, саботажа, штета и крађа.

Физички напад може бити коришћен у подршци информационих операција, као средство за напад на противникову командну инфраструктуру ради утицаја на циљне групе. Психолошке операције могу бити комбиноване заједно са физичким нападом са основним циљем да се максимално искористи ефекат напада и да се максимално утиче на морал противника.

Контраобавештајне активности подразумевају прикупљање информација и спровођење активности ради спречавања шпијунаже, саботаже, других обавештајних активности, убистава које се спроводе под окриљем страних влада, организација, итд. Контраобавештајне активности су критичне за заштиту пријатељских информација и информационих система. Робустан безбедносни програм који обухвата информациона поузданост, физичка безбедност, физички напад, контраобавештајне активности и оперативну безбедност омогућава добре предуслове за заштиту пријатељских информација.

Јединице „борбених камера" (*Combat Camera – COMCAM*) подржавају све способности (дисциплине) информационих операција са видео материјалима и сликама, било да утичу на противника, на циљне групе или да подржавају савезничке здружене операције. Оне производе видео материјале за јединице *PSYOP*, за операције војног обмањивања, итд.

Операције које су повезане са информационим операцијама

Војне активности које су у вези са информационим операцијама су: односи са јавношћу и цивилно-војне операције.

Односи са јавношћу обухватају: упућивање тачних и благовремених информација интерној јавности у оквиру сопствене организације, екстерној публици; стварање свести о војним циљевима за време похода или операције; задовољавање потребе интерне и екстерне публике да буде информисана о походу или операцији; информисање интерне и екстерне публике о важним догађајима који са њима имају неке везе; омогућавање команданту здружених снага да путем јавних медија обавести противника или потенцијалног противника о намерама и потенцијалима пријатељских снага.[15] Активности у домену односа са јавношћу не смеју се користити као потенцијал војног обмањивања или дезинформисања било интерне, било екстерне публике.

[15] „Доктрина односа са јавношћу", ЈП 3-61.

Под цивилно-војним пословима подразумевају се активности које војни команданти предузимају ради успостављања и одржавања веза између њихових снага и цивилних власти, становништва, ресурса и институција на савезничкој, неутралној или противничкој територији на којој се снаге налазе. Активности у вези са цивилним пословима јесу подршка иницијативама команданата здружених снага за унапређивање односа са пријатељским страним војним снагама и цивилним становништвом. Цивилни послови, исто тако, доприносе спровођењу регионалне стратегије и дугорочних циљева јачањем потенцијала земље домаћина кроз ефикасну примену локаних ресурса у ублажавању или елиминисању нестабилности, оскудице или нереда. Цивилни послови и психолошке операције (међусобно се подржавају у оквиру цивилно-војних операција – *CIMIC*). За време нератних војних операција *PSYOP* подржава разне активности из домена цивилних послова (нпр. успоставља мере управљања становништвом како би изборио подршку за владу земље домаћина у редовима међународне заједнице и, истовремено, смањио подршку и ресурсе снагама које дестабилизују и представљају претњу легитимним процесима којима руководи влада земље домаћина. Људство и снаге за извођење цивилних операција могу саветовати команданте о најбољим начинима да се војно подржи цивилна добробит, безбедност и развојни програми у пријатељској земљи или земљи домаћину. *PSYOP* максимизира поменута настојања информативном продукцијом и програмима. *PSYOP* обзнањује постојање и успех тих цивилно-војних активности како би се придобило поверење одређеног становништва и створила позитивна слика о потезима савезничких снага.

Основе руских и кинеских теоретских ставова о информационом ратовању и информационим операцијама

Руски теоретски приступи

У анализи руских ставова везаних за информационо ратовање почећемо са навођењем ставова изнетих у ауторском тексту др Андреја Лиаропулоса[16] из јануара 2003. године у којем наводи ставове руског експерта В. И. Цимбала који износи гледиште да „коришћење средстава информационог ратовања против Русије или њених оружаних снага, са становишта руских војних теоретичара, категорички неће бити третирано као невојна фаза су-

[16] Др. Андреј Лиаропулос, Russia's Approach to Information Operations, January 2007, www.rieas.gr/

коба“, без обзира на то да ли ће током могућег напада доћи до жртава или не. Када се процењују могућности да дође до катастрофалних последица стратегијског информационог ратовања од стране противника, било на економију Русије, борбени потенцијал оружаних снага или командни систем, Русија задржава право да прва употреби нуклеарно оружје против оружаних снага противника за информационо ратовање, као и против противничке земље у целости.

Руски војни теоретичари сматрају да „информација“ представља важан фактор који може бити искоришћен у постизању политичких циљева, али и циљева после завршетка војних операција. Сматрају да се информационе операције спроводе не само информационо-техничким средствима (нападом на критичне објекте националне инфраструктуре, сајбер нападима), него и информативно-перцептивним методама (пропагандом, управљањем перцепцијом противника, дезинформацијама, психолошким операцијама и обманом).[17]

У разматрању војно-технолошког аспекта информационих операција сматрају да је Русија способна да се такмичи са САД у одређеним областима, и у том смислу треба да прати асиметрични приступ. Посебно се наглашава да у примени *ИО* треба да се комбинују, како еволуционални, тако и револуционални алати. Тежиште треба да буде на извиђању и командно-контролним системима, посебно на оперативним и тактичким нивоима. Главни приоритет у развоју новог информационог оружја треба да буде на унапређењу вођеног оружја и оружја на бази електромагнетне енергије, сајбер оружју и невидљивим беспилотним борбеним платформама. Иако руски стручњаци сматрају да је развој војно-техничке компоненте у оквиру трансформације оружаних снага веома важан за сустизање западних оружаних снага и њихових борбених способности, такође усмеравају тежиште на „меку димензију“ информационог рата, тј. на психолошки и пропагандни аспект.

Мека димензија информационог рата ушла је у сферу интересовања руских војних и безбедносних стручњака из неколико очигледних разлога. Слободан прекогранични проток информација и људи пружио је могућност да многи појединци и организације из Русије дођу у додир са новим идеолошким и политичким ставовима и информацијама, што раније није био случај. Таква револуционарна промена може да има социо-политичке импликације у смислу обликовања домаћег јавног мњења и чувања унутрашње безбедности.[18] Руски војни научници већ дуже време изучавају потенцијал информационих операција да утичу на систем вредности, емоције, веровања

[17] Timothy L. Thomas, ‘Russian Views on Information-based Warfare’, Airpower Journal (Special Edition 1996), pp. 25–35, and Timothy L. Thomas, ‘The Russian Understanding of Information Operations and Information Warfare’ in Alberts, David S. and David S. Papp (eds), Volume III of Information Age Anthology: The Information Age Military (Washington DC: DoD, C4ISR Cooperative Research Program, 2001), pp. 777–815.

[18] Armistead, Information Operations, p.191.

циљних група (традиционално психолошко ратовање), али и методе за утицање на објективно резоновање и процес доношења одлука војних и цивилних руководилаца. У том смислу, руска војна теорија се бави не само изучавањем могућег утицаја информационог оружја на рачунарске системе и процесе него и на могући информациони утицај на људски ум.[19]

Енглески стручњак Тимоти Томас,[20] који се детаљно бави наведеном темом, указује да такав став има не само практични него и културолошки разлог.[21] Неки руски теоретичари изражавају сумњичавост према америчком концепту информационог ратовања. Оцењују да се амерички концепт информационог рата може упоредити са трком у наоружању којом су од краја педесетих до деведесетих година САД изнуриле руску економију. Сматрају да и новим концептом САД жели да наведе руску страну да знатно улаже у скупо оружје за информационо ратовање, како би се руска економија поново изнурила.[22] Према наведеној оцени, стању војног буџета и садашњој техничкој опремљености оружаних снага, сматрају да Русија није способна, бар у актуелном тренутку, да изврши високотехнолошку војну револуцију у оружаним снагама, еквивалентну америчкој. С тим у вези, Русија би требало да се определи на развој меке димензије информационих операција. Та опција има упоришта у ранијој совјетској војној теорији и пракси, при чему се има у виду да су совјетске оружане снаге имале велико искуство и дугу традицију у проучавању вештине управљања перцепције противника на тактичком и оперативном нивоу, како ради обмањивања, тако и ради дезинформисања противника.

Информационо ратовање и информационе операције до сада је дефинисало неколико руских аутора. У књизи која је изашла 2003. године, под насловом „Увод у формалну теорију информационог ратовања“, руски експерт С. П. Расторгујев дискутује о концепту информационог ратовања. Његов концепт се сматра значајним у руским круговима, јер је исти стручњак аутор књиге под називом „О информационом рату за Савет безбедности Руске Федерације“, што указује на то да је Расторгујев веома утицајан теоретичар у овој области. Он дефинише информациони рат као „сукоб између држава у којем се ексклузивно користи информационо оружје, и то у сфери информационих модела“. Коначни циљ који се жели постићи јесте стицање

[19] Armistead, Information Operations, p.196.

[20] Timothy L. Thomas, Comparing US, Russian and Chinese Information operations conceptr, Foreing Military studies office, Fort Leaverton, Cansas, 2004., www.dodccrp.org/events/2004_CCRTS

[21] Timothy L. Thomas, 'Russian Information-Psychological Actions: Implications for U.S PSYOP', Special Warfare, 10, 1 (1997), pp.12-19 and Timothy L. Thomas, 'Russia's Reflexive Control Theory and the Military', Journal of Slavic Military Studies, 17, 2 (2004), pp. 237–256.

[22] Timothy L. Thomas, Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations (Fort Leavenworth: Foreign Military Studies Office, Center for Army Lessons Learned, September 1998), p.1.

сазнања о одређеном информационом систему и касније намерно коришћење тог сазнања за модификацију или уништење модела света (окружења) противника. Наводи да информатичко оружје може бити техничко, биолошко или друштвено средство које се користи за намерну производњу, преношење, презентовање или блокирање података и процеса који су повезани са базом података.[23]

По Расторгујеву, информационо оружје треба да има следеће карактеристике: мора бити коришћено према противничком циљу са максималном брзином у односу на другу врсту оружја, треба да проузрокује потребну штету противнику у одређеном периоду, да буде довољно јефтино и једноставно за производњу, да је упоредиво са другим врстама оружја у сличној класи, као и да је могућа његова масовна производња[24]. Расторгујев дели теорију информационог ратовања на две компоненте, информативно-техничку и информативно-психолошку, што је другачије него што је наведено у америчким доктринарним документима. Таква подела је, на пример, наведена у Војној доктрини Руске Федерације из априла 2000. године, као и у војном часопису *Информациона безбедност* из 2000. године. У каснијим издањима наведеног часописа, информативно-технички аспект и средства подељени су на техничко-обавештајна средства, средства и мере за заштиту информација, супер високофреквентна оружја, ултрасонична оружја, радиоелектронске контрамере, електромагнетно импулсно оружје и специфичне софтвере и хардвере. Информативно-психолошки аспект укључује употребу масмедија, употребу несмртоносног оружја, психотронично оружје и специфична фармаколошка средства.

Октобра 2003. године у брошури под називом „Ургентни задаци за развој оружаних снага Руске Федерације“ истиче се да информационе операције представљају претњу по безбедност Русије и њених савезника. Такође, у престижном војном часопису *Војна мисао*, у 2003. години, аутор С. А. Богданов напомиње да се савремени сукоби воде истовременом применом војних, економских, информативно-техничких и информативно-психолошких средстава. У журналу поморских снага *Morskoy Sbornik*, (октобар 2003), официр у пензији Р. Бикеин напомиње да је информациони рат постао једна врста „војне уметности“ где се офанзивни и дефанзивни актери ангажују на утицају на интелект цивилног становништва и припадника оружаних снага противника. Бикеин дефинише информационо оружје као средство за елиминисање, мењање или узимање (крађу) информација ради прибављања потребних података после „уласка“ у информациони систем противника; блокирање приступа информацијама легитимним корисницима, и, коначно, дезорјентацију свих средстава друштвене подршке, укључујући и против-

[23] S. P. Rastorguyev, An Introduction to the Formal Theory of Information Warfare, Moscow 2003, p. 6, 7.
[24] Ibid., pp. 7, 8.

ничку војну инфраструктуру.[25] Овде се примећује да Бикенин користи појам дезорганизације уместо појма информационе супериорности. Он даље разлаже информативно-технички аспект информационих операција и наводи да се састоји од: дезинформисања, обмањивања, обавештајног рада, криптографије и стенографије. Говорећи о информативно-психолошком аспекту, Бикенин износи да и цивилна популација и припадници оружаних снага представљају мете тих активности. Наводи да се такве активности спроводе коришћењем масмедија (штампе, радија и телевизије), преко летака, религиозне пропаганде, а посебно преко интернета. За Бикерина интернет може да се користи и у информативно-техничком и информативно-психолошком аспекту информационих операција.

Интересантно је да су, анализирајући документ Министарства одбране САД *Information Operation Roadmap*, руски војни експерти изнели оцену да је америчко руководство тим документом указало да у САД постоји политичка одлука да се у будућности одвраћању претње мирним путем од стране потенцијалног противника да предност у односу на решавање сукоба оружаним путем.

Кинески теоретски приступи информационом ратовању

Када се сагледају радови кинеских војних теоретичара, поготово оних који су публиковани у последњих 15 година, долази се до закључка да Кина поклања велики значај информационом рату и његовој улози у трансформацији Народноослободилачке војске Кине (НОВК) из механизоване и једну „информатизовану“ војску. Познати западни теоретичар Тимоти Томас наводи да је је 6. августа 2003. године, на састанку министра одбране Кине господина *Cao Gangchuan* са представницима локалних влада и представницима Генералштаба НОВК-а изнео да је „циљ одбрамбене реформе и изградње оружаних снага да Кина буде способна да победи у будућем информационом рату“.

Кинеске дефиниције информационог ратовања и информационих операција временом су се мењале. Један кинески стручњак тако напомиње да „се информационо ратовање води и у миру и током рата и да је то једна врста идеолошке борбе“. Он, такође, напомиње да се, са друге стране, информационе операције воде само током рата. Кина у својој теорији дефинише шест „форми“ информационог ратовања, за разлику од руског гледања које наводи две основне форме, и америчког, који дефинише 10 активности информационих операција. Током 2002. године, водећи експерт за информа-

[25] R. Bikkenin, “Information Conflict in the Military Sphere: Basic Elements and Concepts,” Morskoy Sbornik, No 10, 2003, pp 38–40 as translated and downloaded from the FBIS web site on 6 February 2004.

ционо ратовање у Генералштабу НОВК, генерал *Dai Qingmin*, у престижном листу *Кинеска војна наука,* прецизира шест форми: оперативна безбедност, обмана, рачунарско-мрежни напади, електронско ратовање, обавештајни рад и физичка деструкција.[26]

Генерал Даи је у истом листу[27] 2000. године дефинисао информационе операције као „серију операција у информационом окружењу, са војним информацијама и информационим системима као директним оперативним циљевима, и са електронским ратовањем и рачунарско-мрежним ратовањем као основном формама извођења информационе операције". У истом чланку Даи напомиње да „информациона контрола" може да буде основна тежња зараћених страна у будућем сукобу. Зараћене стране ће тежити да у будућем сукобу остваре информациону супериорност, али, како Даи напомиње, информациона контрола је само предуслов за остварења иницијативе и остварења коначне победе у сукобу. Даи наводи три карактеристике информационе супериорности: 1) то је интегрисана војна позиција и однос који може да утиче на рат у целини; 2) омогућава слободу покрета у информационој димензији; 3) води се у три димензије: а) електромагнетном простору, б) рачунарско-мрежном простору и в) у сазнајном и вредносном систему надлежних особа. Напад се изводи се на два нивоа: 1) први је ниво напад на информациони систем противника и други 2) напад на људски сазнајни систем и систем веровања и убеђења. Такав утицај на догађаје у информационој сфери може да утиче и на догађаје у физичкој сфери.[28]

Анализа доступне кинеске литературе указује на то да Кина планира да користи ИР за остварење три могућа стратешка циља, зависно од геополитичке ситуације: као средство за вођење рата, као средство за остварење победе без вођења рата или као средство за остварење стабилности своје међународне позиције кроз промоцију нових војних теорија. Тимоти Томас коментарише да ће наведене могућности за западне теоретичаре представљати константну загонетку у смислу објашњења: „Да ли се тиме Кинеска војска показује слабим тамо где је јака, или се показује јака тамо где је слаба". Он даље наводи да постоје подаци који указују на то да је НОВК већ формирала јединице нивоа бригада за вођење офанзивних и дефанзивних информационих операција. Како се наводи, у марту 2003. године, војни представници који су присуствовали „свекинеском народном конгресу" изјавили су да ће јединице за информационо ратовање ускоро бити оформље-

[26] Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," China Military Science, Feb 2002, pp 112-117 as translated and downloaded from the FBIS web site.

[27] Dai Qingmin, "Innovating and Developing Views on Information Operations", China Military Science, August 2000, pp 72-77, FBIS web site.

[28] Dai Qingmin, "On Seizing Information Supremacy," China Military Science, April 2003, pp 9-17, FBIS web site.

не. Истиче да те јединице већ имају развијано оружје за електронско ометање и електронско „бомбардовање“ способне да парализују све противничке електронске системе, укључујући интернет и војне командне системе. Томас, такође, наводи да је 4. новембра 2003. године Ђијанг Цемин позвао оружане снаге да развију јединице за информационо ратовање, како би Кина била способна да победи у будућим сукобима.

Наводи се, такође, да теорија психолошког ратовања има изузетан значај и вредност за Кину. Кинески теоретичари теже да развију и осавремене теорију и идеологију психолошког ратовања која ће се заснивати на застрашивању и која ће користити предности разлике источног и западног менталитета. НОВК планира да оформи командне структуре за психолошко ратовање, као и специјализоване јединице за *PSYOP* како би применом *PSYOP*-а у војним операцијама умањио технолошку инфериорност кинеске војске. Оно што је још значајније јесте чињеница да кинески теоретичари сматрају да модерно психолошко ратовање може да обезбеди стабилност и допринесе обликовању и изградњи шире културе мишљења о значају националне безнедности (*national-security thinking*), што доводи до закључка да су *PSYOP* операције много примењеније у миру него у рату.[29]

Може се закључити да кинески војни теоретичари сматрају да су у информационом ратовању нашли „наклоњеног“ и „компромисног“ савезника, релативно јефтиног, који би могао да Кину учини способном да сустигне Запад, како на пољу војне моћи, тако и на пољу међународног угледа и позиције. Успех у тим пољима треба да омогуће Кини да у будућности оствари стратегијски одвраћај противника или улогу потенцијалног утицајног фактора у Азијско-пацифичком региону. У примени тих активности Кина види стратегијску шансу да прескочи историјску фазу „механистичког друштва“ и уђе у фазу информационог доба.

