

УПОТРЕБА СИЛЕ У МЕЂУНАРОДНИМ ОДНОСИМА

Уредила
Жаклина Новичић

Београд, 2018.

Издавач
Институт за међународну политику и привреду, Београд

За издавача
Проф. др Бранислав Ђорђевић
директор

Уредила
Др Жаклина Новичић

Рецензенти
Проф. др Драгољуб Тодић
Доц. др Милош Јовановић
Проф. др Драган Ђукановић

Лектор за српски језик
Маја Јовановић

Лектор за српски језик
Маја Јовановић

Компјутерска обрада и корице
Сања Баловић

Штампа:

ИСБН 978-86-7067-255-0

Тематски зборник радова је резултат рада на пројекту Министарства просвете, науке и технолошког развоја: „Србија у савременим међународним односима: Стратешки правци развоја и учвршћивања положаја Србије у међународним интегративним процесима – спољнополитички, међународни економски, правни и безбедносни аспекти, из програма основних истраживања код Министарства просвете, науке и технолошког развоја Републике Србије” (евиденциони број 179029).

САДРЖАЈ

Реч уредника	7
--------------	---

Први део

ГЕОПОЛИТИКА, ИНТЕРВЕНЦИЈЕ И ВЕЛИКЕ СИЛЕ

Географија и употреба силе: Геополитичка анализа војног ангажовања Сједињених Држава крајем XX и почетком XXI века <i>Бранислав Ђорђевић, Небојша Вуковић</i>	11
„Употребљивост“ силе за остваривање спољнополитичких циљева у XXI веку: Руске интервенције у Грузији (2008) и на Криму (2014) <i>Владимир Трапара</i>	34

Други део

РАЗОРУЖАЊЕ, НУКЛЕАРНО ОРУЖЈЕ И НОВЕ ТЕХНОЛОГИЈЕ

Забрана оружја за масовно уништење: Од Женева до Њујорка век касније <i>Весна Кнежевић Предић, Милош Хрњаз</i>	59
Развој војних нуклеарних потенцијала у постхладноратовском поретку као инструмент тврде моћи у међународним односима <i>Душан Пророковић</i>	91
Етичке и оперативне специфичности технологије офанзивних дрона у контексту међународних односа <i>Александар Фатић</i>	121

Сајбер ратовање и промена физиономије савремених сукоба <i>Дејан Вулетић, Милинко Врачар</i>	137
---	-----

Трећи део **УЈЕДИЊЕНЕ НАЦИЈЕ И УПОТРЕБА СИЛЕ**

Употреба силе у поретку Уједињених нација <i>Душко Димитријевић</i>	157
--	-----

Примена силе против појединаца, везано за међународне односе у миру <i>Борис Кривокапић</i>	201
---	-----

Право држава на употребу силе у самоодбрани и његова злоупотреба <i>Сенад Ганић</i>	229
---	-----

Подобност хуманитарне интервенције као правне норме <i>Михајло Вучић</i>	240
---	-----

Четврти део **ЕВРОПСКА УНИЈА И УПОТРЕБА СИЛЕ**

Постепени развој Европске уније као безбедносне заједнице — на путу од Венере ка Марсу <i>Душко Лопандић</i>	257
--	-----

Европске жандармеријске снаге – савремени облик полицијске сарадње и деловања <i>Александар Јазић</i>	273
---	-----

САЈБЕР РАТОВАЊЕ И ПРОМЕНА ФИЗИОНОМИЈЕ САВРЕМЕНИХ СУКОБА

Дејан ВУЛЕТИЋ¹

Милинко ВРАЧАР

Апстракт: Рат, као деструктивна друштвена појава, представља најгрубљи облик примене силе у међународним односима. Карактеристике савремених сукоба указују да се суштина рата променила. Војна моћ држава, исказана кроз примену оружане силе, све више показује неефикасном у остваривању спољнополитичких интереса. Тренд смањења њене ефикасности може се објаснити утицајем процеса глобализације и информатичке револуције на друштвене токове чиме је знатно измењено оперативно окружење у којима се одвијају савремени сукоби. Глобализација доводи до све веће улоге недржавних актера у међународним односима чиме се, тако се сматра, они трансформишу у глобалне односе. С друге стране, информатичка револуција је поспешила нове димензије неоружаних међународних сукоба. Сајбер ратовање, као облик информационог ратовања, представља еклатантан пример вођења савремених сукоба.

Кључне речи: сила и моћ, међународни односи, савремени сукоб, информационо ратовање.

УВОД

Крајем 19. и почетком 20. века људско друштво карактеришу нагле и драматичне промене у скоро свим областима живота и рада. Убрзани развој науке и технологије, интензивна индустријализација учинили су да свет поприма сасвим нова обележја као што је нпр. појава нових врста претњи по

¹ Др Дејан Вулећић, Институт за стратегијска истраживања Универзитета одбране, Београд, dejan.vuletic@mod.gov.rs; др Милинко Врачар, Институт за стратегијска истраживања Универзитета одбране, Београд, milinko.vracar@mod.gov.rs.

Рад је настао у оквиру научноистраживачког пројекта „Хибридно ратовање – искуства и перспективе“ који се реализује у Институту за стратегијска истраживања Универзитета одбране.

појединце и државе. Период од друге половине 20. века, поред изузетне динамике, карактеришу и извесне контроверзе, које су указивале на тзв. „тамну страну прогреса”. Напредак науке, а посебно техничких и природних наука доноси, поред позитивних резултата који су његово основно обележје, одређене потенцијалне опасности.²

Институционализација дипломатије у новим условима и изградња савременог безбедносног система у свету утицала је на ограничење примене војног фактора у реализацији постављених циљева спољне политике од стране држава као субјеката међународних односа. Такво стање у међународној заједници је утицало да се остварење интереса не врши само применом оружане силе, већ другим средствима. Нови начин ангажовања држава у сукобу условио је појаву нових средстава, а са њима и нових начина ратовања (информационо, хибридно итд.). Захваљујући ефикасности примене ти нови начини ратовања заузимају све значајније место у савременим сукобима.

