УДК 355.02:004.056(497.11)
DOI:https:doi.org/10.22182/ni.4022021.5
Прегледни рад

НАЦИОНАЛНИ ИНТЕРЕС
NATIONAL INTEREST
Година XVII, vol. 40
Број 2/2021.
стр. 105-131

Милан Миљковић[1*]

Универзитет одбране Министарства одбране

Драган Јевтић[2*]

Универзитет одбране Министарства одбране,
Војна академија

СУКОБИ У ИНФОРМАЦИОНОМ ПРОСТОРУ ИЗ УГЛА САВРЕМЕНЕ ВОЈНЕ МИСЛИ У РУСКОЈ ФЕДЕРАЦИЈИ – ИСКУСТВА ЗА БЕЗБЕДНОСТ РЕПУБЛИКЕ СРБИЈЕ

Сажетак

Савремене државе, услед масовне примене информационе технологије у области комуникација, суочавају се са проблемом ефикасне контроле и заштите националне информационе сфере, а самим тим и националне безбедности. Информације се од давнина користе у манипулативе сврхе и као средство за вођење сукоба, а савремено информационо доба је само додатно актуелизовало информациони простор као борбени простор савременог глобалног друштва. Актуелизована је употреба дезинформација и лажних вести у оквиру концепта „хибридног и информационог ратовања“, као начина вођења геополитичких сукоба између великих сила, али и као средства утицаја и притиска на мале државе. С тим у вези, у раду је извршена анализа теоријског и концептуалног приступа безбедносних и војних теоретичара Руске Федерације у вези одбране од претњи из информационе

* Доцент др Милан Миљковић је наставник на Унивезитету одбране Министарства одбране у Београду. Е-пошта: milanmiljkovic04011@gmail.com

* Доцент др Драган Јевтић је наставник на Војној академији Унивезитету одбране Министарства одбране у Београду. Е-пошта: dragan.jevtic179@gmail.com

сфере. Резулати анализе указују да је теоријски приступ Руске Федерације у овој области применљив за Републику Србију која је у својим актуелним стратегијским документима из области одбране и безбедности нагласила потребу да развија система одбране од претњи из информационог простора.

Кључне речи: информационо деловање, информациони простор, перцептивна средства.

ИНФОРМАЦИОНИ СУКОБИ КАО ПРЕДМЕТ ИНОВАТИВНЕ ВОЈНЕ МИСЛИ У РУСКОЈ ФЕДЕРАЦИЈИ

Од почетка 21. века, промене у начину и методима вођења сукоба између држава постале су предмет дискусија и изучавања научне и стручне заједнице Руске Федерације. У периоду од 2000. године до закључно са првим годинама друге деценије 21. века, могу се разликовати две опште врсте војностратегијске мисли у Руској Федерацији. Прва је традиционална и конзервативна, а друга је новонастала и иновативна, која нуди другачије разумевање садржаја и метода вођења сукоба у савременом безбедносном окружењу и будућности.

Заговорници традиционалне мисли, међу којим дугогодишњи председник руске Академије војних наука, генерал армије у пензији Гареев Махмут Ахметович, иако не поричу појаву промена садржаја рата, сматрају да је преувеличана улога „невојног фактора“ у постизању коначног успеха у сукобу (Ахметович, 2003, стр. 52- 59).

Иновативни правци руске војностратегијске мисли су се у јавности појавили у првој деценији 21. века. У оквиру овог правца посебно се издваја теорија о вођењу сукоба у информационој сфери. Имајући у виду да су сукоби у информационом простору по својој суштини и пореклу војне природе, теоретичари Руске Федерације користе појам информациона дејства (рус.-*„информационная война“*) или информациона борба (Папарин, 2012).

Већина теоретичара из Руске Федерације заступа шири приступ при дефинисању и објашњавању природе информационих сукоба, наводећи да њихов крајњи циљ није

само утицај на информације, информационе системе и изворе информација противника, него и промена начина мишљења противничке стране (Rastorguyev, 2003, pp. 6- 7)

У анализи руских ставова везаних за информационе сукобе може се почети са навођењем ставова руског експерта В. И. Цимбала који износи гледиште да коришћење средстава информационих сукоба против Русије или њених оружаних снага, категорички неће бити третирано као невојна фаза сукоба, без обзира на то да ли ће током могућег напада доћи до жртава или не (Лиаропулос, 2007).

Руски војни теоретичар, политолог, пуковник у пензији Игор Панарин у својој књизи „Технологија информационог рата“ пише да у 21. веку можемо закључити да је информациони рат главно средство модерне светске политике и доминантан начин да се постигне политичка и економска моћ држава (Панарин, 2003).

Руски социолог и политички теоретичар Манојло Андреј Викторович дефинише информационо-психолошки сукоб као процес конфронтације између људских друштава усмерен на достизање политичких, економских, војних и других циљева стратегијског нивоа, офанзивним деловањем на цивилно становништво, органе власти или оружане снаге противничке стране посредством пласирања и дистрибуције специјално одабраних и припремљених информација и информативних материјала, као и ради супростављања деловању противника према сопственим ресурсима (Викторович, 2005, 73-80).

Пензионисани адмирал Владимир Пирумов наводи да су сукоби у информационом простору нови облик борбе две или више страна која се састоји од циљано оријентисане употребе посебних средстава и метода за утицај на информационе системе непријатеља и њихове изворе информација, као и заштите сопствених извора информација, а ради постизања дефинисаних циљева (Bikkenin, 2003).

Слично, теоретичар Расторгујев дефинише информациону борбу као сукоб између држава у којем се ексклузивно користе информациона средства, и то у сфери информационих модела. Финални циљ који се жели постићи је стицање сазнања о одређеном информационом систему и касније намерно коришћење тога сазнања за модификацију

или уништење модела окружења тј. информационог окружења противника (Bikkenin, 2003, 6).

За експерте из Руске Федерације информација представља важан фактор који може бити искоришћен у постизању политичких циљева али и циљева током извођења и после завршетка ратних операција.