Искуства из примене информационих операција у савременим оружаним сукобима

Информационе операције и рат у Персијском заливу

За време рата у Персијском заливу информационе операције су умногоме допринеле победи Западне коалиције над политичком стратегијом Садама Хусеина.[30] Одмах по инвазији на Кувајт Ирак је започео поход за придобијање јавног мњења у арапским земљама. Та настојања су обухватала оп-

[29] Xu Hezhen, “Focus on Psychological War.”

[30] Извор: „Вођење рата у Персијском заливу“, завршни извештај пред Конгресом, априла 1992.

тужбе на рачун кувајтске владајуће породице и представљање Ирака као лидера у борби против колонијализма, за социјалну правду, арапско јединство, палестинску ствар и ислам. У намери да ублажи међународну осуду инвазије Кувајта Садам је неистинито објавио да ће ирачке јединице почети да се повлаче из Кувајта 6. августа 1990.

Земље Залива су, упркос претњама Садама Хусеина, уз помоћ САД, формирале Коалицију. Арапске земље нису „стале" на страну Садама, а Израелци су се уздржали под претњом напада „скадова", што је „минирало" Садамов план да Израел увуче у борбу и рат претвори у арапско-израелски сукоб. Коалиционо руководство је агресивно одговарало на Садамове претње масовним жртвама и отмицама које су добиле велики публицитет и није дозволило да буде одвраћено од својих намера. Садамов покушај да преузме иницијативу употребом „скадова" и нападом на саудијски град Ел-Кафжи, није постигао стратегијски циљ: да умањи решеност Коалиције да се бори. На информационим фронтовима, коалициона ефикасна употреба информационих операција против Садамове информационе стратегије обезбедила је не само да Ирак буде побеђен, већ и да не буде у могућности да предузме било какву иницијативу.

Обмањивање и операциона безбедност у „Пустињској олују"

„Пустињска олуја" је показала ефикасност интегрисане употребе операционе безбедности и обмањивања у формирању ставова противничког команданта и постизању изненађења.[31] Активности у оквиру обмањивања *(MILDEC)* и операционе безбедности *(OPSEC)* комбиноване су са циљем да Садам Хусеин поверује да је намера Коалиције да главну офанзиву изведе коришћењем копнених и поморскодесантних снага у централном делу Кувајта и одврати му пажњу од стварних намера коалиционих снага да са западне стране заобиђе ирачке одбрамбене снаге у Кувајту и главни напад изведе у самом Ираку. Процес планирања операционе безбедности показао је да се припреме коалиционих снага за копнену офанзиву не могу сакрити од ирачке обавештајне службе. Зато је израђен план да се започне са припремама у области Саудијске Арабије, што би било логично за напад на Кувајт. Ваздушни напади су искоришћени за заваравање већине ирачких обавештајаца и истовремено су снаге тајно пребачене на запад ради извођења главне копнене офанзиве на Ирак. Као подршка тог плана, обмањивањем су створене лажне, а операционом безбедношћу прикривене или измењене праве индиције стварних намера. Све је то допринело да Садам Хусеин закључи да ће Коа-

[31] Извор: Одељење за специјалне техничке операције при здруженом штабу.

лиција напасти преко Кувајта. Примењене мере обмањивања обухватале су емитовање хуке тенкова и артиљеријског оруђа преко звучника, као и симулирање радио-комуникација са старих локација јединица. Мере операционе безбедности обухватале су пружање могућности неким ирачким обавештајцима да виде неке аспекте коалиционих припрема за прави подржавајући напад на Кувајт и организовање веома интензивног патролирања у том сектору. Поморскодесантне снаге, лоциране на извесној удаљености од обале, имале су задатак да спроводе и обмањивање и операциону безбедност. Америчка централна команда се надала да ће задатак тих снага бити само да ирачку пажњу задрже на Кувајту, мада су оне биле спремне да у случају неуспеха обмањивања буду ангажоване у стварној акцији.

Примена јавне дипломатије и PSYOP у операцији „Ирачка слобода“

Данас, после 11. септембра, из „Беле куће“ (*White House Office of Global Communications*) усмеравају се активности јавне дипломатије, ради објашњавања и стварања позитивне међународне перцепције о америчкој политици и одбрамбеним активностима. Амерички Национални савет за безбедност и политику координира поруке и политику између Беле куће, Одељења за јавну дипломатију и Пентагона. Та тела су заједно подржала до сада највише финансирано тело за управљање перцепцијом на стратегијском нивоу. Тело, које је основано још 1987, сада је фокусирано на исламски свет и има буџет од 750 милиона америчких долара само за регион Блиског истока.

Упркос том великом напору, резултат јавне дипломатије САД у арапском свету, у вези са операцијом „Ирачка слобода“, био је врло слаб. Један од инструмената за повећање утицаја на арапски свет остварио је *Radio Sawa* (Радио „Заједно“), који је финансирао амерички конгрес. Та радио-станица емитовала је и арапску и поп музику, као и вести из америчке перспективе. Већ после једне године емитовања (основана је 2002. године) показала се као најомиљенија међу младим арапима. Током похода на Ирак Коалиција је намеравала и да обликује општи поглед и перцепцију о сукобу, користећи и „уграђивање“ новинара у војне јединице које су биле ангажоване, што се показало као добар потез, јер су се, после одређеног времена, ти новинари везивали за те јединице, а извештаји су добијани у реалном времену. Један од фактора који поткопава идеју „светског глобалног става“ о неком проблему јесте и појава пролиферације ресурса за вести (*proliferation of news sources*). Повећан број сателитских телевизијских вести и станица и интернет веза створило је чак и сложенију ситуацију да се глобално утиче на мишљење људи, па чак и регионално.

Док је стратегијско коришћење јавне дипломатије донело помешане резултате, коришћење *PSYOP*-а у операцијама у Ираку и на тактичком нивоу били су ефикаснији. Коришћење медија, као што су радио, леци, и-мејлови усмерени према одређеним циљним групама као што су кључне надлежне особе, коришћење возила са звучницима током војних операција, итд. имали су важан утицај. Више од 40 милиона летака бачено је на Ирак пре првог напада 20. марта и још толико током кампање. Поставља се питање да ли су ирачки војници савладани као резултат америчког *PSYOP*-а, као резултат бомбардовања коалиционе авијације, због слабе логистике или као резултат комбинације сва три чина. Претпоставка коалиционих снага да ће „употреба масовне војске и прецизне муниције шокирати и уздрмати ирачки режим" који ће се срушити као кула од карата био је погрешан. Уочена погрешна процена натерала је конвенционалне америчке трупе да промене свој приступ и да натерају њихове *PSYOP* снаге да промене и преиспитају њихове „теме и поруке", на оне које које ће се више заснивати на сталним и непрекидним применама *PSYOP* продуката, а не „једним снажним који ће одувати непријатеља". Поред летака, коришћен је и радио-програм емитован са фиксног места, као и са специјалног EC-130E *Commando Solo*. Емитовањем радио-програма *Radio Sawa* и *Radio Nahrain* (Две реке), коалиционе снаге су желеле да електронски пригуше Ирачки радио режима Садама Хусеина.

Сукоб у Чеченији и информациони рат

Сукоби у Чеченији обилују примерима који описују оба аспекта информационог рата – и информационо-техничког и информационо-психолошког. Руски аутор В. В. Панченков описује узрок руског „пораза" у информационо-психолошком рату током првог оружаног сукоба (1994–1996) у Чеченији и упоређује га са сукобом у Чеченији током 1999. године. Панченков наводи да током првог сукоба руски медији нису били под државном контролом и да су их у много случајева финансирали Чечени. Руско министарство одбране није новинарима ни домаћем јавном мњењу давало своје официјалне информације. Генерал Армије Махмут Гарејев износи запажања да у наведеном информационом вакууму и недостатку званичних руских ставова и вести, руска армија није била у стању да нормално функционише и да је била „морално побеђена" од својих противника на медијском фронту. Информационо-психолошки утицај на чеченске паравојне јединице био је неефикасан. Са друге стране, у другом сукобу, руска страна је формирала два информациона центра у оближњим републикама, Дагестану и Северној Осетији. Новинари су редовно били снабдевани видео материјалима и званичним информацијама руске стране. Обезбеђивана им је пратња до специфичних локација. Такође, током 1999. године руска страна је пронашла и уништила преко 150 радио-елек-

тронских уређаја и станица на територији која је била под контролом терориста. До краја септембра 1999. године, 77 радио-елекртонских уређаја је уништено у оружаним нападима, укључујући 22 од 38 радио-станица. Уништено је напајање на 18 радио-електронских уређаја. Скоро 90% радио-релејних станица противника такође је стављено ван функције.

Пример сајбер напада на Естонију као облика информационог ратовања

Средином маја 2007. године дошло је до рачунарског напада на интернет сајтове државних институција у Естонији, што је привремено парализовало рад владиних министарстава, банака и других компанија у земљи. Највећи број интернет напада догодио се 8. и 9. маја 2007. године током обележавања Дана победе у Русији и балтичким државама. Највиши естонски званичници оптужили су институције Русије за умешаност у сајбер нападе који су погодили земљу.

Као разлог напада помиње се спор са Русијом око уклањања споменика из Другог светског рата у Талину, главном граду Естоније, што се догодило неколико недеља пре изведених рачунарских напада. Такозвани напади ускраћивања услуга на интернет сајтове почели су убрзо након што су естонске власти, 27. априла 2007. године, из центра Талина уклониле статуу „Бронзаног војника“, подигнуту у част војника Црвене армије погинулих у Другом светском рату. Тај потез изазвао је протесте локалних Руса. Једна особа је погинула, а више од 150 је повређено.

Естонски званичници су тврдили да су у иницијалним нападима идентификовали „ИП бројеве“ из канцеларија руске Владе. Ипак, потврђено је да није било доказа о улози владе Русије. Русија је одбацила наведене тврдње, а независни стручњаци износе да је починиоце те врсте напада тешко поуздано лоцирати.

Мете напада нису били само интернет сајтови, него и мрежа мобилне телефоније, банкарски систем и мрежа спасилачке службе Естоније, чиме је била угрожена и економија и безбедност те земље.

По извештају стручњака, најмање милион рачунара је било коришћено у сајбер офанзиви на интернет сајтове естонских институција. Са добро успостављеним системом електронске владе и банкарских услуга, заснованих на интернету, та балтичка република сматра се врло напредном у погледу коришћења интернета. Та предност, међутим, показала се као слабост са аспекта информационе безбедности. Наведени напад представљао је велику опасност за економију земље у којој се велики број послова обавља електронским путем.

Рачунарски напад извршен је методом тзв. „*DDoS* напад“, када се сајтови „истовремено нападну“ огромним бројем посета са различитих рачунара – „бомбардовањем електронским порукама“. Стање у рачунарима при таквим

виртуелним нападима стручњаци упоређују са „лифтом регистрованим за три особе у који покушава да уђе 14 јако дебелих људи“. Владине институције и друге службе због засипања непотребним и-мејл порукама, нису биле у стању да читају своју електронску пошту, комуницирају са банкама, нити да прате вести путем рачунара. Напади су долазили са разних страна света. Естонија је реаговала тако што су за почетак онемогућене иностране посете, како би домаћи посетиоци могли да приступају сајтовима.

Као одговор на нападе, НАТО је у Талин послао своје експерте из области интернет безбедности да испитају тај случај и да омогуће заштиту од могућих будућих напада. Тренутно, НАТО не означава сајбер нападе као јасну војну акцију. Такав приступ би значио да се против земље која спроводи такве нападе не могу спровести заједничке акције самоодбране који се у војним нападима предузимају. Годину дана након сајбер напада НАТО је покренуо мере за формирање Центра за одбрану од сајбер напада у престоници Талину. Чланица НАТО – Естонија, Немачка, Литванија, Летонија, Словачка и Шпанија потписали су споразум о формалном успостављању такозваног Извршног кооперативног центра за одбрану од сајбер напада. Отварање Центра реализовано је августа 2008. године. Према договору, Центар се бави истраживањем и обуком у домену сајбер криминала. У почетку, у њему је радило 30 људи, од чега су половина бити специјалисти за рачунарску технологију из свих земаља оснивача. Сједињене Државе су саопштиле да ће се придружити пројекту као земља посматрач, док су друге земље савезнице НАТО-а слободне да се касније придруже центру.

Информациони рат у Јужној Осетији

Поред конвенционалног рата, током војних операција у Јужној Осетији, упоредо се водио и информациони рат између Русије и Грузије. Информационе операције се, поред осталог, дефинишу као активности које се предузимају против информација и информационих система противника, уз чување властитих информација и информационих система. У „грузијском случају“ циљ сајбер информационих активности руских неформалних група било је спречавање грузијске стране да међународној заједници наметне своју слику сукоба у Јужној Осетији. У том случају конкретни циљ је био да противничкој страни онемогући комуникацију преко интернета са „спољним светом“. Неформалне групе руских хакера, пре него што је почела војна операција у Јужној Осетији, блокирала је већину интернет сајтова у Грузији. Према западним војним аналитичарима, рачунарске нападне операције претходиле су војним операцијама Русије и на неки начин представљале најаву почетка оружаних сукоба.[32]

[32] Сајтови грузијске владе и медија били су срушени у ноћи 7. августа 2008, ноћ пре него што су руске трупе ушле у Јужну Осетију.

Интернет сајт грузијских вести, *www.civil.ge*, нападнут је истом методом као и сајтови у Естонији, такозваним *DDoS*-ом. Као последица напада, грузијски интернет оператери нису могли да измене садржај на својој страници и тиме пренесу међународној јавности своје виђење сукоба у Грузији. Свака вест коју су Грузини покушали да пласирају на интернету била је одбијана услед нереалног преоптерећења њиховог сервера и целог система. Проблем је превазиђен тиме што је уз помоћ *Googla* и естонских рачунарских експерата грузијски сајт *www.civil.ge* привремено премештен на другу сигурну локацију.

Закључак

У протеклих петнаест година САД, Русија и Кина развиле су концепт информационих операција и информационе супериорности који се међусобно разликују. Русија у својој теорији разматра два аспекта: информационо-технички и информационо-психолошки. Када разматрају питање информационе супериорности руски теоретичари сматрају да основу супериорности представља способност одржавања „организације" и „организованости" система. Сматрају да само када јединице постану дезорганизоване губе способност да одрже информациону супериорност.[33] Кинески експерт за информационо ратовање *Dai Qingmin* дефинише информационе операције као „серију операција у информационом простору са војним информацијама и информационим системима као директним оперативним циљевима, а електронским ратовањем и рачунарско-мрежним ратовањем као основним формама". Кина основу за теорију и праксу своје информационе супериорности види у примени „*стратагемса*"[34] и „контроли". Информационо ратовање омогућава и Кини и Русији да искористе нека научна открића Запада и уштеде новац и време и „ускоче у информационо доба" или, како кажу Кинези, „позајме мердевине да би се попели на дрво".

Амерички експерти сматрају да ће у информационом добу бити све теже да се сазна „ко или шта" напада нацију, и да ће зато комуникације постати још значајније и виталније за националну безбедност. У информационом добу постоји могућност да се маскира напад и да изгледа да је агресија извршена са места које је удаљено и другачије од места са којег је стварно напад покренут. У том смислу, за даље дограђивање знања америчке војне теорије о информационом ратовању, истиче се да је важно даље истраживање руских и кинеских метода, које би требало да открије слабости у америчком информационом и информатичком систему и то кроз процес друга-

[33] Timothy L. Thomas, Comparing US, Russian and Chinese Information operations conceptr, Foreing Military studies office, Fort Leaverton, Cansas, 2004., www.dodccrp.org/events/2004_CCRTS

[34] Кинеска древна теорија и принципи о примени војног обмањивања.

чије идеолошке призме и идеолошког оквира. Напомињу да најгору могућу грешку коју САД може да учини јесте да користи свој сопствени идеолошки и сазнајни процес за откривање слабости противника, пре свега зато што нису упознати са дијалектичким приступом у решавању проблема.

Са војне тачке гледишта савремени сукоби су наглашено окарактерисани као борба у сфери информација. Војни теоретичари информациони простор већ дуже време оцењују као борбено поље савременог глобалног друштва.[35] За разлику од индустријског доба, где су земље које су имале превласт на мору и ваздушном простору „владале" светом, у информационом добу земље које доминирају информационим простором имају доминацију у свету. Основна специфичност информационог ратовања јесте да бојиште није физички, већ виртуелни свет, а потенцијални ратници на том бојишту могу бити државни органи, војне организације, терористи, индустријски конкуренти, хакери и други. Сваки од тих противника је мотивисан различитим циљевима, ограничен различитим нивоима ресурса, сопственим могућностима и могућностима система да се брани. Они који су савладали технике информационог ратовања у предности су над својим противницима. Победник је она страна која може брже да експлоатише информације, односно, она страна која брже анализира, процењује ситуацију и реагује.

Литература

1. Вулетић, Д.: Шта је Информационо ратовање, *Безбедност* 3/'05 стр. 491, 2005.

2. Извор: Вођење рата у Персијском заливу, завршни извештај пред Конгресом, априла 1992.

3. Доктрина здружених психолошких операција, ЈП 3–53

4. Електронски рат у здруженим војним операцијама, ЈП 3–51

5. Здружена доктрина за војно обмањивање, ЈП 3–58

6. Родић, Б. и Сикорски, С.: Информациона безбедност у сфери одбране, иностраних послова и унутрашњих послова, Академија за безбедност и дипломатију, Београд, 2007.

7. Timothy L. Thomas: Comparing US, Russian and Chinese Information operations conceptr, Foreing Military studies office, Fort Leaverton, Cansas, 2004., www.dodccrp.org/events/2004_CCRTS

[35] Дејан Вулетић, „Шта је Информационо ратовање", Безбедност 3/'05 стр. 491, 2005.