СИЛА И МОЋ У МЕЂУНАРОДНИМ ОДНОСИМА

Сила и моћ представљају централне појмове међународних односа. Услед таквог значаја проистиче потреба за разумевањем обима и садржаја тих појмова и њихових међусобних веза, јер и данас они заузимају значајно место при покушају да се опишу или објасне савремене релације између различитих субјеката унутар међународне заједнице. Да би се схватио појам силе полази се од појма моћи. Он је шири појам од појма силе, заснива се на потенцијалу и садржи могућност њене примене.

Кроз историју развоја људског друштва моћ је на различите начине била присутна у теорији и пракси међународних односа, почев од Сун Цуа (*Sun Tzu*), Тикудида (*Thucydides*), преко Макијавелија (*Machiavelli*), Хобса (*Hobbes*) па све до данашњих дана. При анализи међународних односа и спољне политике, већина теоретичара се слаже у констатацијама да постоји историјска константа између моћних и неразвијених држава, дата у виду изреке „јаки чине оно што могу, а слаби прихватају оно што морају“³. На тој парадигми изграђен је реалистички теоријски правац међународних односа који у свој фокус разматрања ставља, у најкраћем, „борбу за моћ“. У оквирима те теорије, сврха вештине руковођења државом јесте да се обезбеди опстанак нације у непријатељском окружењу. У том циљу, ниједан начин није значајнији него стицање моћи, а ниједан приступ није значајнији него самопомоћ. Тако се игра међународне политике врти око тежње за моћи, њеног стицања, увећања,

² Живојин Алексић, Зоран Миловановић, *Лексиком криминалистике*, Глосаријум, Београд, 1995, стр. 16-20.

³ Thucydides, *History of Peloponnesian War*, Penguin Books, New York, 1972, p. 402.

пројектовања и коришћења да би се други покорили нашој жељи. У екстремним, случајевима, чини се да реализам прихвата рат као нормалну, тј. неизбежну појаву.

Многе вође, школоване у духу реалполитике, по навици полазе од традиционалне претпоставке да је моћ нешто што државама даје способност да промовишу националне интересе, превагну у међународном преговорању и обликују правила која управљају глобалним системом. Дакле, на моћ се првенствено гледа као на политички феномен чији се смисао испољава у способности једног чиниоца да убеди другог да уради оно што иначе не би урадио.⁴ Упростијено, моћ је способност остваривања жељених исхода и, уколико је потребно, промене понашања других да би се то остварило. Способност остваривања жељених исхода често се повезује са поседовањем одређених ресурса па се са тог аспекта моћ дефинише као поседовање релативно великих количина елемената као што су становништво, територија, природни ресурси, привредна снага, војна моћ и политичка стабилност.⁵

Да би одредили компаративну моћ држава, аналитичари их обично рангирају према способностима или средствима која су нужна да се оствари утицај над другима. У том смислу моћ државе се мери различитим чиниоцима или елементима. Од свих елемената моћи реалисти сматрају војну моћ, али и економску, главним елементима моћи држава. Војна моћ се може исказати кроз бројчаност армија, њихову опремљеност, степен технолошког развоја наоружања, поседовање нуклеарног наоружања и слично. У суштини, као што Мишовић и Ковач износе, војна моћ представља израз способности извршавања задатака војске. Она проистиче из друштвене моћи земље, која је садржана у свеукупној способности за опстанак и развој, а посебно је условљена економском моћи.⁶ Дакле, она се може разумети као укупни потенцијал који једна држава (народ, покрет или организација) може да употреби у оружаном борби у остваривању својих интереса.

Моћ, као способност за остваривање националних интереса, није разматрана само унутар реализма. Либерални теоријски правац међународних односа има нешто шири поглед на појам моћи. Према Нају (Nye), моћ државе извире и из других елемената а не само из улагања у војску. У њих свакако спадају релативна величина економије државе, њено становништво и територија, географски положај, сировине, степен зависности од увоза,

⁴ Čarls Kegli, Judžin Vitkof, *Svetska politika – Trend i transformacija*, Centar za studije Jugoistočne Evrope, FPN, Diplomatska akademija MSP SCG, Izdavačko i grafičko preduzeće Prometej, Beograd, 2004, str. 84-87, 645.

⁵ Džozef Naj, *Paradoks američke moći*, BMG, Beograd, 2004, str. 24-26.

⁶ Слободан Мишовић, Митар Ковач, *Систем одбране*, Факултет цивилне одбране, Београд, 2006, стр. 50.

технолошки капацитет, национални карактер идеологија, индустријска продуктивност, обим трговине, образовни ниво итд.⁷ Нај класификује моћ на тврду и меку. Војна и економска моћ су примери тврде командне моћи која се може користити за навођење других да промене став. Тврда моћ почива на подстицајима или претњи. Постоји и индиректан начин за вршење моћи. Држава може доћи до жељених резултата у светској политици јер друге земље желе да је следе, дивећи се њеним вредностима, угледајући се њен пример. У том смислу, једнако је значајно „утврдити дневни ред“ у светској политици и привући друге колико и приморати их да се мењају претњама или употребом војних или економских оружја. Тај аспект моћи – приволети друге да раде оно што желите – назива се меком моћи. То кооптира људе уместо да их присиљава.⁸

Тврда и мека моћ су повезане и могу оснажити једна другу. Обе су у функцији остваривања државних циљева утицајем на понашање других. Понекад исти ресурси моћи могу утицати на цео спектар понашања, од принуде до привлачења. У историји међународних односа присутна су два крајња обележја односа између субјеката, а то су односи сукобљености и сарадње, као и низ прелазних стања између те две крајности. Војна, економска, културолошка, технолошка и друга моћ могу бити подстицај међународне сарадње између држава које деле исте или сличне вредности, што се може видети на примеру НАТО и Европске уније. С друге стране, антагонистички односи између великих сила и глобални безбедносни проблеми који из таквих односа проистичу, упућују на доминантну улогу тврде моћи у међународним односима. У таквим околностима долази до употребе силе уопште а тиме и војне силе као њеног конститутивног елемента.

Појавни облици силе су се развијали кроз историју развоја људског друштва у складу са иградњом различитих капацитета моћи у националним и државним оквирима, као и на глобалном плану. Првобитни облици примене силе углавном су базирали на физичкој примени силе и оружаном насиљу, а сви остали облици који су се испољавали у сукобу били су њима подређени у функцији реализације националних, државних, политичких, религијских и других интереса и циљева. Друштвеним развојем и успостављањем снажнијих политичких, економских, војних и других веза између држава, сила се испољавала у различитим подручјима. Средства за примену силе данас се могу сврстати у више категорија, међу којима су најзначајније политичка, економска и војна (оружана). У новијим теоријским анализама додају се и дипломатска, технолошка, информациона, научна и друге области друштвене

⁷ Robert Keohane, Joseph Nye, *Power and Interdependence*, International Organization, Vol. 41, No. 4, Autumn, 1987, pp. 725-753

⁸ *Ibid.*, стр. 28-29.

делатности преко којих се могу испољити различите силе у функцији достизања крајњег циља. Када се говори о облицима употребе силе у међународним односима, употребљавају се различите класификације, али најчешћа је она на оружане и неоружане облике силе.⁹

Да би се испољила одређена сила, неопходно је да постоји и одређена моћ, односно способност за ту намеру. Према Шварценбергеру (*Schwarzenberger*) „моћ је способност појединаца, групе или државе да наметну своју вољу другоме, ослањајући се при томе на делотворност средстава силе у случају непокоравања“.¹⁰ Према Гађиновићу „сила је продукт моћи, то јест силу примењује само онај ко поседује моћ. Када је у питању примена војне силе, њу успешно примењују само моћне државе“¹¹. Међутим, моћ садржи низ могућности за наметање воље, међу којима је физичка сила само једна од њих.

Оружана сила је један од појавних облика силе. Првенствено проистиче из војне моћи али и из целокупног квантума државне моћи. У савременим условима су у широкој примени оружани облици примене силе попут рата, агресије, интервенције и оружане побуне. Рат представља најгрубљи облик примене оружане силе и примењује се као крајње средство у решавању међународних спорова.

КАРАКТЕРИСТИКЕ САВРЕМЕНИХ СУКОБА

Двадесети век, поред осталог, карактерише све већи број нетрадиционалних форми сукоба. Тај тренд је нарочито испољен у периоду након завршетка Хладног рата, када настаје убрзана и, по обиму и садржају, трансформација сукоба.

Уочавајући настале промене, теоретичари рата су од краја осамдесетих година прошлог века свеобухватним приступом проблематизовали промену његове природе. Затечени у међупростору, у коме постојећи класични (модернистички) теоријски оквири нису у потпуности могли да објасне постојећу праксу а, с друге стране, савремене теорије о рату¹² нису имале своју емпиријску потврду, они су сукобили своја мишљења о адекватности постојеће класичне теорије у перцепцији природе рата. Теоретичари попут Греја (*Gray*), бранили су традиционална (Клаузевицевска) становишта

⁹ Милинко Стишовић, *Примена силе у међународним односима*, ШНО, 1996; Слободан Мишовић, Митар Ковач, *Систем одбране*, оп.цит, стр. 44-45.

¹⁰ Georg Schwarzenberger, *Power Politics*, London, Stevens, 1951, p. 14.

¹¹ Радослав Гађиновић, *Примена силе у међународним односима*, Српска политичка мисао, Београд, број 3-4/2007, год. 14. vol. 19. стр. 9-22.

¹² О савременим теоријама рата видети више у: Слободан Мишовић, Митар Ковач, *Систем одбране*, Факултет цивилне одбране, Београд, 2006, стр. 151-171.

тврдећи да се природа рата није променила већ само његове карактеристике.¹³ Друга група теоретичара, заступника модерног промишљања, попут Кревелда и Калдорове, тврдили су да су постојећа знања о природи рата застарела или погрешна. Разматрајући карактеристике савремених оружаних сукоба они су понудили нови, „неклаузевицевски оквир“ за размишљање на тему промене његове природе.¹⁴

Без обзира на одређено неслагање у вези погледа на промену природе рата, сагласни су да је дошло до промене његове физиономије јер су савремени сукоби одражавали све већу заступљеност неоружаних садржаја рата што их је недвосмислено чинило другачијим у односу на претходне (традиционалне, класичне или модернистичке) сукобе. Тиме је свакако важно место унутар расправа о трансформацији сукоба заузимао утицај процеса глобализације, техничко-технолошког развоја, а посебно информатичке револуције, на различите садржаје рата.

Услед високе цене коштања производње и употребе савременог наоружања, утицаја домаћег и међународног јавног мњења на доносиоце политичких одлука, уочава се да развијене државе све више прибегавају употреби невојних средстава, попут економских, пропагандних, информационих итд, док је употреба оружаног средстава минимизирана. Знатан број теоретичара види специфичност савремених сукоба у томе што је бојно поље изгубило своју јасну физичку димензионисаност употребом високо развијене информационо-комуникационе технологије (ИКТ), те се савремени сукоби све више одигравају у информационој димензији док класичне форме оружаног сукоба у осталим димензијама губе на значају. Доступност савремених информатичких средстава омогућава недржавним актерима успешно супростављање конвенционално супериорнијим противницима у асиметричним сукобима.¹⁵

Бројне су предности примене информационих (сајбер) наспрам оружаних средстава приликом сукобљавања одређених субјеката у међународној заједници. Оштећења имовине, број погинулих или повређених лица су избегнути или су неупоредиво мањи у случају сајбер напада. Брзина деловања и анонимност починилица су предност на страни нападача у сајбер простору што знатно отежава одбрану и предузимање контрамера нападнуте стране. Сајбер напади, који се могу рангирати од неовлашћеног упада у рачунарске

¹³ Colin S. Gray, *War, Peace, and International Relations: An Introduction to Strategic History*, Abingdon, UK: Routledge, 2007.

¹⁴ Martin van Creveld, *The Transformation Of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*, The Free Press, 1991. Mary Kaldor, *New & Old Wars: Organized Violence in a Globalized Era*, Stanford University Press, California, 1999.

¹⁵ Thomas X. Hammes, *Fourth Generation War and Other Myths*, U.S. Army War College, Strategic Studies Institute, November 2005.

системе (хакинга) до озбиљног напада на критичне информационе инфраструктуре, нису увек очигледни и правно регулисани тј. није прецизно дефинисано коју правну санкцију, међународни закон или уговор треба применити у конкретном случају.

ИНФОРМАЦИОНО РАТОВАЊЕ КАО ЕКЛАТАНТАН ПРИМЕР САВРЕМЕНИХ СУКОБА

Информационо ратовање има дубоке корене у људској историји. Историја људске цивилизације сведочи о бројним примерима информационог ратовања који указују на значај информације и постизање информационе супериорности¹⁶ у односу на противника. Експанзија информационог ратовања (*information warfare* – IW) почиње у 20. веку са развојем савремених информационо-комуникационих технологија чиме је револуционарно промењен и сам начин ратовања. Информационо ратовање се води у војној, политичкој, економској, друштвеној и другим сферама, у миру и оружаном сукобу.¹⁷

Убрзани развој и све већа употреба информационо-комуникационих технологија знатно је изменила савремени свет и начин вођења сукоба. Промене информационог окружења чине информациону супериорност кључним фактором за постизање успеха у евентуалном сукобу. Савремени сукоби су наглашено окарактерисани и као борба у сфери информација. Између кључних фактора у међународној заједници постоји заједништво по питању схватања значаја информација али постоје одређене разлике у погледу места и улоге као и периода примене информационог ратовања.

Према Арквили (*Arquilla*) и Ронфелду (*Ronfeld*), информациона револуција трансформише ратовање. Више се неће сукобљавати масивне, укопане војске у крвавим исцрпљујућим борбама. Уместо тога, мале и изузетно мобилне снаге, „наоружане“ информацијама у реалном времену добијених са сателита и тактичких сензора, удариће великом брзином на неочекиваним местима. Победник ће бити страна која може да експлоатише информације тако да распрши маглу рата а противника увије у ту маглу.¹⁸

¹⁶ Информациона супериорност је дефинисана као операциона предност изведена из способности да се сакупи, обради и дистрибуира непрекидни ток информација док се истовремено искоришћавају или онемогућавају непријатељски напори да се учини исто. *FM 3-0 Operations*, Headquarters Department of the Army, Washington, DC, 14 June 2001. У борбеном правилу САД FM 34-45 под информационом супериорношћу се сматра степен доминације над непријатељским снагама који омогућава прикупљање, коришћење и заштиту информација без стварног супростављања.

¹⁷ Дејан Вулетић, *Безбедност у сајбер простору*, МЦ „Одбрана“, Београд, 2012. стр. 139.

¹⁸ John Arquilla, David Ronfeldt, *Мрежни рат и кибер рат*, RAND корпорација, извод из студије објављене у „Comparative Strategy“, Volume 12, 1995, стр. 141-165.

Информациона супериорност је дефинисана као операциона предност изведена из способности да се сакупи, обради и дистрибуира непрекидни ток информација док се истовремено искоришћавају или онемогућавају напори супротне стране да учини то исто.¹⁹

Појам информационо ратовање је сведен и на оперативном нивоу означен као информациона операција.²⁰ Информационе операције интегришу све аспекте информације да би пружиле подршку и повећале елементе борбене моћи, са циљем да се доминира бојиштем у право време, на правом месту и са правим ресурсима.

Информациона операција је заједничко ангажовање способности везаних за информације (*Information Related Capabilities – IRCs*) током војних операција, у складу са другим операцијама, којима се утиче, омета, компромитује или онемогућава процес доношења одлука непријатеља и његових савезника док се истовремено штите властити ресурси.²¹

Способности везане за информације су алати, технике или активности које утичу на неку од три димензије информационог окружења (физичка, информациона и когнитивна). Они утичу на способност циљне групе (*target audience – TA*) да прима, обрађује или дистрибуира информације пре и после доношења одлука.²²

Правило америчке војске „Информационе операције” (*Joint Publication 3-13 Information Operations*) обезбеђује заједничку доктрину за планирање,

¹⁹ *FM 3-0 Operations*, Headquarters Department of the Army, Washington, DC, June 14th, 2001, p. 11-2.