Информациони сукоби се према руским погледима реализују у оквиру много ширег контекста који се назива *информациони простор – сфера*. Руски доктринарни документи дефинишу информациони простор (рус. информационное пространство) као област активности у вези са формирањем, стварањем, трансформацијом, преносом, употребом и чувањем информација, које имају утицај на индивидуалну и јавну свест, информациону инфраструктуру и стварне информације (Министерство обороны Российской Федерации, 2011, 5). У руским документима наводи се да се информациона сфера састоји од три елемента: од 1) информационе инфраструктуре (системи и уређаји за прикупљање, пренос, обраду и достављање информација), 2) од информација и њихових токова и 3) од персонала који обавља различите делатности. Информациона сфера је настала као последица настанка нове друштвено-економске формације друштва – информационог друштва. У оквиру информационе сфере постоје три концептуалне димензије: физичка, информациона и сазнајна.

Упоређивањем руског и западног приступа запажа се да руски експерти у својим дефиницијама истичу да се информациони сукоби обављају у доба мира и у рату. У миру, термин информациони сукоби се односе на ширу категорије активности, информациону безбедност друштва и владе у психолошком, научном, културном и производном аспекту, са посебним нагласком на заштити државних информационих извора и система и покушаја да се утиче на непријатељске информационе ресурсе. У рату, термин информациони сукоби се односе како на цивилну тако и на војну информациону сферу, кроз остваривање супериорности или смањење неизвесности, путем заштите информација, електронско ратовање, извиђање, као кроз покушаје дезорганизовања непријатеља.

Када се анализира подела информационих сукоба

према средствима извођења, руски тероретичари сматрају да се информациони сукоби, мада су у крајњем случају војни по својој природи, воде и у политичкој, економској и друштвеној сфери и да се примењују преко читавог скупа активности од значаја за националну безбедност (Синковски, 2005, 49) За руске ауторе, безбедност информационе сфере је сложен и, у својој суштини, вишеслојан проблем. Он је предмет интердисциплинарних, технолошких и хуманистичких научних истраживања. Због тога, руски теоретичари заступају став да се информациони сукоби према примењеним средствима деле на сукобе које се спроводе:

1) информационо-техничким средствима (нападом на критичне објекте националне инфраструктуре, сајбер нападима) и
2) информативно-перцептивним средствима, пропагандном, управљањем перцепцијом противника, обмањивањем, дезинформацијама, психолошким операцијама и обманом (Timothy, 1996, 25-35)

Руски теоретичар Бикенин, говорећи о информационо-психолошком аспекту, износи да и цивилна популација и припадници оружаних снага представљају мете тих активности. Наводи да се такве активности спроводе коришћењем мас-медија (штампе, радија и телевизије), преко религиозне пропаганде, а посебно преко Интернета. За Бикенина, Интернет може да се користи и у информативно-техничком и информативно-психолошком аспекту информационог сукоба (Bikkenin, 2003, 38-40)

Иако руски стручњаци сматрају да је развој информационо-техничких средстава за извођење информационих сукоба веома важан у оквиру трансформације оружаних снага Руске Федерације, као и за сустизање техничке способности западних оружаних снага и њихових борбених способности, указују да примена „меке димензије" информационих сукоба, тј. да његов информационо-перцептивни аспект, захтева много мање финансијских средстава за њену примену (Timothy, 1998, 1). У том смислу предлажу да се Русија определи на развој „меке димензије" информационих сукоба, тј. информационо-перцептивне компоненте, имајући у виду да ова опција има упоришта

у Совјетској војној теорији и пракси. Пре свега ту мисле на дугу традицију у проучавању вештине управљања перцепцијом противника, како ради обмањивања тако и у сврху дезинформисања противника.

Када се разматрају руски погледи према средствима за вођење информационих сукоба, важни су ставови Растроугјева, који наводи да средства за вођење информационих сукоба (информационо оружје) могу бити техничка, биолошка или друштвена средство која се користе за продукцију, преношење, презентовање или блокирање информација и података и процеса који су повезани са базом података. По њему, информациона средства, тј. „информационо оружје" треба да има следеће карактеристике: мора бити искоришћено према противничком циљу са максималном брзином у односу на другу врсту оружја, да може да проузрокује потребну штету противнику у одређеном временском периоду, као и да буде довољно јефтино и једноставно што би омогућило његову масовну производњу и употребу (Rastorguyev, 2003, 6-7).

РУСКИ ПОГЛЕД НА ЗНАЧАЈ ИНФОРМАЦИОНИХ СУКОБА ЗА НАЦИОНАЛНУ И ИНФОРМАЦИОНУ БЕЗБЕДНОСТ И МОЋ

Имајући у виду да је безбедност динамична категорија, искуства из употребе информационих сукоба у савременим кризним ситуацијама утичу на промене концепцијских погледа на објекте и вредности које треба да штити, на опасности које им прете, као и на субјекте и средства заштите. У теоријском погледу, поред традиционалне и превазиђене поделе компоненти националне безбедности на унутрашњу и спољну безбедност, све више је присутан концепт интегралне националне безбедности која се састоји се од више компоненти, где све значајније место заузима информациона безбедност (Мијалковић, 2009, 56).

