ПРИМЕНА ПРИНЦИПА ПРАВА ОРУЖАНИХ СУКОБА НА САЈБЕР РАТОВАЊЕ

Мајор мр *Драган* Младеновић, дипл. инж.

Сајбер ратовање води се применом истих средстава, техника и метода као и у случају сајбер криминала, тероризма и обавештајних активности и има веома специфичну природу, која омогућава државама да прикривено покрећу нападе на противника. Полазна тачка при дефинисању доктрина, процедура и стандарда у области сајбер ратовања јесте утврђивање његове праве природе. У међународним оквирима не постоји консензус држава света око дефинисања и регулисања сајбер ратовања. Тај недостатак и брз развој природе сајбер ратовања могу изазвати несагледиве последице по светску безбедност. У овом раду дат је допринос настојању да се нова област сајбер ратовања сагледа у оквиру примене досадашње међународне праксе у области сајбер ратовања и примене принципа права оружаних сукоба.

*Аутор ради у Гарди

Интерес за сајбер ратовање као нетрадиционалног средства за остварење политичких, војних и економских циљева доживљава интензиван раст у целокупној светској заједници. Тај интерес првенствено се огледа у развоју националних капацитета за сајбер ратовање, који укључују средства, технике, методе, оспособљено људство, доктрине и стратегије, али и у све чешћој практичној примени овог облика вођења сукоба у ситуацијама које се разликују од класичног облика рата. Та примена среће се у различитом облику, од изазивања физичког уништења важних инфраструктурних система,

Снимио Ј. МАМУЛА

Снимио Д. БАНДА

преко праћења, онеспособљавања или измене жељеног деловања војних средстава које противник користи за вођење рата, за обавештајне активности, дејства на противнички систем командовања и руковођења, па чак и за информационо-пропагандна дејстава у сајбер простору на широке слојеве друштва којима се подстичу немири, побуне и револуције, чији је крајњи циљ дестабилизација и сламање противничког државног система власти. Сајбер ратовање може се применити на разне начине, од којих се многи не могу поистоветити са традиционалним значењем примене оружане силе. У зависности од властитих државних интереса, разне државе и државне групације у међународној заједници заузимају опречне ставове о могућој међународној правној регулацији сајбер ратовања. Ипак, поред свих потешкоћа у дефинисању и одређивању природе, техничких карактеристика и начина деловања сајбер ратовања, јасно је да његова дејства остварују последице, које су по својим ефектима сличне или идентичне последицама примене традиционалних облика кинетичке силе, које је својствено војном дејству које подлеже позитивним нормама међународног права оружаних сукоба. Ово право оружаних сукоба исказано је својим општим принципима који су универзално примењиви на све облике сукоба, укључујући и сајбер ратовање. Међутим, у случају сајбер ратовања јавља се проблем њихове практичне имплементације (слика 1).

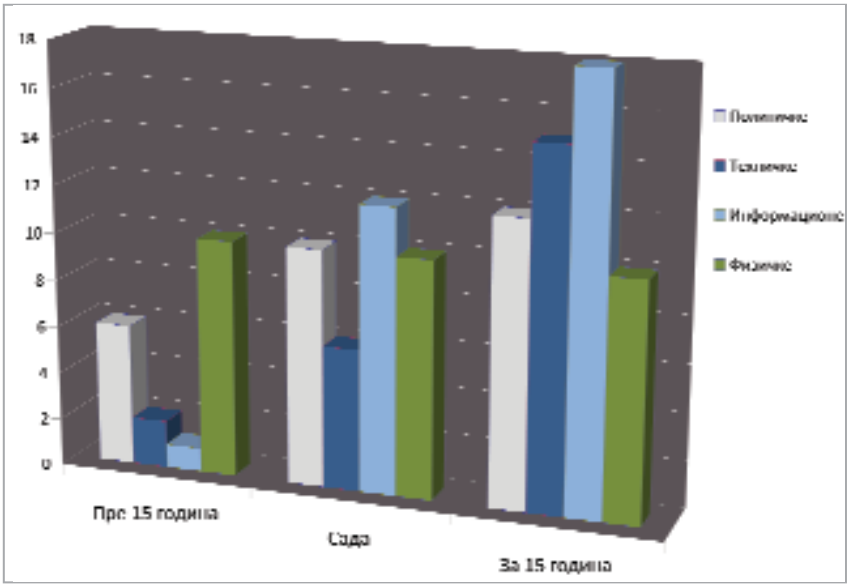
ШТА ЈЕ САЈБЕР РАТОВАЊЕ

Да би се могла извршити анализа примењивости принципа права оружаних сукоба на сајбер ратовање, потребно је претходно одредити његову природу, што укључује разумевање средстава, метода, сврхе и начина дејства, његове учеснике и последице. Као што је то случај са свим дисруптивним ратним технологијама које револуционарно мењају природу сукоба, по њиховом појављивању потребно је да протекне одређено време и да се створи међународно искуство да би светска заједница била у стању да формира јединствен став о њиховој природи, а затим и да усвоји општеприхватљиву регулацију, која ограничава деструктивно дејство тих технологија. Тај процес некада тече деценијама (на пример, у случају нуклеарног наоружања, тече од његовог настанка до данашњих дана), па је донекле разумљиво садашње одсуство заје-

ничког става међународне заједнице по питању регулисања сајбер ратовања.

Да би се одговорило на питање шта је сајбер ратовање, потребно је поћи од општеприхваћених премиса. Сајбер ратовање представља примену сајбер простора, утицај кроз њега и примену сајбер инфраструктуре у војне сврхе, која има природу ратовања. С обзиром на теоретску неодређеност сајбер ратовања, као и на динамичност и брзину мењања његове природе, сајбер инфраструктуру треба схватити у најширем могућем значењу. У том смислу сајбер инфраструктуру сачињава окружење (објекти, средства, физичка инфраструктура, простор на копну, мору, ваздуху и свемиру у коме се налазе та инфраструктура и средства), енергија која омогућава рад информационих система и постројења, хардвер (процесори, рачунари и њихови склопови, оптички и други проводници и слично), софтвер (машински, кориснички, слој везе, електронске базе података и слично), мреже (мрежни уређаји, комуникације, топологије и слично), садржај (информације и датотеке које се чувају и крећу у системима и мрежама, мрежни и статистички подаци који настају аутоматизовано у рачунарским системима и мрежама и слично), људи (програмери, администратори, оператери, особље за одржавање, корисници) и регулативе (прописи, споразуми, стандарди и друго)[1].

У односу на схватање сајбер простора, сајбер ратовање може имати уже или шире поимање. У односу на облик дејства, сајбер ратовање састоји се од дефанзивних, офанзивних и обавештајних операција.[2] Сједињене државе су глобални лидер у примени сајбер ратовања, па је корисно обратити пажњу на начин на који њихова војска дефинише ово подручје. У америчкој војној терминологији војна дејства која се воде применом рачунара дефинишу се као рачунарске мрежне операције (Computer Network Operations) и представљају војне операције предузете ради напада, одбране и обавештајног прикупљања. Усмерене су против непријатеља, његових информација, информационих система и мрежа, а служе и за одбрану властитих информација, система и мрежа.[3]



Слика 1. *Тенденција раста друштвених претњи по врстама (релативни степен друштвене опасности у односу на време и физичке претње)*[4]

Сајбер напади упућују се на циљ путањом која је делимично или у целини у сајбер простору. Та „оружја" представљају примењена софтверска решења или логичке технике. Она директно нападају информације и информационе сервисе и процесе, а дејство на људе и материјални свет остварују посредно преко тих система, процеса или информација. Основна примена средстава помоћу којих се покрећу

[1] Karl Rausher, Valery Yaschenko, Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations, стр. 21.

[2] У војној терминологији операција је такав облик дејства који могу да изводе снаге на било којем нивоу организовања који захвата и садржаје изван појмова рат и оружана борба.

[3] US DOD Dictionary of Military Terms, http://www.dtic.mil/doctrine/dod_dictionary, (01. 02. 2010).

[4] RAND Europe, Kevin A. O'Brien, „Cyber Intelligence: For Threat Profiling of Sub-State Actors in the Information Age", 2009, strana 11, www.randeurope.com, (14. 04. 2010).

Слика 2. *Могући случајеви сајбер ратовања у односу на врсту напада и природу циља*

сајбер напади врло често је мирнодопска. Лако су доступна свима и често су релативно јефтина. Важно је нагласити да се само сајбер напади на циљеве који директно или посредно зависе од сајбер простора могу сврстати у подручје сајбер ратовања. Напади конвенционалном силом на сајбер инфраструктуру јесу облик традиционалног ратовања које оставља последице на сајбер инфраструктуру и не представљају примену сајбер ратовања.

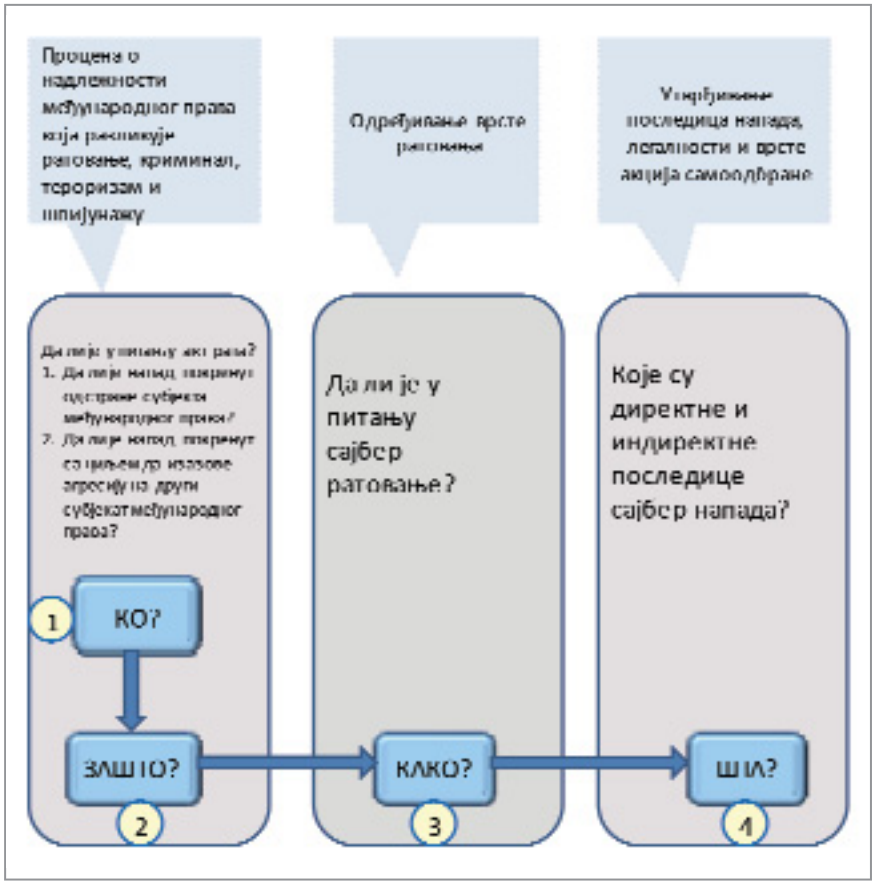
Без обзира на различита схватања, досадашњи случајеви примене сајбер дејстава у сукобима између држава показали су неке његове универзалне карактеристике и потенцијале. У стварности, упркос многобројним сумњама и медијским наводима, до сада не постоје докази ни за један озбиљан случај сајбер ратовања који је покренула једна држава према другој држави. Највећи број сајбер напада тако се односи на криминал (и његове специфичне облике – тероризам[5] и шпијунажу[6]), а у свим тим ситуацијама нападачи подлежу санкцијама националних и међународних кривичних прописа у складу са прихваћеним правилима јурисдикције правних система. При одређивању сајбер ратовања стога је, без обзира на врсту примењених средстава и техника, неопходно утврдити ко је стварни нападач, односно чињеницу да ли иза напада стоји државни ентитет који има међународни правни субјективитет или не. То је у садашњем тренутку развоја информационих технологија и мрежа често готово немогуће, посебно имајући у виду околност да се за сајбер ратовање и криминал користе иста средства, методе и технике и да сајбер напади у целини више зависе од недостатака у сајбер инфраструктури противника него од војних доктрина. Стога је за сајбер ратовање кључно утврдити нападача, његове циљеве и намере, али и саму мету, јер

[5] Појам сајбер тероризма и тероризма у општем случају није међународно дефинисан, али је, у начелу, сајбер тероризам специфичан случај сајбер криминала који представља употребу сајбер простора, информација, информационих система и мрежа ради остваривања терористичких циљева.

[6] Сајбер шпијунажа је у принципу легална у међународним оквирима и забрањена националним законодавствима уколико је покренута од стране противника, а дозвољена уколико служи сопственим интересима. Шпијунажа је дозвољена у међународним оквирима у складу са Конвенцијом о поштовању закона и обичаја рата на копну (IV Хашка конвенција) и њеним анексом ИВ: Уредба о законима и обичајима рата на копну, члан 24, 18. октобар 1907, (у наставку Хашка конвенција ИВ), који наводи следеће: „Ратна лукавства и примена мера које су неопходне ради прикупљања података о непријатељу и његовој држави, сматрају се дозвољеним",http://avalon.law.yale.edu/20th_century/hague04.asp, (17. 03. 2008).

Томас Вингфилд, научни истраживач вашингтонског Потомак института за политичке студије, сматра да право на примену шпијунаже представља неотуђиви део права на самоодбрану сваке државе и тврди: „Бечка конвенција о дипломатским односима из 1961. године препознаје право држава да се укључе у шпијунске активности у миру, а државна пракса учествовања у прикривеним обавештајним активностима представљају неотуђив део у међународним односима и политици". Thomas C. Wingfield, „The Law of Information Conflict: National Security Law in Cyberspace", Aegis Research Corporation, 2000. Међународно право оружаних сукоба предвиђа обавештајна дејства у току сукоба и регулише их. Зато се обавештајни рад може сматрати активношћу у надлежности кривичног права, али и права оружаних сукоба уколико је предузета као војна активност, посебно у време оружаног сукоба.

у многим ситуацијама ширења сајбер напада није јасно да ли је неки циљ директна мета противничког дејства или колатерална штета неког ширег дејства (као што је то било у случају ширења рачунарског црва Stuxnet у ширем региону Азије, а директне последице биле су значајно ометање рада иранских нуклеарних постројења Натанц и Бушер).



Слика 3. *Логички ток утврђивања природе сајбер ратовања*

Може се сматрати да је дејство неког сајбер напада облик ратовања (или, још уже, облик војне операције која представља агресију) само у случају уколико постоје докази да је напад предузео субјекат међународног права са намером да почини акт агресије над другим субјектом међународног права. Најважније чињенице при регулисању сајбер ратовања стога су подаци о починиоцу напада и његовој намери. У случају када се може доказати да је сајбер напад облик агресије једног међународног субјекта на други[7], оправдано је и право на самоодбрану, које укључује примену оружане силе ради спречавања агресије.


Снимила Д. СТЕФАНОВИЋ

Однос међународног ратног права према сајбер ратовању

Међународно право оружаних сукоба део је јавног права који представља систем правила који уређује односе између држава у ору-

[7] Оно регулише односе између свих субјеката међународног права (не само међу државама, како је то у прошлости била пракса). Иако не постоји јединствен став, у начелу су то државе и међународне организације. То значи да међународно право регулише односе између држава, између држава и међународних организација и између и унутар самих међународних организација. Одређени међународни правни субјективитет (углавном ужи од оног који имају државе и међународне организације) признаје се и разним квазидржавама, квазимеђународним организацијама, специфичним субјектима, друштвеним групама, човечанству као целини, па чак и појединцима.

жаном сукобу и поводом оружаног сукоба. Његов основни циљ је да ограничи последице оружаних сукоба и да патње и разарања сведе на неопходну (минималну) меру. Међународно право оружаних сукоба[8] често се поистовећује са међународним ратним и хуманитарним правом. У пракси оно представља скуп међународних споразума који су груписани у Женевском праву (које штити оне који не учествују или су престали да учествују у сукобима) и Хашком праву (које ограничава средства и методе ратовања), као и општеприхваћене норме обичајног права.

У оквиру међународног права оружаних сукоба истичу се две засебне скупине правних принципа, и то: ius ad bellum, који се баве легалношћу употребе силе, као што су право неке државе на самоодбрану и принудних мера Савета безбедности УН и ius in bello правила понашања у рату која се примењују када државе прибегну оружаном сукобу. Оно је примењиво само у случајевима оружаних сукоба и односи се на међународне сукобе, али и неке који немају међународни карактер. При процени могућег ограничења сајбер ратовања нарочито је битан део права оружаних сукоба који се односи на употребу средстава и метода ратовања. Његова основа је у Женевској конвенцији, њеним Допунским протоколима I и II из 1977. године[9] и обичајном међународном праву.[10] До ратног сукоба долази онда када су актери супротстављених оружаних снага намерно ангажовани у војним операцијама једних против других или при намерном нападу циљева на територији или у територијалним водама друге државе, са изузетком пограничних инцидената изазваних грешкама. То значи да оружани сукоб подразумева само случај када је војна акција ауторизована или прихваћена на нивоу влада држава које учествују у сукобу. Право оружаних сукоба примењује се само у

[8] По професору Стевану Ђорђевићу појам „ратно право" замењује се појмом „право оружаних сукоба", јер више одговара садашњем степену развоја општег међународног права. Стеван Ђорђевић, „Подела међународног права и разграничење од сродних научних дисциплина", Анали Правног факултета у Београду, година X, бр. 1–2. 2002. године страна 60.

[9] Additional Protocols I and II to the Geneva Conventions, 1977. године.

[10] Knut Dormann, „Computer network attack and international humanitarian law", The Cambridge Review of International Affairs Internet and State Security Forum, Trinity College, Cambridge, 2001.

ратним сукобима и не прави разлику између нападача и браниоца, већ подједнако обавезује све учеснике у оружаном сукобу. Оно представља компромис између војне потребе и захтева хуманости, јер његова примена не спречава војничку победу, нити се бави питањем законитости ратовања, већ само ограничава непотребне патње и разарања. Питање законитости или незаконитости рата уређено је Повељом Уједињених нација. Модерни међународни сукоби су све инвазивнији и суптилнији. То не значи да су државе одустале од употребе оружане силе са кинетичким дејством, јер се она користи у све софистицираније и ефикаснијем облику, већ значи да се све више сукоба води и у време мира, ван објављеног ратног стања, разним методама сукоба ниског интензитета, које су задржале моћ да истовремено и повремено буду и смртоносне и разарајуће. У ту групу свакако спада и сајбер ратовање. Да би право оружаних сукоба могло ефикасно да ограничи модерне облике сукоба, укључујући и сајбер ратовање, његова правила о употреби оружане (смртоносне) силе морала би бити способна да ефикасно регулишу природу и интензитет савремених техника, метода и облика примене силе која се користи у тим модерним сукобима. Иако овај захтев није нов, јер су и у ранијим историјским периодима постојале, за њихово време, нове технике и средства за вођење рата, проблеми сајбер ратовања су по много чему специфични. У складу са њима, посебну пажњу треба посветити следећим захтевима[11]:

– дефинисању околности под којима сајбер напад представља акт рата,

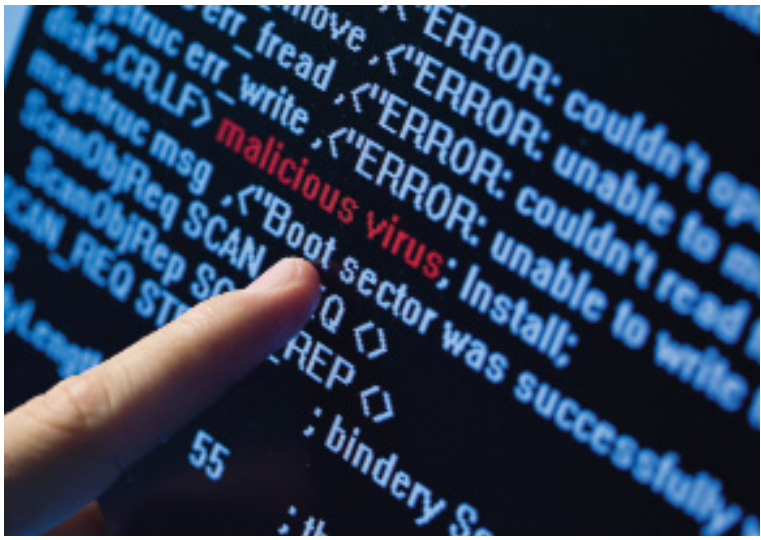
– јасном разликовању бораца и цивила у току сајбер сукоба,

– разликовању војних и цивилних циљева (инфраструктуре) и

– забрани непропорционалних напада.

КАДА САЈБЕР НАПАД ПРЕДСТАВЉА АКТ РАТА

Централно питање односа сајбер ратовања и права јесте да ли сајбер напад, под којим околностима и у ком облику, има карактер оружаног напада? Тек након одређења



природе сукоба, а у случају да се процени да је сајбер ратовање облик рата, могу се применити норме и прописи права оружаних сукоба и одредити остали изведени принципи, попут начина утврђивања права на примену силе и природе те силе у сајбер ратовању. Ово питање је компликовано, јер ни у случају традиционалног ратовања није увек јасно шта чини оружани напад. У међународној заједници чести су неслагања по овом питању. У општем случају, постојеће дефиниције оружаног напада се односе на облик, подручје, трајање и интензитет примене силе у датом контексту. Овакве недоумице постају још веће у сајбер ратовању. У стручној јавности постоје три различите групе гледишта у погледу тога, да ли и када се неки сајбер напад може сматрати еквивалентним са оружаним нападом.[12]

Једно гледиште осврће се на поређење могућих последица са кинетичким ратовањем. По њему сајбер напад има карактер оружаног напада уколико изазове последице које се могу остварити искључиво дејством кинетичког оружја. Проблем примене оваквог гледишта је питање да ли се као основ за аналогију требају узети искључиво директне последице напада

[11] Scott Shackelford, „From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", Berkley Journal of International Law, Vol. 25, No.3, 2009, стр. 240.

[12] National Security Threats in Cyberspace, A Wokrshop, American Bar Association Standing Comittee on Law and National Security And National Strategy Forum, McCormick Foundation Conference Series, September 2009, стр. 14. www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf, (16. 05. 2010).

кинетичком силом или и посредне последице? Одређење ове недоумице је кључно, с обзиром на то да су основна дејства на физички свет и људе у сајбер ратовању првенствено посредне последице које настају након дејства сајбер напада на информације и информационе системе. Друга група гледишта односи се на процену апсолутног обима и интензитета ефеката изазваних сајбер нападом на циљ и не врши њихово поређење у било ком погледу са кинетичким нападима. На пример, блокирањем рада финансијских институција се без физичког уништења могу остварити последице које посредно и дугорочно могу изазвати нечију смрт, повређивање или уништење добара, па је такав напад еквивалентан оружаном нападу.

Трећа група гледишта заступа правило стриктне одговорности – било какав напад на државне капацитете, чак и неуспешан, треба да се сматра оружаним нападом сам по себи.

Иако у међународној заједници не постоји консензус око одређења карактера сајбер напада, од сва три наведена приступа најзаступљенији је онај који посматра природу сајбер напада и њихову квалификацију оружјем на основу последица које ти напади остварују.[13]

Само је екстремне случајеве сајбер напада релативно лако одредити по питању квалификације карактера напада. Неовлашћено преузимање туђих података или привремено блокирање или измена изгледа интернет странице без изазивања битне штете сигурно се не може окарактерисати као примена оружане силе. Насупрот томе, сајбер напад који директно изазове смрт и повређивање људи или физичко разарање је у истој равни са оружаном применом силе. Проблем дефинисања природе сајбер напада лежи у огромној сивој зони између наведених крајности. Те околности могу имати скоро неограничене комбинације ситуација које треба да регулише међународно право, а које се односе на природу и врсту последица напада, начин њиховог предузимања, време предузимања напада и манифестовања њихових последица, статус и намере нападача, одговорност државе за нападе и многе друге.

ПРИМЕНА ОСНОВНИХ ПРИНЦИПА ПРАВА ОРУЖАНИХ СУКОБА НА САЈБЕР НАПАДЕ

Основна правила права оружаних сукоба могу се груписати у неколико главних принципа: војна неопходност (потреба), разликовање циљева, пропорционалност, избегавање непотребне патње, забрана ратне подмуклости и неутралност. Ови принципи представљају основу ратног права и зато се морају у изворном облику применити на сукоб у сајбер простору.

Принцип војне неопходности подразумева да је у ратном сукобу допуштена примена само неопходне силе за остварење војничке победе и то изричито у складу са правилима рата. Забрањено је користити оружје или методе ратовања који могу проузроковати непотребне губитке или прекомерну патњу. То оправдава примену војних средстава и мера у току сукоба која нису забрањена међународним правом, под условом да су неопходна за победу над 4непријатељем у што краћем року.[14] Допунски протокол I Женевских конвенција наводи да је војни напад законит једино против „оних циљева који по својој природи, положају, сврси или употреби дају битан допринос војној акцији и чијим се потпуним или делимичним уништењем, заузимањем или неутрализацијом у датим околностима обезбеђује јасна војна предност".[15]

Принцип разликовања одређује да стране у оружаном сукобу у сваком тренутку морају да праве разлику између цивилног становништва и бораца, између цивилних и војних циљева, као и да војне операције могу бити усмерене само против војног противника. Члан 48. Допунског протокола I, наводи основно правило: „Да би обезбедиле поштовање и заштиту цивилног становништва и цивилних објеката, стране у сукобу треба у свако доба да праве разлику између цивилног становништва и бораца и између цивилних објеката и војних ци-

[13] „National Security Threats in Cyberspace - Workshop Report", 2009. године, стр. 14.

[14] Хашка конвенција IV, члан 23 (г).

[15] Допунски протокол Женевској конвенцији од 12. августа 1949. који се односи на заштиту жртви у међународним оружаним конфликтима (Допунски протокол I), члан 52 (2), 8. јун 1977.

Ф-18 за електронска дејства

лъева и да, сходно томе, усмере своје војне операције само против војних циљева"[16]. Овај принцип универзално важи за све сукобе[17] и из њега проистиче забрана сајбер напада који не праве разлику између војних и цивилних циљева, као и обавезе да се директни сајбер напади могу предузимати искључиво против војних циљева, да нападачи морају минимизирати колатералну штету над цивилима и уздржати се од напада ако је штета од напада непропорционална са значајем војног циља, као и обавеза да се у сваком моменту предузимају мере опреза да се претходни захтеви поштују.

Забрана напада који не праве разлику између војних и цивилних циљева има највећи значај за примену у сајбер ратовању. У складу са чланом 51 Допунског протокола[18], напад који не прави разлику између војних и цивилних циљева дефинисан је као напад који није пажљиво усмерен на конкретан војни циљ (било због одлуке нападача, било због природе оружја) или код којег ефекте напада на војни циљ није могуће контролисати или предвидети. Очигледно је да сви сајбер напади, употребом злонамерних рачунарских програма који имају за циљ инфраструктурне системе које користи широка популација, по Женевском праву нису дозвољени. Овај проблем додатно добија на значају са повећањем степена интеграције и повезаности цивилних и војних рачунарских мрежа. Као карактеристичан пример за овакве нападе може се узети напад рачунарским црвима Stuxnet и Duqu који су направљени да онеспособе системе аутоматске контроле у нуклеарним и високотехнолошким индустријским постројењима. Stuxnet је био програмиран да трага за специфичним софтверским подешавањима у индустријским програмима контролних система компаније Siemens у употреби у нуклеарним постројењима у Ирану, што му је служило да открива програмабилне логичке контролере наведених система и напада их. Крајњи циљ на-

[16] Допунски протокол I, члан 48.

[17] Допунски протокол II Женевској конвенцији од 12. августа 1949, а који се односи на заштиту жртви у немеђународним оружаним сукобима (Протокол II), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8. june 1977, члан 13.

[18] Допунски протокол I, члан 51.

Слика 4. *Дијаграм расподеле ширења вируса Stuxnet у свету*[19]

пада био је изазивање самоуништења индустријског система који је руководио радом пумпи нуклеарних центрифуга у постројењима. Проблем је што је овај вирус, поред нуклеарних постројења Натанц и Бушер у Ирану, напао све контролере индустријских система до којих је дошао, углавном у државама региона у Ирану, Индонезији, Индији, Азербејџану, Пакистану, али и САД и другим државама, иако је у њиховом случају имао сасвим споредне последице. У конкретном случају, злонамерни програм није био селективан по обиму ширења, али по врсти дејства јесте, јер није остављао исте последице по све нападнуте системе, јер је деловао само у случају да препозна специфичну структуру наведених нуклеарних постројења.

Право оружаних сукоба прави разлику између војног и цивилног особља, објеката и постројења и ограничава нападе на војне циљеве.[20] Допунски протокол I одређује: „...војни циљеви су ограничени на оне објекте који по својој природи, локацији, сврси или намени чине јасан допринос војној акцији и чије би делимично или потпуно уништење, заузимање или неутрализација у датим околностима представљало недвосмислену војну предност".[21] Другим речима, није дозвољено војно нападати инфраструктуру која не пружа директан допринос ратним циљевима противника. Овакав принцип међународног права врши уравнотеживање војне предности, са једне стране, и заштите цивила, са друге стране. На пример, у масовном DDoS нападу на естонску информациону инфраструктуру 2007. године није прављена разлика између војних и цивилних циљева и када би било могуће доказати да је за његово покретање одговорна нека држава, он не би био у складу са правилима права оружаних сукоба.

У погледу наведених основних норми права оружаног сукоба, закључак је да је оно примењиво и на сајбер ратовање. Сваки сајбер напад мора бити ограничен, усмерен и пропорционалан војном циљу. Основу за то пружа постојеће међународно хуманитарно право. Америчко министарство одбране у својој Процени међународно-правних питања информационих операција наводи: „Ратно право је вероватно једино подручје међународног права у коме се постојећи законски прописи са највећом поузданошћу могу применити на информационо ратовање".[22]

Избегавање колатералне штете представља захтев да се избегне или минимизира случајна штета над цивилима или цивилним објектима. Непропорционалан је онај напад: „...за који се може очекивати да ће произвести успутан губитак цивилних живота, повреде цивила, оштећење цивилних објеката или ком-

[19] Izvor: http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-071400-3123-99

[20] Допунски протокол I, члан 48.

[21] Допунски протокол I, члан 52.

[22] An Assessment of International Legal Issues in Information operations, Department of Defense, 1999. године, стр. 11, http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf, (23.05.2010)

бинацију ових дејстава, која би била несразмерна у односу на очекивану конкретну и непосредну војну предност која се предвиђа".[23] Напад на војни циљ са дозвољеним средствима или методама ратовања, који изазове колатералну штету није законит уколико прекрши принцип пропорционалности. Ова процена у сајбер ратовању је тешка, пошто се упоређују две различите ствари – непосредна војна предност и колатерална цивилна штета. Да би се испоштовао овај принцип, пре напада је неопходно предузети мере опреза које подразумевају проверу циља пре напада, предузимање свих могућих мера предострожности при избору средстава и методе напада, уздржавања од напада за који се може очекивати да проузрокује цивилне жртве и оштећење објеката и извршити претходна упозорења о нападу.[24]

Сајбер напади користе постојеће грешке у софтверу, оперативним системима, апликацијама и мрежним протоколима. Стандардизација и аутоматизација програмирања софтвера значи да војне организације често користе исти софтвер, хардвер и комуникационе технологије као и цивилне структуре.[25] Већина тог софтвера, хардвера и технологија стога има исте слабе тачке, као и у цивилним системима, а оне су релативно доступне за испитивање нападачима. Стога је реална могућност да сајбер напад који је намењен за онеспособљавање војне мреже оствари деструктивно дејство и на цивилне системе. Без обзира на раст тенденције да се војни рачунарски системи ради заштите података потпуно изолују од интернета, то није могуће остварити у потпуности, јер употреба јавних мрежа битно умањује трошкове војне комуникације. Штавише, проток информација од цивилних ка војним системима ограничен је у мањој мери него проток у супротном правцу, што може охрабрити нападача да прво нападне цивилну инфраструктуру. Сајбер нападачима је примамљиво да нападну цивилне циљеве из стратешких разлога. Обарање рада битних рачунарских система у електроенергетској мрежи, контроли лета, индустрији, систему електро-

[23] Допунски протокол I, члан 51 (5b).

[24] Допунски протокол I, члан 57 (2).

[25] Око 70% порука са војне NIPRNET мреже америчке војске креће се кроз интернет мрежу, а скоро 90% укупног војног саобраћаја у сајбер простору се у неком делу среће или креће делом инфраструктуре цивилне мреже.

нских комуникација или банкарском систему једне земље може више утицати на њен капацитет да води рат него уништавање неколико војних јединица.

Технологија сајбер напада често захтева дејство на велики број транзитних рачунара на путу између нападача и жртве, најчешће због прикривања трага напада. Овакве злоупотребе туђих рачунара и мрежа не могу имати особину етички прихватљивих дејстава. У случају када су рачунари нападача заштићени air gap системима или физички искључени са спољних мрежа, откривање трага до извора напада је немогуће. Колатерална штета у случају сајбер напада је веома вероватна. Ипак, вероватноћа за њен настанак може се битно умањити повећањем прецизности напада и успостављањем механизама заштите нападнутог система који му омогућавају брз опоравак након напада. Сајбер напади могу бити пројектовани тако да буду селективни у погледу система које нападају и предмета напада у тим системима. Напад се може ограничити само на одређена дејства или сервисе. Такође, напади могу имати временско ограничење дејства или могу бити прецизно временски подешени да онеспособе нападнути систем у најповољнијем тренутку у којем би уништење ресурса или чак људске жртве били минимални. Досадашње искуство ратовања је показало да примена нових, непроверених метода ратовања у великом броју случајева може имати за последицу непрецизне или неочекиване ефекте. Политички притисак на војску да примени нова, експериментална средства ратовања на противнику у току сукоба био је релативно чест током историје. Сајбер напади могу изазивати разне карактеристичне проблеме који их чине различитим од традиционалних напада физичком силом. Примењена техника сајбер напада може бити ефикасна само док постоје недостаци у противничком систему који је предмет напада. Начелно, њихова ефикасност је максимална само првог пута, а затим нагло опада[26] и ограничена је на релативно кратак период. Овај ефекат се у жаргону назива напад нултог дана (zero day attack). Он представља

[26] Marcus Ranum, The myth of homeland security, Wiley, Indianapolis, 2004.

[27] Нестанак струје у Северној Америци који је осетило више од 50 милиона људи.

отежавајућу околност за нападаче, јер испитивање сигурносних пропуста на противничким системима није лак и јефтин процес. Нови, неиспробани напади су најефикаснији, али нове пропусте у противничким системима није лако утврдити. Та чињеница у великој мери повећава трошкове офанзивних дејстава сајбер ратовања. У таквим околностима војни системи ће вероватно мање пажње поклањати примени принципа етичности, а више на ефикасност напада.

У већини случајева изузетно је тешко одмах утврдити прави обим штете изазван сајбер нападом. Некада напади могу бити откривени дуго након примарног дејства. У неким случајевима та оштећења нападнутог система могу изазвати додатно дејство напада као последице кумулативног ефекта.[27] Дејство напада који није благовремено откривен додатно може продужити аутоматизовано стварање резервних копија стања система, које се редовно реализује на свим битним системима управљања. Уколико те резервне копије стања садрже претходно неоткривене инфекције система нападачким малициозним програмима, може се десити одложено дејство напада. У случају примене полиморфних вируса, који сами мењају свој програмски код, откривање је знатно отежано, па им дејство може бити продужено годинама. За отказ рада информационих система могу постојати разни узроци, па нападнута страна не мора уопште бити свесна да је отказ настао као последица напада са стране. Тада је то случај прикривеног дејства. За разлику од конвенционалног оружја, тешко је одредити на колико места је настало оштећење као последица сајбер напада. Недовољна поузданост напада изискује од нападача да примене обимније нападе како би постигли што виши степен њихове ефикасности.

Мере опреза у току напада предузимају се ради процене легитимности циља, избегавања прекомерног напада и колатералне штете. На пример, пре започињања сајбер напада потребно је предузети претходне радње попут обавештајних активности, како би се прикупиле потребне информације о противнику, циљу и осталим елементима напада. Међутим, услов је да су такве информације похрањене у доступним рачунарским системима и да нису подметнуте дезинформације. Зато се војска не може ослањати једино на шпијунирање противничких рачунарских мрежа при припреми ратне операције, већ је потребна комбинација сајбер активности са другим облицима обавештајног рада, нарочито оперативним прикупљањем података на лицу места. Овај захтев даје кључно оправдање свакој држави да активно развија капацитете и предузима активности за офанзивне обавештајне активности у сајбер простору. С друге стране, уколико су ове активности неуспешне, лако могу довести до ескалације сукоба.

Принцип пропорционалности забрањује сваку врсту или интензитет примене силе који прекорачује нужну неопходност за постизање војног циља,[28] што значи да штета изазвана ратним дејствима мора бити сразмерна војној користи. Око схватања овог принципа постоје различити погледи. Војни савез НАТО-а има став да колатерална штета[29] приликом напада на војне циљеве не представља нужно повреду међународног права, уколико је пропорционална оствареној војној предности. Право оружаних сукоба захтева од сваког нападача да процени могућу колатералну штету у односу на конкретну војну предност која се постиже тим нападом. Оправдање за допуштење евентуалне колатералне штете налази се у Допунском протоколу I Женевских конвенција, који се односи на заштиту жртава међународних оружаних сукоба. Он наводи да се, поред осталих, као неселективан напад сматра „напад од којег се може очекивати да ће изазвати успутне губитке цивилних живота, повреде цивила, штете на цивилним објектима или комбинацију ових дејстава, која би била несразмерно велика у односу на конкретну и непосредну војну предност која се предвиђа."[30]

---

[28] Rod Powers, "Law of Armed Conflict", about.com, http://usmilitary.about.com/cs/wars/a/loac.htm, (16.05.2010).

[29] Овај термин потиче из терминологије војске САД и почео је посебно да се помиње током ратова у Ираку и бомбардовања Србије. По дефиницији Министарства одбране САД (Joint Doctrine 3-60) колатерална штета представља „Ненамерну или случајну повреду лица или штету објекта који не представљају легитимне војне циљеве у датим околностима. Оваква штета није незаконита све док није прекомерна у односу на укупну војну предност остварену нападом".

[30] Допунски протокол I, члан 51 (5б).


Снимио Д. БАНДА

Да би се одредио степен пропорционалности одговора на такав сајбер напад потребно је извршити анализу многих питања: да ли је употреба силе у виду одговора на нападе у складу са принципом војне неопходности, односно да ли тај инцидент може бити решен на други начин осим војног? Да ли је планирани одговор пропорционалан нападу по својој природи? Ако јесте, да ли је ниво силе која се користи претеран у односу на важност војних резултата који се желе постићи? Да ли планирана употреба силе адекватно разликује војне циљеве и цивилно становништво и добра? Сва постављена питања проистичу из основних принципа права о оружаном сукобу. Међутим, иако су прилично неодређена уколико се посматрају са аспеката супротстављених страна, њихова природа постаје додатно нејасна у сајбер окружењу. Готово је немогуће недвосмислено одредити какав некинетички одговор на претходни сајбер напад може бити оправдан. Очигледно је да не постоји консензус око могуће примене постојећег права оружаних сукоба у међународној заједници, а веома је дискутабилно да ли и на који начин стварање нових прописа о сајбер ратовању може помоћи све док се не дефинишу основни појмови у вези с којима постоји много субјективних ставова заснованих на нејасним чињеницама.

Овакво тумачење не бави се питањем да ли је колатерална штета дозвољена, већ да ли је прекомерна у односу на остварени војни циљ. Члан 51 (4) наведеног протокола дефинише три типа неселективних напада:

(1) нападе који нису усмерени на специфичне војне циљеве,

(2) нападе који користе методе или средства борбе чији ефекти су такви да не могу бити усмерени на специфичне војне циљеве и

(3) нападе који примењују методе или средства ратовања чији ефекти не могу бити ограничени на начин како то захтева Протокол.

Забрана непотребне патње прописана је чланом 22 IV Хашке конвенције који дефинише да „права зарађених страна да изаберу средства за напад на противника нису неограничена”.[31] Члан 23 (е) ове конвенције изричито забрањује примену „оружја, пројектила или материјала срачунату да изазове непотребне па-

тње".[32] То значи да није дозвољена употреба оружја које је намењено изазивању непотребне патње, али ни употреба дозвољених врста оружја на начин који изазива непотребне патње. Подмукло или перфидно вођење рата уништава основу за обнављање мира између зараћених страна (осим у случају потпуног уништења једне од њих). Члан 23 (б) ИВ Хашке конвенције наводи да је „забрањено перфидно убијање или рањавање појединаца који припадају непријатељској нацији или армији".[33] Перфидност подразумева наношење штете непријатељу злоупотребом његове привржености ратном праву[34] и да су забрањени „поступци којима се улива поверење противнику наводећи га да верује да има право или да је обавезан да прихвати заштиту у складу са правилима међународног права која се примењују у оружаном сукобу, с намером да се изигра то поверење".[35] Ипак, постоји разлика између забрањених дела подмуклости и легитимног варања непријатеља применом ратног лукавства која не крше ни једно правило међународног права које се примењује у оружаном сукобу (попут камуфлаже, постављења мамаца, вођења лажних операција или подметања погрешних информација). Подметање намерних дезинформација о властитим војним плановима дозвољено је и, у начелу, не разликује се од било које дезинформације. Дозвољено је и применити домишљатост и позивати непријатеља на предају тврдећи да је окружен много већим снагама него што је то истина.[36] Међутим, стране у сукобу не смеју да прекораче ово дозвољено лукавство.

Пошто је сајбер шпијунажа врло раширена, може се очекивати да многе државе намерно протурају лажне податке на властите војне мреже са циљем да преваре противнике који их шпијунира.[37] Након откривања рачунарског црва Stuxnet, у светској јавности су се сукцесивно појавиле различите информације о начину његовог преношења и деловања. На пример, у америчкој јавности су крајем 2010. године наведене информације да је рачунарски црв подметнут у индустријске уређаје компаније Siemens током њиховог транспорта у луци Дубаи. У независним анализама више аналитичара током 2011. године предочена су њихова сазнања да се наведени софтвер преноси преко УСБ уређаја и да је вероватно убачен у систем нуклеарних постројења Натанц и Бушер преко припадника уговорне фирме из Русије са којом је иранска влада имала уговор о изградњи дела постројења. