KNOWLEDGE – International Journal
Vol. 28.6
December, 2018

THE NEW SECURITY CHALLENGES OF INFORMATION WAR

Olga Zoric
Academy "Dositej", Belgrade, Serbia, olgazoric@yahoo.com
Katarina Jonev
Faculty of political sciences, Belgrade, Serbia, jonev.katarina@gmail.com
Ivan Rancic
Faculty of engineering management, Belgrade, Serbia, ranca76@gmail.com

Abstract: The author starts from the informational dimension of the operational environment in a strategic reality and deal with the problem of defining informational power from the theoretical and practical aspect of information warfare.
The deliberations in the work are aimed to initiate a procedure for auditing of the security documents in order to create a legal basis for the operationalization of the content of information security, as one of the aspects of integral security of the Republic of Serbia. The paper deals with the conceptual determinations and importance of information, information warfare and information operations, as well as the content of information warfare, pointing out the strategic and doctrinal definitions of the information warfare of the United States of America, the Russian Federation and the Republic of Serbia. It is necessary to accurately and objectively observe world achievements in the field of national security and the relation of the most powerful world powers to the problem of information warfare. Based on a comparative analysis of world trends and the state of the theoretical and practical aspects of information security of the Republic of Serbia, the focus is on work, where measures are proposed to improve the security function in the fourth unit of work.
Keywords: operational environment, information, information warfare, Republic of Serbia, Russian Federation

НОВИ БЕЗБЕДНОСНИ ИЗАЗОВИ ИНФОРМАЦИОНОГ РАТОВАЊА

Олга Зорић
Akademija „Dositej, Beograd, olgazoric@yahoo.com
Катарина Јонев
Факултет политичких наука, Београд, jonev.katarina@gmail.com
Иван Ранчић
Факултет за инжињеријски менџмент, Београд, ranca76@gmail.com

Сажетак:Аутору у раду полазе од информационе димензије оперативног окружења у стратегијској стварности и бави се проблемом дефинисања информационе моћи са теоријског и практичног аспекта информационог ратовања.
Разматрања у раду имају за циљ покретање поступка за ревидирање полазних докумената у области безбедности како би се створио правни основ за операционализацију садржаја информационе безбедности, као један од аспеката интегралне безбедности Републике Србије. У раду су обрађена појмовна одређења и значај информације, информационог ратовања и информационе операције као и садржаји информационог ратовања, указујући на стратегијско-доктринарна опредељења о информационом ратовању Сједињених Америчких Држава (САД), Руске федерације (РФ) и Републике Србије. Потребно је прецизно и објективно сагледати светска достигнућа у области националних безбедности и однос најмоћнијих светских сила према проблему информационог ратовања. На основу компаративне анализе светских трендова и стања теоретских и практичних аспеката информационе безбедности Републике Србије, тежиште је рада, где су предложене мере за унапређење безбедносне функције у четвртој целини рада.
Кључне речи: оперативно окружење, информација, инфромационо ратовање, Република Србија, Руска федерација.

1.УВОД

Стратешко опредељење да постане кључан елеменат стабилности и мира у региону Западног Балкана, Република Србија потврђује континуираним процесом изградње безбедносног система. Савремене државе своје полазне теоријске и практичне претпоставке припрема у области безбедности и одбране, је потребно

да искажу у законима, општим актима и другим прописма из области одбране, у основним стратегијско-доктринарним документима, плановима одбране, финансијским плановима одбране и плановима и програмима развоја и функционисања система безбедности и одбране. Органи законодавне и извршне власти Републике Србије су у протеклих десет година предузели велики број мера и активности у спровођењу реформе система безбедности и одбране, чиме су обезбеђене потребне претпоставке за стабилно функционисање система одбране у миру, ванредном стању и рату.

При теоријском разматрању стратегијског концепта безбеднсоти,[167] гм Митар Ковач преузео је енглески модел где су дефинисани инструменти националне моћи (економски, дипломатски и војни). Приступ Сједињених америчких држава подразумева модел где су дефинисани економска, дипломатска, војна и информациона моћ. Овакав приступ је свеобухватнији и даје могућност потпунијег дефинисања безбедносног окружења.

У складу са основним опредељењима Политике националне безбедности Републике Србије да развија и унапређује све аспекте безбедности, а као последица израженог развоја информационо-комуникационе технологије, настаје потреба за изменама и допунама Стратегије националне безбедности и Стратегије одбране Републике Србије.

2.ИНФОРМАЦИЈА, ИНФОРМАЦИОНО РАТОВАЊЕ И ИНФОРМАЦИОНА ОПЕРАЦИЈА

Информација је појмовно одрђење чињеница у објективној стварности које су у мисаоном процесу претпоставке. Што је количник претпоставки и чињеница ближи вредности један то је већа вероватноћа достизања жељеног циља. Целокупан друштвени живот савремене људске цивилизације све више је зависан од процеса у информационим системима.[168] Извршавање функција савремене државе условљено је подацима односно информацијама. Податак је било какав запис у било ком облику, којим је записан неки догађај, појава, чињеница или запажање из околине. Подаци могу бити текстуални, нумерички, знаковни, сликовни и звучни. Информација је податак који се користи, који за примаоца има одређени ефекат односно значење и истовремено знање које се може добити из података. Подаци који се не користе или прималац их не разуме нису информације, (на пример књига је скуп података, али за неписменог или слепог човека то нису информације). Да би од информације имали користи, она мора бити исправна, потпуна и благовремена. Велики део техничко-технолошки проналазака је у основи имао за мотив усавршавања информационог процеса. Циљ науке је дођи до информације о узрочно-последичним везама на посматраном објекту сазнајног процеса. Мотив спознаје везе је утицај на узрок чиме се стварају услови за усмеравање објекта и достизање жељених ефеката. Брзину обраде и пренос информације, коју су омогућили комуникационо-информациони системи је узрок пресудног значаја информације у свим друштвеним процесима. Као посебан феномен ове брзине у савременом друштву је свакако *хипер инфлација информација*, односно проблем несагледиве количине информације које човек својим перцетивно-когнитивним способностима не може да обради. Овакве чињенице неминовно наводе на закључак да је значај информације непорецив јер представља са једне стране, својим квалитетом, везивно ткиво свих функција савремене цивилизације а са друге стране, својим квантитетом канцерогено ткиво појединачних функционалних процеса. Информација је потребна у свим сегментима друштвеног живота али количина и садржај морају бити урамнотежени са људским способностима о свеобухватном сагледавању, верификовању и ефективном деловању сваког појединца.

На основу константованог значаја, може се закључити да информације постају све важније за националну безбедност уопште, а посебно у оружаном сукобу. Безбедност је једна од основнх функција савремених држава. Аналогно претходним ставовима, савремени сукоби су посебно окарактерисани и као борба у димензији информација. Они који су савладали технике информационог ратовања у предности су над својим противницима. Победник је она страна која може брже да опажа, реагује, анализира и процењује ситуацију. Услед научних достигнућа долази до велике промене у начину на које су саме организације организоване да искористе повећан обим информација, као и у начинима на које се информација прикупља, чува, обрађује, предаје и приказује. Предност у комуникационо-информационом систему је неопходан

[167] Ковач М., Стојковић Д., Стратегијско планирање одбране 2009.г, стр. 230

[168] "Информациони систем је систем који прикупља, похрањује, чува, обрађује и испоручује информације важне за организацију и друштво, тако да буду доступне и употребљиве за сваког ко се жели њима користити, кључујући пословодство, клијенте, запослене и остале." (International Federation for Information Processing - IFIP, http://www.ifip.org/, приступљено дана 10.11.2015.г.)

услов за успех и победу. *Информација је постала стратегијски ресурс*. Такво стање у међународној заједници је утицало на то да се остварење интереса не врши применом оружане силе, већ другим средствима. Услед овакве појаве дошло је до другачијег тумачења сукоба, те су и настале теорије попут сукоба ниског интензитета, концепција сведимензионалног рата и мрежноцентрично ратовање. Овакво место, улога и значај информације у савременим сукобима условило је нове начине вођења сукоба, *информационо ратовање.* Захваљујући ефикасности примене садржаја информационог ратовања, оно заузима све значајније место у савременим сукобима.

У савременим сукобима интереси сукобљених страна се све више остварују невојним средствима, а све већи значај добија информација уз све учесталију примену савремене информационе технологије у војне сврхе. Анализом савремених сукоба може се доћи до сазнања о облицима примене информационог ратовања у њима.

Постизање информационе супериорности[169] и остваривање информационе доминације[170] је основни циљ информационог ратовања. Развој информатичке технологије омогућио је таква достигнућа у наоружању и пратећој опреми да је револуционарно промењен начин ратовања. Основна специфичност информационог ратовања је да бојиште информационог ратовања није физички, већ виртуелни свет, а потенцијални ратници на овом бојишту могу бити државни органи, војне организације, терористи, индустријски конкуренти, хакери и други. Сваки од ових противника је мотивисан различитим циљевима, ограничен различитим нивоима ресурса, сопственим могућностима и могућностима система да се брани.

Ради одређења "информационо ратовање" неопходно је одредити значење речи "информација" и "ратовање". Поред дефиниције појма информације у претходним разматрањима рада, овде користи се појашњење информације схватањем према Тофлеру, где "информације (знање) се као ресурс, разликују од свих других. Знање је неисцрпно. Оно може да буде употребљено истовремено од обеју страна. И оно је нелинеарно. То значи да мали инпути могу да проузрокују диспропорционалне последице. Делић праве информације може да обезбеди огромну стратегијску или тактичку предност. Недостатак делића информације може да има катастрофалне ефекте."[171]

Према Ричарду Шафранском, "ратовање је скуп свих борбених и неборбених активности које се предузимају да би се потчинила супротстављена воља противника или опонента. Циљ ратовања није увек да се противник убије, већ да се потчини. Циљ ратовања је, такође, да се увек утиче на информациони систем противника и исход информационог рата на стратегијском, оперативном и тактичком нивоу треба да буде такав да противник прими довољно порука и информација које ће га убедити да треба да престане да пружа отпор. Противник је потчињен када се понаша на начин који је коинцидентан са жељама супротне стране.“[172]

Чињеница да постоје различите дефиниције информационог ратовања, потврђује сложеност садржаја и велики обим овог појма. Један од приступа дефинише информационе системе као циљ, док је према другом то људски ум. У већини дефиниција истовремено су присутна оба приступа, а дефиниције ни у једном случају нису прецизне када су у питању извршиоци или средства. Сматра се да је најпотпунија и најприхватљивија дефиниција Ричарда Шафранског према којој је "информационо ратовање активност

---

[169] „Информациона супериорност у информационој димензији оперативног окружења представља степен остварене предности у односу на непријатеља, која омогућава сопственим и пријатељским снагама да непрекидно и сигурно прикупљају, обрађују, управљају и користе информације“. Концепт информационих операција, фебруар 2015.г. стр. 35

"Информациона супериорност је операциона предност изведена из способности да се сакупи, обради и дистрибуира непрекидан ток информација док се истовремено искоришћавају или онемогућавају непријатељски напори да то исто учини." FM 3-0 Operations, Headquartes Department of the Army, Washington, DC, June 14, 2001.

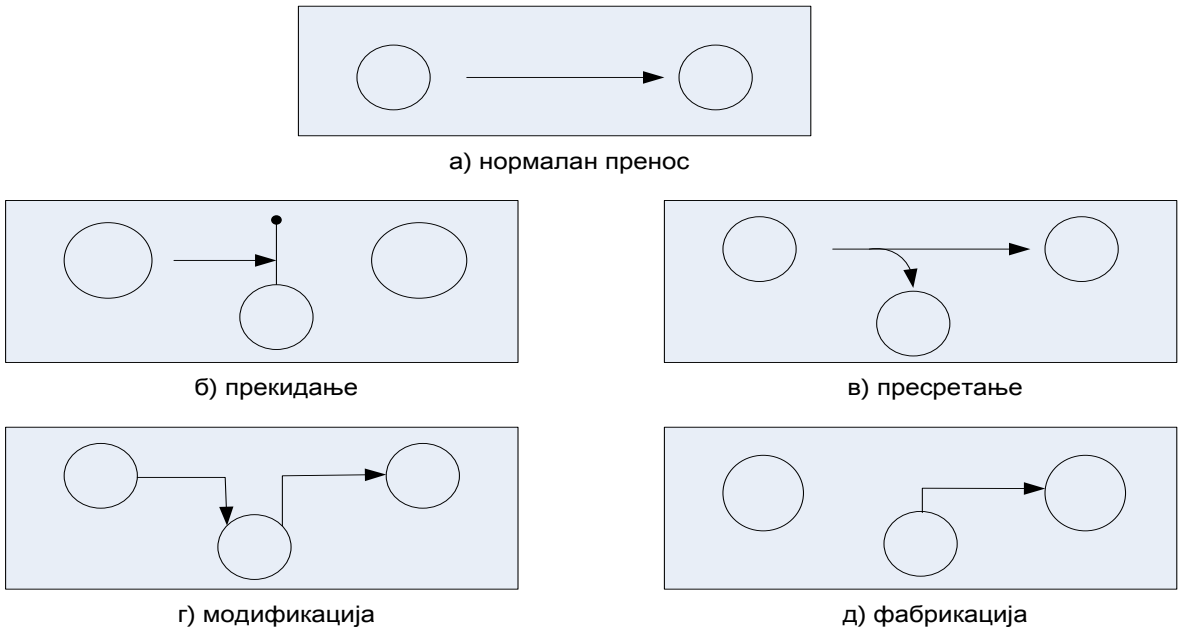
[170] „Информациона доминација подразумева степен информационе супериорности, који омогућава власнику информације да је кроз информационе системе и капцитете употреби на најбољи могући начин, с циљем остварења оперативне предности у конфликту или за потребе контроле ситуације током извођења операције, уз истовремено онемогућавање противника у предузимању истих мера.“ ФМ 3.0 Операције јун 2001.г. и јун 2005.г.

[171] Тофлер А., Рат и анти рат, Паидена, Београд, 1998, стр. 172-173.

[172] Нешковић С., Економске импликације информационог ратовања у савремених међународним односима, Економија теорија и пракса, стр. 7.

уперена против било којег дела система знања и веровања противника. Без обзира на то да ли се води против спољњег противника или унутрашњих група, информационо ратовање има крајњи циљ да употреби информациона оружја да промени (утиче, манипулише, нападне) системе знања и веровања неког спољњег противника."[173] У овом раду ће се информационо ратовање, управо, посматрати са овог аспекта.

Узимајући у обзир Столингсову класификацију напада на информације у току преноса, евидентно је да се информације у информационом ратовању, без обзира на приступ у дефинисању, могу прекидати, пресретати, модификовати и фабриковати (слика број 1).[174]



Слика 1. Класификација напада на информације[175]

Облик информационог ратовања је начин његовог експонирања и исказује се кроз структуру догађаја и активности везаних за процесе који се у њему одвијају. То значи да је облик информационог ратовања посебна карактеристика која га квалитативно разликује од других облика ратовања. У доступној литератури која се бави информационим ратовањем постоји више погледа на облике његовог испољавања од којих су најраспрострањенија схватања еминентних стручњака из те области Швартау и Либицки.

Швартау информационо ратовање класификује у три групе: 1) персонално информационо ратовање; 2) корпорацијско информационо ратовање; 3) глобално информационо ратовање.[176]

Према Либицком информационо ратовање јавља се у следећим облицима: 1) ратовање у сфери командовања и управљања; 2) обавештајно ратовање; 3) електронско ратовање; 4) психолошко ратовање; 5) хакерско ратовање; 6) економско-информационо ратовање; 7) кибер ратовање.[177] Сви ти облици су повезани, међусобно условљени и у збиру њихивог појединачног деловања чине синергију повољних услова за успешну информациону доминацију на непријатељем.

Као и други облици ратовања тако се и информационо реализује извођењем операција.

Активности информационих операција[178] су: психолошко-пропагандне активности, обмањивање, електронска дејства, активности у сајбер простору, физичко уништење и мере физичке и техничке заштите.“[179]

---

[173] исто стр. 8
[174] Војно дело 3/2012.г. стр. 167
[175] исто стр. 167
[176] Петровић С., Компјутерски криминал, МУП Републике Србије, Београд 2001.г. стр.53
[177] Libicki, M., http://www.ndu.edu/inss/books/Books1990to1995/What_is_IW_Aug_95/a003ch03.html приступ интернет страници 30.11.2015. г.
[178] „**Информациона операција** представља низ активности и мера које се предузимају по јединственом плану ради остварења жељеног утицаја на вољу, разумевање услова и способност за адекватним деловањем учесника у оперативном

Ставови у Концепту информационих операција који је усвојен у фебруару 2015. године, заснивају се на определењима концепта тоталне одбране, а ради развоја способности Војске Србије као дела снага одбране Републике Србије за планирање, припрему и извођење активности у информационој димензији оперативног окружења.

3. СТРАТЕГИЈСКО-ДОКТРИНАРНИ АСПЕКТИ ИНФОРМАЦИОНОГ РАТОВАЊА

Информационо ратовање, својом применом, представља безбедносни проблем и један од озбиљнијих безбедносних изазова у двадесет првом веку, како за високоразвијене тако и за све остале државе. У суштини, најбитнији помак се чини у брзини ратовања, јер дигитализована борбена опрема и системи омогућују прецизно познавање тренутне борбене ситуације, непосредан (шематски и визуелан) увид у ток борбених дејстава, физичку контролу над употребљеним снагама и веома брзо преношење информација до непосредних корисника. Заједничка безбедносна комисија Владе САД је 1994. године рањивост на информационо ратовање описала као највећи безбедносни изазов последње декаде двадесетог века и можда двадесет првог века и да се морају формирати снаге и пронаћи начини борбе против такве врсте опасности. Војска САД формирала је центар за информационо ратовање. Немачка и Велика Британија су основале сличне организације, као што има још десетак других земаља, укључујући Кину и Русију, које имају мање формалне, али не мање активне структуре за информационо ратовање.

САД су најраније и најсвеобухватније почели да разматрају теорију и праксу везану за информације и информациону безбедност. „Посматрајући кроз историју се прво шездесетих година прошлог века појавио израз комуникациона безбедност (*COMSEC - communication security*). Са појавом персоналних рачунара, седамдесетих година прошлог века, настала је рачунарска безбедност (*COMPUSEC - computer security*), а крајем осамдесетих година прошлог века *COMSEC* и *COMPUSEC* су обједињене у **информациону безбедност** (*INFOSEC - information security*).“[180] Информациона безбедност је покушала да интегрише раније одвојене безбедности, као што су безбедност особља, рачунарска безбедност, комуникациона безбедност и оперативна безбедност. Тежиште *INFOSEC* је стављено на спречавање не ауторизованог приступа информационим системима. Разматрана је, пре свега, поверљивост (*confidentiality*), интегритет (*integrity*) и расположивост (*availability*) информација.

Значај информација и информационе сфере, те потребе за обезбеђивањем информационе безбедности, поред САД и земаља Европске уније, у задњих две деценије почеле су озбиљно да уважавају и остале државе у свету, а међу њима и Руска Федерација (РФ) и Република Србија.

Према речнику националне информационе сигурности САД информациона безбедност је "заштита информација и информационих система од неовлашћеног приступа, употребе, откривања, разбијања, измене или уништавања, а да би се обезбедила поверљивост, интегритет и расположивост".[181] За САД, информационо ратовање представља нов начин у војном размишљању и уноси револуционарне промене у целокупну војну мисао и начин ратовања.

Озбиљно разматрање појма информационе безбедности (*информационноя безопасностъ*) у Руској Федерацији (РФ) је од 90-их година прошлог века. „Према неким руским ауторима бивши СССР је изгубио хладни рат, добрим делом, због занемаривања безбедности у информационој сфери. “[182] У највишем стратегијском документу РФ јасно је препознала значај информационе безбедности као и могућности угрожавање исте. Као одговор на савремен изазове, ризике и претње по безбедности дефинисане су потребне снаге и њихове способности за успешно супростављање.

Полазна основа при разматрању стратегијско-доктринарне и нормативно-правне изграђености информационог ратовања свакако је анализа одређености овог појма у Републици Србији. Стратегијом националне безбедности између осталих дефинисани су изазови, ризици и претње.[183] Ово су полазна

окружењу. Ове операције се планирају, припремају и изводе у миру, ванредном и ратном стању.“ Концепт информационих операција, фебруар 2015.г. стр.13

[179] исто стр.13

[180] Daniel G. Wolf, Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development, Nacional Security Agency US, Juli 22, 2003. г.,

[181] Committee on National Security Systems, National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, USA, 26 April 2010. г.,

[182] Панарин И., Н., Проблемы обеспечения информационной безопасностъ. Москва, 1998. г.,

[183] "Обавештајна делатност коју стране обавештајне организације спроводе кроз незаконито и прикривено деловање, представља реалну претњу безбедности Републике Србије. Остварује се кроз слабљење њених

упоришта за свеобухватније дефинисање проблем информационе безбедности односно информацоног ратовања у највишем стратегијском документу.

У Стратегији одбране Републике Србије у поглављу 1. Безбедносно окружење прописано је: "Снажан *развој информационо-комуникационе технологије* и интензивирање економских интеграционих токова убрзали су глобализацију скоро свих аспеката међународних односа....“.[184]

Ове одредбе говоре о новим детерминантама безбедносног окружења услед снажног развој информационо-комуникационе технологије и убрзане глобализације али свеукупне одредбе Стратегије одбране не дефинишу адекватне одговоре на овакве нове услове угрожавања безбедности.

У поглављу 2. Изазови, ризици и претње одбрани Републике Србије[185] и у поглављу 4. Политика одбране Републике Србије[186] прописано су одредбе које говоре о новим изазовима, ризицима и претњама одбрани Републике Србије али нема полазних основа за прописивање мера које би се супроставиле оваквим претњама и спречиле угрожавање безбедности. Ове одредбе дају право и обавезу да се у овим документу дефинишу полазна начела значаја и улоге информационе моћи, која би се операционализовала у доктринарним документима. Потребно је прописати Доктрину информационих операција.

4. ПРАКТИЧНА ИЗГРАЂЕНОСТ ИНФОРМАЦИОНОГ РАТОВАЊА

Полазна основа при разматрању практичне изграђености информационог ратовања свакако је анализа теоријске одређености овог појма у Републици Србије. Недовољна стратегијско-доктринарна и нормативна-правна изграђеност утицала је негативно на практично спорвођење мера и активности у области информационе безбедности. Потребно је најпре извршити доградњу теоријских аспеката информационог ратовања, а након тога исте имплементирати кроз снаге и средства за практично спровођење мера и активности информационог ратовања.

Због великог броја начина испољавања и обимности садржаја информационог ратовања, при анализи практичне изграђености информационог ратовања у области безбедности Републике Србије, биће разматран део садржаја односно елктронско и сајбер ратовање као и пример корпоративне безбедности компаније НИС.

Увод у практичну изграђеност електронског ратовања у области безбедности Републике Србије свакако је у историјској анализи снага и средстава које су започеле реализацију садржаја противелектронске борбе после Другог светског рата, као специјализоване организацијско-формацијске јединице Југословесне армије.[187] Војне снаге и средства за електронско ратовање на простору бивше Социјалистичке Федеративне

политичких, економских и безбедносних капацитета и кроз утицај на смер и динамику друштвених процеса, супротно националним интересима. Комбинација традиционалних обавештајних метода са средствима *софистицираних могућности отежава откривање њиховог деловања*....Тенденција повећаног коришћења *информационо-комуникационих технологија праћена је константним повећањем ризика од високотехнолошког криминала и угрожавања информационих и телекомуникационих система.* Ризик у овом погледу постоји од угрожавања споља, али и у могућности злоупотребе података о грађанима и правним лицима.... Присутни су и други ризици и претње безбедности, са мањом или већом вероватноћом испољавања и препознавања, као што су: злоупотреба *нових технологија и научних достигнућа у области информатике,* генетског инжењеринга, медицине, метеорологије и других научних области....“. СВЛ 31/09, стр. 703

[184] СВЛ 31/09, Стратегија одбране Републике Србије, стр. 716

[185] „Развојем савремених информационих технологија које су битан део системског уређења и остваривања функција државе, настају нове околности за деловање различитих група и недржавних актера у остваривању њихових циљева. На тај начин може да дође до угрожавања функционисања битних елемената система одбране кроз деловање сајбер претњи. Због тога је неопходно континуирано развијати технолошку и процедуралну заштиту елемената система одбране на свим нивоима организовања..“ исто , стр. 718

[186] „Ставови политике одбране представљају основу за израду нормативних и доктринарних докумената. Операционализацијом тих ставова стварају се услови за њихову примену у процесу достизања утврђених циљева политике одбране...“. исто, стр. 718

[187] Прва јединица за противелектронску бору (ПЕБ) формирана 11.11.1946. године, радио-извиђачка чета Југословенске армије, (овај дан је прихваћен за Дан рода јединица за ЕД, прим. аутора), а користећи стечена искуства, убрзани развој радио-извиђачких јединица материализује се формирањем радио-извиђачких

Републике Југославије, свој максимум су достигле 80-тих година прошлог века. У том периоду ове снаге су биле организоване на тактичком нивоу као самостални водови-чете, на оперативном као самосталне чете-батаљони и на стратегијском нивоу као јединице ранга пука. У том периоду оперативни распоред јединица за противелектронску борбу обезбеђивао је извршавање наменских стратегијских, оперативних и тактичких мирнодопских и ратних задатака. Размештај организацијских елемената јединица за ПЕБ и њихова опрема обезбеђивала је потпуну доминацију у електромагнетном спектру и задовољавала успешно супростављање свим изаовима, ризицима и претњама тог периода.

На примеру историјске анализе настанка, развоја и нестанка јединице за електронско ометање може се практично сагледати недовољна пажња система безбедности за информациону безбедност. Наиме од 148. вода за активна електронска дејства, јула 1976. године у Ужицу, формира се 50. самостална чета за противелектронско обезбеђење, која 1978. године улази у састав 398. пука везе а 1985. године прераста у 50. батаљон за противелектронска дејства. Овај батаљон 1990. године добија нови формацијски назив - батаљон за електронско ометање при 224. центру за извиђање и ометање. Формацијским променама које су наступиле у току ратног периода 1999. године, јединица је преименована у 4. центар за противелектронска дејства при 224. центру за ЕИ и ПЕД, Управе за ЕИиПЕД, Сектора за везу, информатику и ЕИиПЕД. Након преформирања и предислокације из Ужица у Београд 2006. године, јединица је задржала ранг батаљона али је након преформације 224. центра за ЕД 2010. године ова јединица је расформирана.[188] Губитак оперативних способности које једино може да има оваква јединица, систем безбедности можда не би приметио да се није појавио терористички акт употребе дрона на фудбалској утакмици у Београду између Србије и Албаније. Овај врло велики ризик по систему безбедности је очигледан пример недовољне изграђености снага за електронско ратовање и налаже ургентну потребу за предузимање мера, јер наредни сличан акт могуће да прерасте у претњу по живот и здравље свих становника Републике Србије.

Задатак да се одгонетне шта је сајбер оружје и сајбер ратовање није ни мало једноставан, а последице њиховог утицаја могу бити тешке чак и катастрофалне како по деловима тако и за целу државу. Упркос заједничком интересу многих влада широм планете, стручњаци за сајбер домен верују да је концепт сајбер оружја превише „апстрактан“ и из тог разлога постоји бојазан да се према сајбер оружју државне институције односе подцењивачки и да немају свест о правој опасности које сајбер оружје може да нанесе. Главни аргументи за предходну тврдњу су да је до данас постојање сајбер оружја под утицајем неколико хиљада људи, сва јавно позната сајбер оружја имају далеко мању ватрену моћ него што се обично претпоставља у јавности и сајбер оружје се може користити у комбинацији са средствима НВО. Сајбер простор ће се дубоко променити, а са њим и концепт сајбер безбедности. Очигледно је да главни адут свих претњи у сајбер простору јесте сајбер оружје које се креира писањем програмског кода у неком програмском језику са пред припремним активностима – обавештајним радом и креираном методологијом за напад од једне или више сајбер ћелија.

Субјекти система безбедности (државна администрација, војска, полиција и приватни сектор) морају улагати у развој сајбер јединица – ћелија, да би спремани дочекали изазове сајбер напада, не потцењујући могуће ризике. Да би се могућност одбране од сајбер оружја у рачунарске и телекомуникационе системе као и „увреда“ дигиталних ресурса Војске Србије свела на минимум потребно је испитати сваки софтвер преко метода и линија кода. Скромни су организацијско-формацјски капацитет јединица и установа Војске Србије за успешно вођење сајбер ратовање. Прописано је око десетак фромацијски места[189] у Војсци Србије. У Центру за командно-информационе системе прописана је организацијска јединица за сајбер ратовање а у бригади везе два формацијска места за сајбер заштиту.

У Техничко опитном центру прописана је организацијска јединица за испитивање софтвера у систему одбране. Припадници ове групе би требали свакодневно да прикупљају информације о новим малверима, њиховом деловању, логици рада и могућој штети коју могу да проузрокују. Ова организацијска целина за оцену квалитета софтвера у ТОЦ-у мора имати кључну улогу у одбрани информационих система и дигиталних ресурса Војске Србије од могућих сајбер напада коришћењем сајбер оружја. Софтвери који се испитују могу бити самостални као средство или су део средстава НВО. Лабораторија има могућност да по

батаљона у армијским областима, ратном ваздухопловству и ратној морнарици а 30.01.1957. године формира се радио-извиђачки центар ГШ, примедба аутора.

[188] Монографија 4.цПЕД, "Графопринт"-Ужице 2005. г.,

[189] што не значи да су сва попуњена, примедба аутора,

пријему задатка за испитивање преузме софтвер у изворном коду[190], приступи комплетном програмском коду, да га отвори и да прође кроз сваку линију кода, да анализира сваки метод одвојено или у целини.

Овој тематици потребно је да надлежни управни органи посвете далеко већу пажњу или можда боље речено да прихвате чињеницу да **смо сви међусобно повезани свесно или несвесно на огромној глобалној мрежи, тако да онај ко контролише мрежу, контролише све нас и контролише свет.**

Компанија Газпром Њефт (*Gazprom Neft*) је државно-државна компанија у власништву РФ и Републике Србије. Ова комапнија је практичан пример односа према проблему свеукупне безбедности привредног субјекта, а тако и према информационој безбедности, који је у складу са доктринарним документима РФ. По Доктрини информационе безбедности РФ, обавезе у области информационе безбедности нису само обавеза и одговорност државних органа власти или неких државних специјализованих институција за ову област, већ сваког појединца, групе, институције, привредног субјекта РФ.

У организационом делу "НИС МАТИЦА" компаније НИС налази се Функција за корпоративну заштиту.[191] У оквиру Функције за корпоративну заштиту налази се Дирекција за корпоративну заштиту[192] у чијој одговорности је економска безбедност, физичко-техничко обезбеђење, **заштита информација** и одбрамбене припреме[193] компаније НИС. Заштита информација се остварује кроз заштиту података, заштиту комуникационе инфраструктуре и контролу апликативних решења. У оквиру заштите података компанија НИС израдила је и усвојила Стратегију заштите информација у НИС, израдила је више нормативних аката која ближе регулишу заштиту података (службена, пословна, војна и државна тајна) и увела обавезно вођење Поверљивог деловодства.[194] У оквиру заштите комуникационе инфраструктуре користе се решења која спречавају неовлашћени приступ рачунарској мрежи и информатичким ресурсима НИС, софтверска решења која обезбеђују заштићену комуникацију у оквиру информатичких ресурса НИС, откривање и превенцију неовлашћених приступа рачунарској мрежи, као и строгу контролу корисничког приступа. Контрола апликативних решења обухвата контролу сигурности апликација чиме се спречава деловање злонамерног софтвера на пословне информације у НИС, као и строго поштовање и извршавање процедура за чување и архивирање пословних информација НИС.

Поред напред наведеног, у понашању НИС су прописане још две обавезе које су, поред осталог, и у служби информационе безбедности. Прва је безбедносна провера особља која се проводи при пријему у радни однос, као и касније током рада запослених у НИС. Друга активност је безбедносна провера добављача, опреме и софтвера, при набавци информатичке и телекомуникационе опреме, опреме за информатичку и телекомуникациону инфраструктуру и софтвера. Ова безбедносна провера постала је пракса НИС након куповине већинског дела акција НИС од стране Газпром Њефт.

5.ПРЕДЛОГ ЗА СТРАТЕГИЈСКО-ДОКТРИНАРНО УРЕЂЕЊЕ И ПРАКТИЧНЕ ИЗГРАДЊЕ КОНЦЕПТА ИНФОРМАЦИОНОГ РАТОВАЊА У ОБЛАСТИ ОДБРАНЕ РЕПУБЛИКЕ СРБИЈЕ

У циљу стварања бољих услова за практичну изграђеност информационе безбедности а на основу анализе која је извршена у овом раду, предлог за теоријску основу при стратегијском планирању одбране и дефинисању националне моћи је усвајање модела који заступају САД. У моделу САД је прихваћена идеја да на стратегијском нивоу државе националну моћ чини дипломатска, економска, војна и информациона моћ.[195] На основу овог теоријског модела потребно је извршити измене и допуне Стратегије националне безбедности РС и створити предуслове за доктринарну разраду информационих операција. Активности информационих операција у доктрини операција прилагодити активностима дефинисаним у усвојеном Концепту информационих операција.

[190] у току је припрема и писање стандарда који ће дефинисати боље уговорне услове за купца – Војске Србије и обавезе продавца, примедба аутора,

[191] Презентација "НИС а.д Нови Сад - организација, делатност, капацитети и технолошки процеси производње". Посета седишту компаније НИС, Нови Сад, 28.10.2015. године.

[192] Презентација "Ризици и безбедоносни аспекти дистрибуције нафте и нафтних деривата". Посета седишту компаније НИС, Нови Сад, 28.10.2015. године.

[193] исто

[194] исто

[195] Ковач М., Стојковић Д., Стратегијско планирање одбране 2009.године, стр.243-244

У складу са усвојеним концептом информационог ратовања потребно је извршити анализу свеобухватности и актуелности концепта, и приступити изради доктрине информационе операције и дефинсати носице активности информационог ратовања који ће израдити студију одрживости и развоја појединих садржаја информацоног ратовања.

Психолошко-пропагандне активности потребно је планирати, припремати и реализовати ради остваривања жељеног утицаја на свест, морал и емоције непријатеља а у складу са следећим начелима: „усмереност на мисију, усмереност на релевантне учеснике, истинитост и повезаност.“[196]

Активност обмањивање вршити ради стварања погрешне представе код непријатељевих команданата о оперативном окружењу а у складу са следећим начелима: „усмереност, централизовано планирање и контрола, безбедност и заштита сопствених планова, временска осетљивост и интеграција.“[197]

Све већи ризик по систему безбедности од масовне употребе електронских средстава и изражена претња нарушавања способности одбрамбеног система за успешно супростављање савремено наоружаним непријатељима, захтевају модерно опремљене и добро организоване јединице за електронска дејства.

Активности у сајбер простору потребно је планирати, припремати и реализовати ради ометања, прекида и уништења непријатељевих информационих и рачунарских система, одбране од ометања, прекида и уништења и несметаног коришћења сопствених и пријатељских информационих и рачунарских система. За успешну реализацију задатака потребно је организацијска јединица са минимум петнаест формацијских места чиме би се креирала дефанзивно - офанзивна ћелија - лабораторија за сајбер одбрану војних рачунарских, телекомуникационих система и дигиталних ресурса. Тиме би се у потпуности могло да одговори на могуће нападе споља и изнутара од једне или више сајбер ћелија из иностранста али и домаћих хакера.

ЗАКЉУЧАК

При стратегијском планирању одбране и дефинисању националне моћи Републике Србије потребно је усвојити теоријски модел националне моћи који заступају САД. На стратегијском нивоу националну моћ Републике Србије требало би да чине дипломатска, економска, војна и информациона моћ.

На основу овог теоријског модела потребно је извршити измене и допуне Стратегије националне безбедности Републике Србије и Стратегије одбране Републике Србије, и створити предуслове за доктринарну разраду информационих операција. Садржаје информационих операција у доктрини операција прилагодити садржајима дефинисаним у Концепту информационих операција који је усвојен у фебруару 2015. године.

Пресудан је значај информације за успешно управљање цивилним и војним процесима у савременом друштву, а посебно у фази припреме и фази извођења савремених војних операција. Све савремене војне теорије информацију препознају као пети фактор војних активности, који има одлучујући утицај на човека, технику, простор и време. Ефекти садржаја информационог ратовања имају константан утицај на процес доношења одлуке од фазе оријентације до фазе израде докумената, на свим нивоима одлучивања.

Предлози за стратегијско-доктринарно уређење и практичне изградње садржаја информационог ратовања, који су изложени у раду, претстављају минимум мера које је потребно хитно предузети ради заустављања губитка основних способности које систем одбране Републике Србије поседује за успешно извршавање задатака у оквиру информационих операција. Ови предлози су искључиво иницијални али и изузетно важни јер директо указују на потребу за оперативним и функционалним способностима без којих команде и јединице Војске Србије и организационе јединице министарства одбране немају оновне претпоставке за испуњење својих мисија.

Без информације систем не зна где је, ко је око њега, куда треба да се усмери, које поступке да планира и где би требало да стигне. Ако не знате одакле, када, зашто и куда сте кренули, где год да стигнете ви сте и на погрешном месту и у погрешном времену и са погрешним резултатима.

ЛИТЕРАТУРА

[1] Устав Републике Србије,
[2] Daniel G. Wolf, Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development, Nacional Security Agency US, Juli 22, 2003.,
[3] Ковач М., Стојковић Д., Стратегијско планирање одбране 2009.г.,

[196] Концепт информационих операција, фебруар 2015.г. стр. 28
[197] исто, стр. 29

[4] Нешковић С., Економске импликације информационог ратовања у савремених међународним односима, Економија теорија и пракса,
[5] Петровић С., Компјутерски криминал, МУП Републике Србије, Београд 2001.г.,
[6] Панарин И., Проблемы обеспечения информационной безопасностъ. Москва, 1998. г.,
[7] Тофлер А., Рат и анти рат, Паидена, Београд, 1998.г.,
[8] Стратегија националне безбедности Републике Србије, СВЛ 31/09,
[9] Стратегија одбране Републике Србије, СВЛ 31/09,
[10] Стратегија националне безбедности САД, (превод 2015.г.),
[11] Војна доктрина Руске Федерације (превод 2015.г.),
[12] Концепт информационих операција, фебруар 2015.г.,
[13] ФМ 3.0 Операције јун 2001.г. и јун 2005.г.,
[14] Правило електронских и противелектронских дејстава,
[15] Монографија 4.цПЕД, "Графопринт"-Ужице 2005. г.,
[16] Војно дело 3/2012,
[17] Војно дело 3/2015,
[18] Committee on National Security Systems, National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, USA, 26 April 2010. г.,
[19] Committee on National Security Systems, National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, USA, 26 April 2010. г.,
[20] Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, A/Res/53/70, January 12, 1999.
[21] http://daccess-dds-ny.un.org/doc/.pdf (приступљено 04.12.2015.г.),
[22] Захтев РФ за разматрањем *International Code of Conduct for Information Security;* http://www.un.org/ga/search/view_doc.asp (приступљено 04.12.2015.г.),
[23] Извештај са састанка одржаног 20.10.2011. године по питању Кодекса; http://www.un.org/News/Press/docs/2011/gadis3442.doc.htm (приступљено 04.12.2015.г.),
[24] Презентација "НИС а.д Нови Сад - организација, делатност, капацитети и технолошки процеси производње". Посета седишту компаније НИС, Нови Сад, 28.10.2015.г.,
[25] Презентација "Ризици и безбедоносни аспекти дистрибуције нафте и нафтних деривата". Посета седишту компаније НИС, Нови Сад, 28.10.2015.г.,
[26] International Federation for Information Processing - IFIP, http://www.ifip.org, (приступљено дана 10.11.2015.г.),
[27] Извештај са састанка одржаног 20.10.2011. године по питању Кодекса, http://www.un.org/News/Press/docs/2011/gadis3442.doc.htm (приступљено 20.11.2015.г.),
[28] http://www.support.google.com. (приступљено дана 30.11.2015.г.),
[29] Libicki, M., http://www.ndu.edu/inss/books/Books (приступљено дана 30.11.2015.г.).