Термин информациона безбедност се у теориским приступима и доктринарним документима из Руске Федерације користи у ширем смислу, јер се информациона безбедност везује за безбедност целокупне националне информационе

сфере, док је у америчким доктринарним ставовима реч о ужем смислу појма, јер се информациона безбедност у већини односи на безбедност важних националних компјутерских система. Овакви различити концепцијски приступи у поимању информационе безбедности последица су различитог искуства Руске Федерације са једне стране и САД са друге стране, у одбрани од спољног офанзивног информационог напада.[1]

Разматрање безбедности информационе сфере (*информационноя безопасностъ*) у радовима теоретичара у Руској Федерацији није новијег датума. Према руским ауторима, бивши СССР је изгубио хладни рат због занемаривања безбедности у информационој сфери друштва (Панарин, 1997). У информационом добу, потцењивање безбедности информационе сфере, могло би по Белаеву да доведе до непредвидивих политичких, економских, еколошких и материјалних последица, а можда чак и немира. Белаев износи да у информационом добу земље морају своје информационе ресурсе сврстати и сматрати као стратешке ресурсе истог ранга као нуклеарна средства. Руски теоретичари износе следећу дефиницију информационе безбедности: „ако је безбедност одсуство претњи или могућност поуздане заштите од њих, онда је информациона безбедност одсуство информационих претњи, или стање заштићености и стабилност основних сфера људских делатности у односу на могућа информациона дејства“ (Урсул, 2000). Информациона безбедност је у овим документима дефинисана „као стање заштићености животно важних интереса личности, друштва и државе у информационој сфери од спољашњих и унутрашњих опасности“ (Доктрина информационной безопасности Российсой Федерации, 2000).

У контексту објективних промена које је глобализација произвела након Хладног рата, посебно се може анализирати вртоглави раст светских телекомуникација и њихов утицај на моћ државе на унутрашњем и међународном плану. Све

1 САД у медијима углавном оптужују Кину и РФ за компјутерску крађу података и шпијунирање путем сајбер простора. Са друге стране Русија је много пута оптуживала САД да покушава да путем информационог рата утиче на јавно мњење у Русији током важних догађаја као што су председнички и парламентарни избори у Руској Федерацији.

већи значај се придаје „меким облицима моћи“, способности да се интересовања и мишљења других обликују у складу са одређеним жељеним културним вредностима и идејама. Из угла једне државе, мека моћ је „садржана у националној вољи, дипломатском умећу и подршци коју власт једне земље ужива у свом народу“, док шире гледано, у условима настајања информатичког друштва долази до изражаја информациона моћ (Nye 1990, 153-170).

Руски теоретичари сматрају да се информација сама по себи развила у веома важну врсту националног или стратешког ресурса за остварење националног интереса и моћи. Руски експерти сматрају да земље које поседују информациону супериорност могу бити више склоне употреби информационих средстава пре него употреби војне силе. Информациона предност подразумева да су сопствене снаге и политичко руководство, обавештени у већој мери него снаге и командни кадар противника. Информативну предност има онај ко поседује комплетаније, детаљаније, тачније и благовременије информације (Bikkenin, 2003, 38-40). Многи руски експерти верују да настајање глобалне информативне сфере омогућава многим земљама да искористе овај простор ради промене глобалне равнотеже снага. Због ових разматрања, изградња способности за вођење информационих сукоба постало је веома значајно за руске теоретичаре војне безбедности.

У савременим свету сукоби у информационом спектру користе се као средство за остварење утицаја и моћи на регионалном и глобалном плану. У вези са наведеним, Руска Федерација је предводник велике групе држава које сматрају да су информациони сукоби, облик агресије на политички и друштвени систем нападнуте државе и да као такви подлежу међународној регулацији као и оружани сукоби. По руском схватању, у информационом простору се могу предузети технолошки сајбер напади, али се могу ширити и дезинформације. Русија сматра да се свако намерно ширење информације на Интернету од стране неке стране владе са циљем подривања или рушења владе друге државе мора у међународним односима квалификовати као агресија (Младеновић 2012, 17).

РУСКИ ПОГЛЕД НА МЕСТО ИНФОРМАЦИОНИХ СУКОБА У НОВИМ РАТОВИМА

Савремени сукоби се, према руским погледима, заснивају на идеји да је ум противника главно поље војног и невојног надметања. Циљ је да се противничкој војсци и цивилном становништву наметну одлуке и активности које су у складу са интересима нападача, а на штету противничке државе. Као резултат тога, нове генерације војних сукоба су доминантно информационе и психолошке природе, јер се на тај начин постиже контрола над информационом сфером противника, депресивно психичко стање и пад морала непријатеља. Применом ових операција, смањује се потреба за значајнијим ангажовањем војних снага у нападним операцијама (Chekinov, Bogdanov, 2013).

Савремени војни теоретичари због тога указују да је главна разлика између традиционалне и „нове генерације сукоба“ концептуални прелазак: 1) са директног уништења на директан утицај; 2) са уништења противника ка његовом унутрашњем пропадању; 3) са оружаних сукоба на сукобе путем културе и информација; 4) из рата са конвенционалним снагама у рат са специјално припремљеним снагама или нерегуларним групацијама; 5) са традиционалног бојишта у три димензије у рат са информацијама / психолошким ратом и ратом перцепције; 6) од директног сукоба до бесконтактног рата; 7) из сегментних сукоба до тоталног рата; 8) из сукоба у физичком окружењу до сукоба у људској свести и у сајбер простору; 9) од симетричног до асиметричног сукоба - истовременом и усклађеном применом политичких, економских, информационих, технолошких и еколошких кампања; и 10) од рата у одређеном временском периоду до стања перманентног рата као природног стања у животу сваке нације (Berzins, 2016).

Анализирајући активности Руске Федерације, западни војни експерти закључују да руски поглед на савремене војне сукобе карактеришу следећи приципи:

– потпуно упознати и анализирати противника користећи научне методе, са циљем да се идентификују и искористе рањивости противника, посебно на стратешком нивоу,

- развити кохерентне стратегије: повезивањем свих војних (конвенционалних, иррегуларних и нуклеарних) и цивилних инструмената државне структуре, као и свих нивоа командовања (стратешки, оперативни и тактички) под јединствену националну команду која развија, примењује и прилагођава мање политике у велику стратегију,
- стратегије спроводити непредвидиво и флексибилно, прилагођавати их непредвиђеним могућностима и ризицима,
- оспоравати постојећу парадигму војних сукоба, уздржавати се од званичног проглашења почетка и завршетка рата,
- конвенционални војни сукоб би требало да траје што краће могуће, док хибридна претња може да траје непрекидно,
- користи време као стратегијску предност, употребом скривених стратегија, стратегијског прикривања и обмањивања и стратегијског изненађења,
- користи оружане снаге без ризика од стратегијског пораза. Користи војна средства за упућивање претњи и притисака према цивилним актерима противничке стране, као и за одвраћање противника од могућих војних акција, и
- тежити да се постигне доминација у информационом простору у односу на противника, и то на свим нивоима (стратегијском, оперативном и тактичком), путем примене комлексних информационих операција.

С тим у вези, високи руски војни представници истичу да је употреба информационих средстава за постизање политичких и стратешких циљева у сукоба порасла, и у многим случајевима премашила моћ силе оружја у његовој делотворности. Напомињу да информациони простор отвара широке могућности за примену метода хибридних сукоба ради смањења борбеног потенцијала јачег и богатијег непријатеља. (Gerasimov, 2013). Следеће карактеристике информационог простора погодују примени информационог и сајбер оружја у такозваном хибридним сукобима: 1)

могућност приступа са дистанце, 2) тешкоће идентификовања нападача и приписивања одговорности за напад и 3) мала цена производа високе технологије који су слободно доступни на тржишту (Миљковић, Путник, 2016, 177-178.).

„Мека димензија" информационих операција, тј. на њен информационо-перцептивни аспект (пропаганда, одмањивање и дезинформисање), захтева много мање финансијских средстава, имајући у виду да многе сиромашне земље имају дугу традицију у проучавању вештине управљања перцепције противника на нижем нивоу вођења сукоба. Информационо оружје може бити искоришћено према противничком циљу са већом брзином у односу на друге врсте (Gerasimov., 2013, 7-8). Масовност и доступност информационог оружја погодује примени концепта „народног рата" или „тоталне одбране" у хибридним сукобима.

Такође, треба се подсетити да се победа постиже не само материјалним већ и духовним ресурсима народа, његовим јединством и тежњом да се свим снагама одупре агресији. Са друге стране, деловање према противничком становништву, као једном од важнијих циљева и „центара гравитације"[2] чије расположење и понашање пресудно утиче на токове догађаја, могуће је путем многих асиметричних операција на информативном плану.

Руски теоретичари због тога закључују да ће информациони сукоби имати кључну улогу у савременим и будућим конфликтима. Циљ у наредним сукобима неће бити постигнут уколико се не постигне информациона супериорност над противничком страном. У суштини, оквир за хибридне и нелинеарне сукобе, како су представили рукси војни експерти Чекинов и Богданов, ослања се на успешној

2 Речи центар и гравитација, потичу од латинских (односно грчких) речи „centrum" и „gravitatio". У свом незавршеном делу О рату Клаузевиц је користио појмове centra gravitates и schwerpunkt за описивање концепта достизања циљева рата. Тврдио је да се из карактеристика зараћених страна развија један центар, који је извор свих снага и покрета зараћених страна и од којег све зависи, тј. који представља ону тачку на коју се усмеравају сва енергија и ресурси. Центар гравитације дефинисан је у Америчким војним долументима као оне способности или извори снаге „из којих војне снаге црпе своју слободу акције, физичку снагу и вољу за борбом" (Види шире: Драгомир Ђурић и Сретен Егерић, „Појмовно одређење центра гравитације", *Војно дело*, пролеће/2012, стр. 228-252.

примени информатионих операција на почетку сукоба како би се обликовали повољни услови за извођење војних операција. Један од њихових аргумената је да се применом ових операција, смањује се потреба за значајнијим ангажовањем војних снага у нападним операцијама (Chekinov, Bogdanov, 2013).

Руски концепт примене информационих сукоба користи војна и невојна средства, која ангажује истовремено и брзо кроз све физичке и информационе домене (просторе сукоба), кроз примену асиметричних и индиректних активности. Нападач, применом информационих сукоба, ублажава и умањује борбене могућности и спремност противника, ствара хаос, заузима виталне објекте и зоне и изолује непријатељско вођство. Иако концепт подразумева употребу конвенционалне силе, која је супериорна и чија је победа скоро извесна, њена употреба се априори не подразумева. Војни сукоб се сматра и оцењује као нежељена активност која се употребљава по потреби и за строго дефинисане циљеве и мисије. Циљ овог концепта је да тежи психолошкој победи, а не победи у физичком домену. Не жели се да војна акција има главну улогу, већ се пушта да механизми информационих сукоба остваре ефекте другог и трећег реда – фазе кампање, како би се „освојила“ подручја која су предмет сукоба.

Наведени теоријски погледи о значају информационих сукоба у новим ратовима утицали су и на конципирање стратегијских и доктринарних докумената Руске Федерације из области безбедности и одбране.

Тако важећа Стратегија националне безбедности Руске Федерације у члану 82. препознаје утицај деструктивног информационо-психолошког дејства као опасност по националну безбедност Руске Федерације (Стратегия национальной безопасности Российской Федерации, 2015). Војна доктрина Руске Федерације из 2014. године препознаје значај заштите информационог простора Руске Федерације у сврху заштите националних интереса. Посебно се у члану 12. наведеног документа, поред ширења НАТО на исток, препознаје и „коришћење информационих и комуникационих технологија у војно-политичке сврхе, противно међународном праву“. Такође, у чл.15, истиче се „сложена примена

војне силе, политичких, економских и информационих и других средства невојног карактера“ као једна од битних одлика савремених сукоба (Военная доктрина Российской Федерации, 2014).

Током децембра 2016. године Руска Федерација је усвојила нову Доктрину о информационој безбедности, замењујући Доктрину из 2000. године. Доктрина информационе безбедности Руске Федерације наводи да „обавештајне службе одређених држава повећано користе информационе и психолошке алате у циљу дестабилизације унутрашње политичке и друштвене ситуације у разним регионима широм света и угрожавања суверенитета и територијалног интегритета других држава“. Исти документ, такође, истиче борбу „против информационих и психолошких активности, укључујући и оне усмерене на омаловажавање историјских чињеница и родољубивих традиција које се тичу одбране отаџбине“ као једну од кључних области од значаја за обезбеђивање информационе безбедности Руске Федерације (Доктрина информационной безопасности Российской Федерации, 2016).