²⁰ У Доктрини Војске Србије, информационе операције се сврставају у неборбене операције (пored операција цивилно-војне сарадње и операција подршке цивилним властима у супротстављању неоружаним претњама безбедности). Неборбене операције се могу изводити самостално или у склопу борбених операција, у миру, ванредном и ратном стању. У наведеној Доктрини се наводи да се информационе операције изводе на свим нивоима командовања као интегрални део осталих операција или самостално, у периоду њиховог планирања, оперативног развоја снага, у току и на завршетку осталих операција. Циљ извођења информационих операција остварује се реализацијом различитих војних и невојних мера и активности. *Доктрина Војске Србије*, Медија центар „Одбрана”, Београд, 2010, стр. 81. У Доктрини операција Војске Србије, информациона операција се дефинише као „скуп координираних активности ради деловања на процес доношења одлуке непријатеља”. Задатак операције је испуњење војних и политичких циљева деловањем на информације, информационе процесе и системе непријатеља и остралих страна помоћу истовремене заштите сопствених и пријатељских информација, информационих процеса и система. *Доктрина операција Војске Србије*, ГШ ВС (ЗОК), 2012, стр. 36.

²¹ *Joint Publication 3-13 Information Operations*, Joint Chief of Staff, USA, 2014, p. GL-3; *Information operations*, Air Force Policy Directive 10-7, Department of the Air Force, USA, 2014, p. 2.

²² *Ibid.*

припрему, извршавање и процену информационих операција као део низа војних операција.

Руски поглед према националном суверенитету је описан у доктринарним и стратегијским документима као што су Војна доктрина и Доктрина информационе безбедности Руске Федерације. Идентификована су три типа потенцијалних конфликта који могу представљати претњу Русији. Прва претња је ризик од ескалације конфликта у непосредној близини националних граница. Друга претња је могућност директне конфронтације са Сједињеним Америчким Државама (САД) и њеним западним савезницима. Трећа претња је могући конфликт са Народном Републиком Кином која је у експанзији. Ризик од последња два могућа конфликта је означен као низак.²³

Русија и Кина немају званичне доктрине о информационом ратовању и информационим операцијама које су познате јавности. Насупрот томе, САД има *US Joint Pub 3-13* и документ о заједничкој визији 2020 (*Joint Vision 2020*). Термин информационо ратовање је избачен из последње верзије *Joint Pub 3-13* док га Русија и Кина још увек користе. Све три стране наглашавају значај информација у савременом конфликту и сматрају да ће њен значај расти. Русија и Кина шире посматрају информационе операције, како у периоду мира тако и у ратном стању, док је америчко гледиште уже и односи се само на период ратног стања.²⁴

У кинеском гледишту, информациона операција је компонента информационог ратовања, супротно од америчког гледишта. За Сједињене Америчке Државе, информациона операција је начин борбе (*way to fight*) док се у Кини сматра да је информациона операција борба за себе (*the fight itself*) и реализује се на више различитих нивоа и димензија више година.²⁵

Руски поглед је знатно ближи схватању НР Кине, по којем се информационо ратовање води у миру и рату (мање, више константно), на тактичком, оперативном и стратегијском нивоу.²⁶

Руски приступ схватању информационих операција се разликује у неким елементима од приступа западних земаља.²⁷ Са руског гледишта, информација

²³ Roland Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency, Stocholm, 2010, p. 4.

²⁴ *Ibid.*, p. 23,24.

²⁵ *Ibid.*

²⁶ *Ibid.*

²⁷ Као и НР Кина и Русија, Република Србија нема званичну доктрину информационих операција. Слично гледиштима поменутих земаља, у доктринарним документима Војске Србије наводи се да се информационе операције могу изводити самостално или у склопу борбених операција, на свим нивоима командовања, у миру, ванредном и ратном стању.

има своју вредност и мора се штитити у миру и рату. У доктрини информационе безбедности Руске Федерације, заштита информација има стратегијски значај и представља кључни фактор за стабилност државе, политички режим као и могућност утицаја и вођења сукоба. У војној доктрини, публикованој у пролеће 2010. године, наглашена је важност информационог ратовања током почетне фазе конфликта ради слабљења способности командовања и управљања непријатеља, али и извођења информационе кампање током трајања сукоба да би се формирао позитиван став у међународној заједници.²⁸

САЈБЕР РАТОВАЊЕ КАО ОБЛИК ИНФОРМАЦИОНОГ РАТОВАЊА

Сајбер ратовање представља облик информационог ратовања који се састоји од низа акција којима се прекидају или уништавају информационо-комуникациони системи противника (нпр. убацивање вируса у војне рачунарске система противника).

У Естонији 2007. године, дистрибуирани напад одбијања услуга (*Distributed Denial of Service – DDOS*)²⁹, био је један од највећих икад виђених напада у сајбер простору. Напад је реализован уз помоћ више различитих ботнетова (*Robot Networks*)³⁰, сваки са десетинама хиљада заражених рачунара.³¹ Неки називају случај Естоније „првим ратом на мрежи“ (*Web War One – WWI*).³² Годину дана касније, 2008. године, DDOS нападима били су погођени и Грузијски владини сајтови и *web* сервер на којем је био хостован сајт председника Грузије. Грузија је, иначе, повезана на Интернет преко Русије

²⁸ *Ibid.*

²⁹ Напад ускраћивањем услуга је тип напада који покушава да спречи легитимне кориснике да приступе мрежним услугама. То се остварује преоптерећењем мрежних сервиса или прекомерном конекцијом, што узрокује пад конекције или сервиса. Инфраструктура међусобно спојених система и мрежа састоји се од ограничених ресурса. *DoS* алати су намењени да пошаљу велики број захтева циљаном серверу, с циљем да преплави ресурсе сервера и учини га неупотребљивим. Напад ускраћивањем услуга је организован тако да омета или потпуно обуставља нормално функционисање *web* сајта, сервера или других мрежних ресурса. Постоје различити начини којима нападачи то постижу.

³⁰ Ботнетови су координиране групе од неколико десетина, стотина или хиљада рачунара, заражених истим малициозним програмом, које даљински контролише „господар“ (*master*).

³¹ Richard A. Clarke, Robert Knake, *Cyber War – The next treat to National Security and What to do about it*, HarperCollins e-books, 2010, p. 21.

³² Scott J. Shackelford, *Estonia three years later: A progress report on combating cyber attacks*, Journal of Internet Law, February 2010, p. 23.

и Турске. Већина рутера у Русији и Турској су били преплављени нападима тако да се саобраћај није могао обављати. Потпуно је преузет национални домен „ge“, а корисници нису могли слати електронску пошту ван земље, нису се могли конектовати на спољне информационе ресурсе.³³

У јуну 2010. године, велику пажњу јавности привукао је *Stuxnet* – специјално направљен малициозни програм који је заразио рачунарске системе који контролишу нафтоводе, електрична, нуклеарна и друга индустријска постројења у Ирану, инфицирајући најмање 30.000 рачунара широм земље. Наведени малициозни програм прозван је првим сајбер оружјем. Према проценама стручњака, *Stuxnet* је најсофистициранији малициозни програм из домена рачунарске саботаже икад направљен.³⁴

Две године касније појавио се *Flame* (*Skywiper*), најсофистициранији малициозни програм из домена рачунарске шпијунаже, комплекснији од *Stuxnet-a*. Убрзо затим су се појавили и други, врло озбиљни, малициозни програми као што су *Mahdi*, *Gauss*, *Shamoon*, *Dark Comet* и други. Најчешће мета напада био је Иран а „нагађало“ се да иза одређених напада стоје Сједињене Америчке Државе и Израел.³⁵

Војно присуство у сајбер простору је несумњиво. Данас су сајбер напади јефтин и лак начин да једна држава нападне другу. Наведени, а и други бројни, примери показују озбиљност претњи у сајбер простору и последице које могу наступити по систем одбране земље.³⁶

ПРИМЕНА САЈБЕР РАТОВАЊА У СУКОБУ НАТО – ИРАК

Штури новински извештаји из времена трајања првог Заливског оружаног сукоба наводили су ,наводни, успех Сједињених држава у вези убацивања вируса у ирачке војне рачунарске системе.

Годину дана после завршетка операције „Пустинска олуја“ у америчкој публикацији „*US news and world report*“ објављен је чланак у ком је наведено да су амерички шпијуни успели да убаце један нов рачунарски чип у француски штампач који су Ирачани својевремено поручили од Француске.

³³ Clarke R., Knake R., *Cyber War – The next treat to National Security and What to do about it*, оп. цит., pp. 24-25.

³⁴ *EU Agency analysis of Stuxnet malware: a paradigm shift in threats and Critical Information Infrastructure Protection*, European Network and Information Security Agency, Интернет: <http://www.enisa.europa.eu> (приступљено 12.11.2017)

³⁵ *Злонамјерни програми у служби држава*, CARNet, Загреб, 2012, стр. 4-12.

³⁶ Дејан Вулетих, *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011, стр. 33-34.

Чип је у свом електронском струјном колу имао вирус чија је намена била да онеспособи главни рачунарски центар при Врховној команди ирачке војске. Чип са опасним вирусом су произвели стручњаци из америчке Националне агенције за безбедност у *Fort Midu* (држава *Merilend*). Иако не располажу поузданим доказима, стручњаци ове агенције су истицали, да верују да је опасни вирус деловао тачно онако као му је било наложено. Уз то они додају да је Пентагон пре првог заливског сукоба почео да финансира истраживачке радове о употреби рачунарских вируса за војне потребе. Истовремено са тим истраживачким радовима у Пентагону се јавила и група стручњака за рачунаре која је критиковала идеју о коришћењу рачунарских вируса у војне сврхе и захтевала забрану даљих радова у његовим лабораторијама. Из вести која је тек касније објављена, критика поменуте групе стручњака очито није дала резултата, па је тако рачунарски вирус, по свој прилици, успео да онеспособи главни рачунарски центар при Врховној команди ирачке војске.³⁷

ПРИМЕНА САЈБЕР РАТОВАЊА У СУКОБУ НАТО – СРЈ

Поједини експерти, као што је нпр. Атина Карацојани, сматрају да је сукоб 1999. године био први већи сукоб који је праћен сајбер ратовањем.³⁸ *Web* сајтови и сервери НАТО били изложени бројним нападима од стране југословенских и кинеских хакера у току агресије 1999. године.³⁹

Крајем деведесетих година прошлог века, САД је формирала и своју прву малу групу информационих ратника („хелије за информационе операције“). Тај потез је навео одређене експерте да поверују да су оружане снаге САД током оружаног сукоба у Савезној Републици Југославији (СРЈ) водиле и сајбер ратовање. Иако су амерички званичници то негирали, пензионисани генерал-мајор Дојли Ларсон, који је био командант Команде за електронску заштиту ваздушних снага осамдесетих година прошлог века је истицао да је био уверен да су САД изводиле нападе на српске информационе системе, указујући да су и САД биле све време нападане од стране различитих нападача.⁴⁰

³⁷ Наводи из: Бошко Родић, *Интеракција јавних рачунарских мрежа и рачунарских мрежа специјалних институција (докторска дисертација)*, Војнотехичка академија, Београд, стр. 26.

³⁸ Athina Karatzogianni, *The Politics of Cyberconflict*, Routledge, London, 2006, p. 155.

³⁹ *Centre of Excellence Defence Against Terrorism, Responses to Cyber Terrorism*, IOS Press, Ankara (Turkey), 2007, p. 121; Allen D. Patrick, *Information Operations Planning*, Artech House, Boston-London, 2007, p. 8.

⁴⁰ Слободан Петровић, *Компјутерски криминал*, МУП Републике Србије, Београд, 2001, стр. 362.

Током НАТО агресије на СРЈ, Пентагон је разматрао напад на српске рачунарске мреже да би ометао војне операције и основне функције друштва. План за предузимање информационих операција је био коначно припремљен и одобрен средином оружаног сукоба. План је укључивао примену различитих облика информационог ратовања у којем је значајно место заузимало и сајбер ратовање.⁴¹

У вези НАТО агресије на СРЈ интересантан је и податак да је средином те агресије Министарство одбране САД издало смернице (*An Assessment of International Legal Issues in Information Operations*) које су упозоравале да би употреба сајбер оружја могла изложити одређена лица у САД каснијим оптужбама. Смернице су сугерисале командантима да приликом напада на информационе инфраструктуре примењују исте принципе закона рата које примењују код коришћења бомби и ракета, а који подразумевају да се гађају само циљеви који су војног карактера, минимизирајући колатералну штету и избегавајући насумичне нападе.⁴² Документом се, такође, сугерише да у оружаном сукобу сајбер нападе смеју вршити само припадници оружаних снага. Такође, формулисано је да пре започињања сајбер напада команданти морају пажљиво да процене потенцијалну штету за одабрани циљ као што се у Пентагону процењују губици у људству класичним наоружањем.⁴³

Од таквих акција Пентагон се уздржао због континуиране неизвесности и лимитираног амбијента у коме би се реализовао тај облик информационог ратовања. С друге стране, званичници Министарства одбране САД су истицали да су правне недоумице и ограничења били једни од разлога зашто су се амерички званичници уздржали од сајбер напада на Југославију. Други разлози су укључивали, у то време, ембрионално стање америчког арсенала за сајбер напад и његову недовољну истестираност, као и децентрализовану природу неких југословенских система, који нису представљали погодне мете за сајбер напад.⁴⁴

ЗАКЉУЧАК

Оружана сила, односно рат који представља најгрубљи вид њене употребе, представља крајње средство у међународним односима које државе, али све више и недржавни актери, користе за постизање сопствених циљева. Савремена ратна пракса указује да утицај процеса глобализације, техничко-

⁴¹ *Ibid.*

⁴² *Ibid.*

⁴³ Слободан Петровић, *Кибертероризам*, Војно дело бр. 2, ГШ ВЈ, Београд, 2001, стр. 117.

⁴⁴ Слободан Петровић, *Компјутерски криминал*, оп. цит, стр. 362.

технолошког развоја, а посебно информатичке револуције, резултује нетрадиционалним формама сукоба у којима се чини да примена оружане силе, као основни и неизоставни садржаја рата, све више губи на свом значају. Оперативно окружење у којима се одвијају савремени сукоби се знатно изменило те се војној моћи, традиционално схваћеној као способности употребе оружане силе у постизању националних интереса, смањује ефикасности. Самим тим, војна опција решавања спорова међудржавних спорова као и спорова на релацији држава и недржавних актера, се чини „све мање привлачном”, односно ризичном, неизвесном и скупом.

Негативни став домаћег јавног мњења, услед финансијских трошкова и људских губитака, све више утиче на доносиоце политичких одлука великих сила у смеру избегавања покретања и вођења рата. Свакако да је и став међународне заједнице од велике важности за доносиоце политичких одлука. Посматрајући са становишта недржавних актера, класични приступ вођењу рата кроз примену оружане борбе у сукобу са супериорнијим противником је неефикасан. Из тих разлога прибегава се комбинованом методу супростављања у којима су невојни садржаји доминантнији у односу на војне. Наведени, као и многи други разлози неефикасности класичних, оружаних приступа решавању међународних проблема допринели су томе да државе, и недржавни актери, све више примењују нетрадиционалне приступе у савременим сукобима како би остварили сопствене интересе. Тежиште, у савременом сукобу, се помера са оружаних на неоружане садржаје. Оружано насиље, као до сада примаран и доминантан садржај, потискује се на сам крај, постаје крајње средство самог сукоба, док информациона димензија ратовања све више добија на значају.

Анализом савремених сукоба може се закључити да су савремени сукоби све чешће праћени значајном информационом активношћу. Различити облици информационог ратовања ескалирају у запремини, софистицираности и координацији. Услед тренда све веће економске, војне и уопште друштвене зависности од информационо-комуникационе технологије и тренда међусобног повезивања рачунарских мрежа, сајбер ратовање као облик информационог ратовања представља еклатантан пример вођења савремених сукоба.

Претње у сајбер простору карактерише изразита динамичност и велики број појавних форми. Претње у сајбер простору представљају све већу друштвену опасност због сталног усавршавања техника, релативно једноставног извршења одређених дела као и велике базе одакле се регрутују починиоци. Тешко је дефинисати претње у сајбер простору као што је и тешко идентификовати извор и мотив нападача.

У модерном друштву је дошло до промене природе рачунарских напада – напади све малициознији, боље координирани, софистициранији. Све већа расположивост и приступачност алата за напад као и релативно ниска цена

омогућава скоро сваком да изврши напад. С друге стране цена детектовања, опоравка, одговора је знатно већа.

Због наглашене комплексности информационо-комуникационих технологија и велике међузависности, националне инфраструктуре које повезују, покрећу и опслужују рачунари, постале су изузетно осетљиве, и, ако се организовано нападну, могу се проузроковати далекосежне последице. Друштва су закорачила у све већу глобализацију, и по питању рачунарских мрежа, што је повећало њихову осетљивост и рањивост на потенцијалне нападе.

ЛИТЕРАТУРА

- Arquilla, John, David Ronfeldt, *Мрежни рат и кибер рат*, RAND корпорација, извод из студије објављене у „Comparative Strategy”, Volume 12, 1995.
- Алексић, Живојин, Миловановић Зоран, *Лексиком криминалистике*, Глосаријум, Београд, 1995.
- Van Creveld, Martin, *The Transformation Of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*, The Free Press, 1991.
- Вулетић, Дејан, *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011.
- Вулетић, Дејан, *Безбедност у сајбер простору*, Медија центар „Одбрана”, Београд, 2012.
- Гаћиновић, Радослав, *Примена силе у међународним односима*, Српска политичка мисао, Београд, број 3-4/2007, год. 14. vol. 19.
- Gray, Colin S., *War, Peace, and International Relations: An Introduction to Strategic History*, Abingdon, UK: Routledge, 2007.
- Доктрина Војске Србије*, Медија центар „Одбрана”, Београд, 2010.
- Domitru Ducaru, Sorin, *The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO*, Europolity, vol. 10, no. 1, 2016.
- Злонамјерни програми у служби држава*, CARNet, Загреб, 2012.
- Joint Publication 3-13 Information Operations*, Joint Chief of Staff, USA, 2014, p. GL-3; *Information operations*, Air Force Policy Directive 10-7, Department of the Air Force, USA, 2014.
- Kaldor, Mary, *New & Old Wars: Organized Violence in a Globalized Era*, Stanford University Press, California, 1999.
- Kaplan, Fred, *Dark Territory: The Secret History of Cyber War*, Simon&Schuster, US, 2016.
- Karatzogianni, Athina, *The Politics of Cyberconflict*, Routledge, London, 2006.

- Kegli, Čarls, Vitkof Judžin, *Svetska politika – Trend i transformacija*, Centar za studije Jugoistočne Evrope, FPN, Diplomatska akademija MSP SCG, Izdavačko i grafičko preduzeće Prometej, Beograd, 2004.
- Keohane, Robert, Nye Joseph, *Power and Interdependence*, International Organization, Vol. 41, No. 4, Autumn, 1987.
- Latiff, H. Robert, *Future War – Prepare for the new global battlefield*, Penguin Random House, US, 2017.
- Мишовић, Слободан, Ковач Митар, *Систем одбране*, Факултет цивилне одбране, Београд, 2006.
- Милашиновић, Радомир М., Милашиновић Срђан М., *Основи теорије конфликта*, Факултет безбедности, 2007.
- Микић Слободан Б., *Поглед на рат*, ВИЗ, Београд, 2003.
- Naj Džozef, *Paradoks američke moći*, BMG, Beograd, 2004.
- Patrick, D. Allen, *Information Operations Planning*, Artech House, Boston-London, 2007.
- Петровић, Слободан, *Кибертероризам*, Војно дело бр.2, ГШ ВЈ, Београд, 2001.
- Петровић, Слободан, *Компјутерски криминал*, МУП Републике Србије, Београд, 2001.
- Родић, Бошко, *Интеракција јавних рачунарских мрежа и рачунарских мрежа специјалних институција (докторска дисертација)*, Војнотехичка академија, Београд
- Strachan, Hew, *The Direction of War: Contemporary Strategy in Historical Perspective*, Cambridge University Press, UK, 2013.
- Schmitt, N. Michael, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, UK, 2013.
- Schvarzenberger, Georg, *Power Politics*, London, Stevens, 1951.
- Shackelford, Scott, *Estonia three years later: A progress report on combating cyber attacks*, Journal of Internet Law, February 2010.
- Thucydides, *History of Poloponesian War*, Penguin Books, New York, 1972.
- FM 3-0 Operations*, Headquarters Department of the Army, Washington, DC, June 14th, 2001.
- Hammes, Thomas X., *Fourth Generation War and Other Myths*, U.S. Army War College, Strategic Studies Institute, November 2005.
- Heickero, Roland, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency, Stocholm, 2010.
- Centre of Excellence Defence Against Terrorism*, Responses to Cyber Terrorism, IOS Press, Ankara (Turkey), 2007.

- Clarke A. Richard, Knake Robert, *Cyber War – The next treat to National Security and What to do about it*, HarperCollins e-books, 2010.
- Cohen, A. Eliot, *The Big Stick: The Limits of Soft Power and the Necessity of Military Force*, Basic Books, New York, 2017.
- Yuichiro, Nagao, *Unconventional Warfare: A Historical Perspective*, in: *Essence of Military Power: At the Dawn of the 21st Century* The National Institute for Defence Studies, Ministry of Defence of Japan, 2001.

CYBER WARFARE CHANGE OF THE PHYSIOGNOMY OF CONTEMPORARY CONFLICTS

Dejan Vuletić
Milinko Vračar

Abstract: War, as a destructive social phenomenon is the most severe form of the use of force in international relations. The characteristics of contemporary conflicts indicate the essence of war has changed. The military power of states, expressed through the use of the armed force, increasingly shows its inefficiency in the achievement of foreign policy interests. The declining trend of its efficiency can be explained by the impact of the globalization process and the information revolution on social trends, which has significantly changed the operational environment in which contemporary conflicts occur. Globalization led to the growing influence of non-state actors in international politics. According to that, international relations transformed into global ones. On the other hand, the information revolution led to the emergence of a new dimension of the conflicts. As a form of information warfare, the cyber warfare is an obvious example of modern conflicts.

Key words: force and power, international relations, contemporary conflict, information warfare.