Из наведеног се може закључити да савремени стрегегијско-доктринарни документи Руске Федерације прате токове у области карактера савремених сукоба и значаја информационог и психолошког аспекта савремених сукоба.

УМЕСТО ЗАКЉУЧКА: ПОУКЕ ЗА РЕПУБЛИКУ СРБИЈУ ЗА УПОТРЕБУ ИНФОРМАЦИОНИХ ДЕЈСТАВА ЗА ОДБРАНУ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Примена информационих дејстава у међународним сукобима налази се у сталном порасту. Развијене земље успостављају националне стратегије и доктрине примене инфорамационих дејстава у којима дефинишу циљеве, снаге за њихову реализацију, као и методе офанзивног и дефанзивног деловања. Полазе од претпоставке и искуства из савремених сукоба да се жељени циљеви у садашњим односима снага могу у потпуности или делимично постићи и силом без насиља, „ненасилном агресијом“, прихватљивом

алтернативом од директне конфротације, односно једном од „најмање узнемиравајућих облика међународних конфликата“.

Примена информационих дејстава према СФРЈ, СРЈ и Републици Србији има дугорочни карактер, са великим бројем носилаца таквих дејстава како националних тако и наднационалних. Противничко деловање у информационој сфери било је један од најбитнијих фактора који су утицали на унутрашња дешавања у Републици Србији, политичке промене и безбедносна дешавања које су се десиле у нашој ближој прошлости. Анализа истраживачке грађе о догађајима за време НАТО агресије указује да је информационо дејство НАТО према СРЈ имало стратегијски значај, као и да је НАТО користио сва достигнућа у извођењу информационих дејстава, од растурања летака широм СРЈ, емитовања са стационарних, пловећих и ваздушних платформи сопствених пропагандних програма на радио и ТВ фрекфенцијама наших станица, максимално коришћење медијских гиганата, свакодневних конференција за штампу у седишту НАТО у Бриселу, формирања и слања бројних екипа за непосредно лобирање у све значајније светске земље и форуме.

Такође, анализа догађаја у периоду промене власти у Републици Србији октобра 2000. године указује да су наведени догађаји имали карактеристику „обојене револуције“ са усклађеним субверзивним активностима западних обавештајних служби, у оквиру којих су значајно место заузимале информационе и психолошке активности које су спроводиле администрације западних сила и њихове службе према тадашњем режиму и јавном мњењу у Савезној Републици Југославији, путем домаћих и страних медија (Миљковић, Тадић, 2017).

Имајући у виду да у међународном праву не постоји сагласност у вези са легалношћу употребе информационо – медијских дејстава, информационих напада у сајбер простору и контроле употребе Интернета, основано се може очекивати да ће се информациона дејства убудуће примењивати као и до сада, прилагођавајући се потребама конкретног политичког тренутка и користећи реалне могућности које јој стоје на располагању.

У „информационом добу“ информација дејства постају све важније као активност за остварење циљева националне безбедности, односно средставо за одговор безбедносним изазовима на међународној сцени. У том смислу, намеће се потреба покретања конкретних активности Републике Србије на националном и међународном плану.

На међународном плану, Република Србија би требало да, као активни члан међународне заједнице правовремено узме учешће у међународној акцији регулисања сукоба у информационој сфери. У складу са властитом позицијом у светском информационом простору, посебно у сајбер подручју, Србија би могла пође путем руског схватања да су сукоби у информационој сфери усмерени против нација облик агресије који је потребно забранити.

На националном плану треба покренути активности за доградњу стратегијских и доктринарних докумената, као и нормативних аката Републике Србије из области националне безбедности и одбране ради унапређења улоге и капацитета институција које учествују у извођењу информационих дејстава у одбрани националне безбедности.

Основу стратегијско-доктринарног оквира употребе информационих дејстава за одбрану информационе сфере Републике Србије чине Стратегија националне безбедности Републике Србије и Стратегија одбране Републике Србије из 2019. године и Доктрина Војске Србије из 2010. године.

Стратегија националне безбедности и Стратегија одбране представљају систем комплементарних норми које се односе на реализовање специфичних одбрамбених функција државе, између осталих и у информативној области. У вези са тим, на плану усклађивања стратегијских и доктринарних докумената са савременим изазовима и претњама из информационе сфере, потребно је, у складу са одредбама ових докумената, актуелизује значај безбедности и одбране националне информационе сфере Републике Србије[3] а претње из информационе сфере третирају као

3 Године 2001. од стране Председника Републике Белорусије, А. Г. Лукашенка, утврђена је Концепција националне безбедности. У овом документу постоји посебна целина под називом „Безбедност Републике Белорусије у информационој сфери“. Један од основних фактора који чини претњу у информационој и хуманитарној сфери овако је опредељен: „Ширење непроверених или

врсту претњи како војне тако и невојне природе. [4] Посебан подстицај унапређењу заштите од противничког дејства путем информационог деловања, допринело би доношење Стратегије информационе безбедности Републике Србије где ће бити дефинисани национални информациони системи од значаја за безбедност и одбрану земље, дефинисане улоге појединим државним органима као и опредељени састави за њену одбрану у информационом простору.

Још је Стратегија националне безбедности из 2009. године означила спољну информативну делатност као могућу претњу унутрашњој безбедности земље (Стратегија националне безбедности Републике Србије, 2009). У њој је било наведено да су развојем савремених информационих технологија, настале нове околности за деловање различитих група и недржавних актера у остваривању њихових циљева, што повећава ризике од угрожавања информационих и телекомуникационих система земље. Претходна стратегија је истицала да до угрожавања функционисања битних елемената система одбране може да дође и кроз деловање сајбер претњи које потичу ван територије Србије (Стратегија националне безбедности Републике Србије, 2009, 9-13). Због тога је у претходној Стратегији био наведен значај благовременог прикупљања и размена података и информација, односно инсистирано је на сталном унапређивању информативне и превентивне делатности. У Стратегији из 2019. године, додатно се наглашава да динамика глобалног развоја информационих технологија условиће даље интензивирање активности повезаних са ширењем лажних вести и дезинформација путем друштвених мрежа. С тим у вези, наводи се да ће у циљу заштите од ових претњи унапређивати способности и капацитета обраде, преноса и заштите информација и информационо-комуникационих система и

измишљених информација, усмерених на рушење... духовних и моралних вредности друштва, а такође подстицање националне и религиозне мржње...“; (Концепция национальной безопасности Республики Беларусь, Минск, 2001. стр. 45 – 48.)

4 Стратегија оружане борбе Савезне Републике Југославије, која је донешена пре агресије 1999. године, међу облике угрожавања неоружаним деловањем убрајала је, између осталих и психолошко-пропаганднадејства (ППД), обавештајну активност и друга субверзивна дејства.

одбране од техника хибридног и информационог ратовања у информационом и сајбер простору (Стратегија националне безбедности, 2019).

Стратегија одбране из 2009. године прецизира да структуру система одбране, као дела система националне безбедности, чине и институције које се баве пословима из области информисања. Ова стратегија, што је врло важно, наводи да основни ресурси одбране Републике Србије, чине људски и материјални ресурси, где у ове друге спадају и *информациони* потенцијали Републике Србије који се ангажују за потребе одбране (Стратегија одбране Републике Србије, 2009, 16-18). Стратегија одбране из 2019. године наводи да хибридне претње, као нови карактер претњи где информациона дејства имају важну улогу, представљају кључне чиниоце у процесу изналажења одговарајућег модела безбедносног и одбрамбеног организовања држава, што додатно указује на обавезу система одбране Републике Србије да развије капацитете за одбрану од претњи из информационог простора. Ова оцена је и посебно наглашена ставом из Стратегије одбране из 2019. године да ширење лажних вести и дезинформација у оквиру концепта хибридног и информационог ратовања могу да се негативно одразе на функционисање елемената система одбране, због чега је наглашена неопходност континуираног развија технолошке и информационе заштите елемената система одбране на свим нивоима организовања (Стратегија одбране Републике Србије, 2019).

Основе употребе информационих дејстава за одбрану Републике Србије најјасније су дефинисане у Доктрини Војске Србије. У Доктрини је наведено да окружење у којем се употребљавају снаге одбране Републике Србије, обухвата, између осталог и информациону димензију. Доктрина истиче да у оперативне способности Војске Србије спада између осталог и способност искоришћења информационог простора, која подразумева могућност Војске Србије или њених делова да прикупља, обрађује, користи и размењује податке о простору, времену, сопственим и противничким снагама (Доктрина Војске Србије, 2010, 17). Та способност се исказује кроз капацитет, брзину и квалитет прикупљања,

обраде, преноса и заштите информација од утицаја на ефикасност употребе снага (Доктрина Војске Србије, 2010, 17-18). Доктрина наводи да Војска Србије изводи борбене и неборбене операције. У неборбене операције спадају и информационе операције, које се изводе на свим нивоима командовања као интегрални део осталих операција или самостално, у периоду њиховог: планирања, оперативног развоја снага, у току и по завршетку других операција. Циљ извођења информационих операција остварује се реализацијом различитих војних и невојних мера и активности (Исто, 31). Невојне мере обухватају политичке и дипломатске акције, информисање јавности и сарадњу с цивилним структурама. Војне мере и активности обухватају: 1) психолошке мере и активности, 2) електронска дејства, 3) безбедносне мере и 4) обмањивање.

Може се закључити да постојећа стратегијска и доктринарна документа из области безбедности и одбране дају основни оквир за употребу информационих дејстава за одбрану земље. Евидентно је да се у Стратегији националне безбедности и Стратегији одбране потенцира значај информативне делатности за безбедност и одбрану Републике Србије. Међутим, информативна делатност се као таква у овим документима не третира као мера активне одбране, односно као средство за одбрану националне информационе сфере, што је потребно доградити у складу са савременим доктринарним опредељењима других земаља, на пример Руске Федерације. У Доктрини Војске Србије став да информативни ресурси представљају ресурсе одбране је јасан, али би требало би да буде детаљније разрађен и примењен у нормативним актима који произилазе из Доктрине, а посебно операционализован кроз конкретне задатке институцијама за заштиту информационих ресурса Републике Србије од значаја за одбрану, као и коришћење информационих ресурса за активну одбрану земље. Позитивно је што је у Доктрини јасно наглашен значај способности искоришћења информационог простора што може да се доведе у везу са "способности искоришћења информационог простора за утицај на противничку страну" и друге безбедносне изазове, а што би требало да буде уграђено у овај документ.

Са друге стране, уочљиво је да у стратегијским документима Републике Србије нису дефинисани стратегијски циљеви и дати основни правци обезбеђења информационе безбедности. У том смислу, поучни су ставови руских теоретичара који су дефинисали и класификовали стратешке циљеве информационе безбедности у области националне безбедности и одбране (Партыка, 2018). Стратешки циљеви информационе безбедности у области националне безбедности су заштита суверенитета, одржавање политичке и социјалне стабилности, територијални интегритет државе, обезбеђивање основних права и слобода човека и грађана, а такође и заштита критичне информационе инфраструктуре (Герзић, 2020). Стим у вези, основни правци информационе безбедности у области националне безбедности Републике Србије могу бити:

- сузбијање коришћења информационих технологија за промовисање екстремистичке идеологије, ширење ксенофобије, националног нејединства ради подривања суверенитета, политичке и друштвене стабилности, насилне промена уставног поретка и кршење територијалног интегритета државе,
- сузбијање активности штетних по националну безбедност, које се врше коришћењем техничких средстава и информационих технологија од стране страних служби и организација страних држава, као и од стране појединаца, повећање заштите критичне информационе инфраструктуре и стабилности њеног функционисања, развијање механизама за откривање и спречавање информационих претњи и отклањање последица њихове примене, повећање заштите грађана и територија од последица ванредних стања изазваних информационо-техничким утицајем на објекте критичне информационе инфраструктуре.
- неутрализација информационог утицаја усмереног на нарушавање традиционалних духовних и моралних вредности државе

Стратешки циљ информационе безбедности у области одбране се дефинише као ефикасна заштита виталних

интереса појединца, друштва и државе од унутрашњих и спољних претњи повезаних са коришћењем информационих технологија у војне и политичке сврхе, у циљу спречавања непријатељских аката агресије, чији је циљ подривање суверенитета државе, кршење територијалног интегритета држава и угрожавање међународног мира, безбедности и стратешке стабилности. У складу са тиме, главни правци заштите информационе безбедности Републике Србије у области одбране могу бити:

– стратешко одвраћање и спречавање војних сукоба који могу настати као резултат употребе информационих сукоба,
– унапређење информационе безбедности оружаних снага и других снага система одбране, укључујући снаге и средства информационог супростављања,
– предвиђање, откривање и процена информационих претњи, укључујући претње оружаним снагама државе у информационој сфери, и
– неутралисање информационо-психолошког утицаја, усмереног на подривање јединства народа, историјских основа и патриотских традиција повезаних са одбраном земље.

Оно што такође треба искористити као позитивне смернице из теоријских и доктринарних приступа из Руске Федерације за доградњу стратегијских и доктринарних приступа Републике Србије је да информациону безбедност треба сагледавати не само као техничко питање, имајући у виду да је за Стратегију развоја информационе безбедности Републике Србије надлежно Министарство трговине туризма и телекомуникација, него као сложен и вишеслојан проблем који је предмет интердисциплинарних, технолошких и хуманистичких научних истраживања. У том смислу информациону безбедност треба дефинисати у ширем смислу као безбедност друштва и владе у психолошком, научном, културном и производном аспекту, са посебним нагласком на заштити државних информационих извора и система, а не онако како је дефинисано у Закону о информационој

безбедности Републике Србије који презентује уско техницистичко гледање на ово безбедносно питање (Закон о информационој безбедности, 2017).[5]

Даље, врло је важно да се у стратегијским докуметима нагласи да се информациона дејства према нашој земљи неће сматрати као невојна фаза сукоба, као и да се одбрана од противничких информационих дејстава води преко читавог скупа активности од значаја за националну безбедност.

Оно што је посебно корисно за Републику Србију, имајући у виду ограничене људске и материјалне капацитете и још недовољан ниво техничког развоја је примена руског приступа који афирмише примену „меке димензије" информационих дејстава, тј. њихов информационо-перцептивни аспект (пропаганда, одмањивање и дезинформисање), који захтева много мање финансијских средстава. Овакво опредељење се уклапа и са релативно свежим и позитивним искуством у вођењу пропагадне одбране током агресије 1999. године, као и са чињеницом да је овакво информационо оружје довољно јефтино и једноставно за производњу, као и да могућност његове масовне употребе погодује примени концепта „тоталне одбране" који је прихваћен и дефинисан у стратегијским документима Републике Србије из области безбедности и одбране.

Трећи правац активности у приступу овом проблему се огледа у неопходној потреби да што пре отпочне са изградњом властитих капацитета за одбрану националне информационе сфере. Они се морају развијати паралелно у свим правцима и не смеју бити ограничени на пасивну одбрану, јер такав правац води у подређен положај у области информационих сукоба. Имајући у виду степен зависности српског друштва од активности у информационом, посебно сајбер простору, приоритетне области развоја би требало да буду активна одбрана сувереног информационог простора. У извођењу информационих операција у циљу одбране

5 У њему је дефинисано да информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ (техничких) система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.

националне информационе сфере треба да се укључе сви субјекти значајни за одбрану земље. Једина ограничења у томе би морала да буду обавезе поштовања постојећих регулатива међународног права оружаних сукоба, људских права и националних интереса (Младеновић, 2012, 37-38).

У закључку, може се констатовати да у ситуацијама, када активности у информационом простору и окружењу Републике Србије, како информационо-технолошке тако и информационо-психолошке природе, представљају претњу по националну безбедност, држава мора имати развијене стратегије и капацитете својих снага одбране за одговор на наведене претње и исте ангажовати на основу стратегијских и законских решења и надлежности институција. Теоријски приступи безбеносних и војних експерата Руске Федерације у конципирању одбране у информационој сфери пружају добру основу за доградњу стратегијског и доктринарног приступа Републике Србије у овој области.

РЕФЕРЕНЦЕ

Андрej Лиаропулос, Russia's Approach to Information Operations, January 2007, www.rieas.gr/

Военная доктрина Российской Федерации, 2014. године, доступно на www.scrf.gov.ru, преузето 30.04.2020. године.

Гареев М.А. *О некоторых характерных чертах войн будущего.* /Военная мысль. - 2003.,бр. 6., стр. 52 - 59.

Герзић Чедомир, Информациона безбедност као елеменат националне безбедности, 15. Међународна конференција Ризик и безбедносни инжењеринг, Копаоник, 16.-18. јануар, 2020. http://www.rizik.vtsns.edu.rs/RSE_2020/radovi/05/RIZIK_05_4.pdf

Доктрина Војске Србије (Службени Војни лист бр. 2/10) стр. 17.

Доктрина информационной безопасности Российсой Федерации, Президент, 09. 09. 2000.

Закон о информационој безбедности „Службени гласник РС“,

бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019.

Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве, Министерство обороны Российской Федерации, 2011, стр. 5

Концепция национальной безопасности Республики Беларусь, Минск, 2001. стр. 45 – 48.)

Манойло А.В. - *Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта.* — Киев: Материалы V Международной научно-практической конференции «Информационные технологии и безопасность», вып. №8, 2005 г., стр. 73-80.

Мијалковић Саша.: „Национална безбеддност – од Вестфалског концепта до послехладноратовског“, *Војно дело* 2/2009, стр. 56.

Миљковић Милан и Дарко Тадић, „Информационе операције западних обавештајних служби у србији октобра 2000. Године“, Војно дело, 5/2017, стр.

Миљковић Милан, Путник Ненад, „Активности савремених обавештајних служби у сајбер простору“, *Војно дело,* (Београд, 7/2016, стр 177-178.)

Младеновић М., Дракулић М., Јовановић Д.: *Међународно право и сајбер ратовање*, *Војно дело*, пролеће 2012, стр.17.

Панарин И.: *Проблемы обеспечения информационной безопасности в савременныхусловиях*, Украинский ресурс по безопасности, http://kiev-security.org.ua , 1997.

Панарин Игор Николаевич - Технология информационной войны./ 2003., стр. 320

Папарин И.: *Доктрина информационе одбране Русије*,Евроазија, јули 2012, http://euroasiaserbia.wordpress.com/2012/07/18/

Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018.

Петровић, Л.:„Информациона безбедност – правни, економски и технички аспект“, *Информациона безбедност 2012 – научно стручни скуп*, Београд, стр. 3.

Синковски, С.: „Информациона безбедност – компонента националне безбедности, Београд“, *Војно дело*, 2/2005, стр. 49.

Стратегија националне безбедности Републике Србије, 2009, стр. 24.

Стратегија националне безбедности Републике Србије„Службени гласник РС“, број 94 од 27. децембра 2019.

Стратегија одбране Републике Србије, „Службени гласник РС“, број 94 од 27. децембра 2019.

Стратегија одбране Републике Србије, Министарство одбране, 2009, стр.16.

Стратегия национальной безопасности Российской Федерации, чл. 82, 2015. године, доступно на www.scrf.gov.ru, преузето 30.04.2020. године

Урсул А.Д., Цырдя Т. Н., „Информационная безопасностъ, сущностъ, содержание и принципы ее обеспечения“, *Журнал Факт*№ 2, 2000.

A.V. Smolovyi, „Problemniye voprosy sovremennogo operativnogo iskusstva i puti ikh Rescheniya“,Voyennaya Mysl no. 12, 2012.

Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgian War*: Lessons and Implications, Monograph, Strategic Studies Institute, U.S. Army, Carlisle, 2011, p 19.

Bikkenin R. “Information Conflict in the Military Sphere: Basic Elements and Concepts“, Morskoy Sbornik, No 10, 2003, pp. 38-40.

Chekinov and Bogdanov, “The Nature and Content of a New-Generation War,” op cit..

General Valery Gerasimov, “The Value of Science in Foresight: New Challenges Require Rethinking on the Forms and Methods of Warfare,”*Military Industrial Kurier*, (27 Feb. 2013), http://vpknews.ru/sites/default/files/pdf/

VPK_08_476.pdf .

Georgii S. Isserson, *The Evolution of Operational Art,*, Fort Leavenworth, SAMS Theoretical Special Edition, 2005.

http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No. 4_2013.pdf

Janis Berzins*, Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* Riga, National Defense Academy of Latvia, Center for Security and Strategic Research, 2014, pp 2-3.

Janis Berzins, *Russia's New Generation Warfare,* October 11, 2016, http//www.thepotomacfoundation.org/The New Generation of Russian WarfareThe Potomac Foundation. htm

M. D. Ionov, „On Reflexive Control of the Enemy in Combat",*Military Thought* (English edition), No. 1, January 1995.

McAfee, Virtual Criminology Report 2009, Santa Clara, McAfee, 2009.

Nathan D. Ginos, *The Securitization of Russian Strategic Communication*, Monograph, School of Advanced Military Studies, Fort Leavenworth, 2010.

Nye J. S. Jr.: „SoftPower", *Foreign Policy*, no. 80, 1990, pp. 153-170.

Rastorguyev C.: An Introduction to the Formal Theory of Information Warfare, Moscow, 2003, p. 6.

Scott J. Shackelford, "Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*"*, in: *Journal of Internet Law*, February 2010.

Sergei Chekinov, Sergei Bogdanov, "The Nature and Content of a New-Generation War, *Voyennamysl,* No.4, October 2013,

*mysl,*No.4,October2013,http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No. 4_2013.pdf

Thomas L. T., „Russian Views on Information-based Warfare", *Airpower Journal* (Special Edition 1996), pp.25-35.

Through Toughness, Fort Leavenworth, Foreign Military Studies Office, 2011, p 131.

Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness*, Fort Leavenworth, Foreign Military Studies Office, 2011.

Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology*

Timothy L.T.: 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.

Valery Gerasimov, „The value of science in anticipation", *VPK news*, 27 February 2014, http://www.vpk-news.ru/articles/14632 (преузето 07.04.2017).

Vasily K. Kopytko, „Evolution of Operational Art",*Voyennaya Mysl* 17, no 1, 2008, pp.202-214

Volodymyr N. Shemayev, „Cognitive Approach to Modeling Reflexive Control in Socio-

Milan Miljkovic
Dragan Jevtic

CONFLICTS IN THE INFORMATION SPACE FROM THE ANGLE OF MILITARY THOUGHT IN THE RUSSIAN FEDERATION - EXPERIENCES FOR THE SECURITY OF THE REPUBLIC OF SERBIA

Resume

Modern states, due to the mass application of information technology in the field of communications, face the problem of effective control and protection of the national information sphere, and thus national security. Information has long been used for manipulative purposes and as a means of leading conflicts, and the modern information age has only further actualized the information space as a combat space of modern global society. The use of misinformation and false news within the concept of „hybrid and information warfare“ has been actualized, as a way of conducting geopolitical conflicts between great powers, but also as a means of influencing and putting pressure on small states. In this regard, the paper analyzes the theoretical and conceptual approach of security and military theorists of the Russian Federation regarding the defense against threats from the information sphere. The results of the analysis indicate that the theoretical approach of the Russian Federation in this area is applicable to the Republic of Serbia, which in its current strategic documents in the field of defense and security emphasized the need to develop a system of defense against threats from the information space.

Keywords: information action, information space, perceptual means.

* Овај рад је примљен 07. априла 2021. године, а прихваћен на састанку Редакције 12. јула 2021. године.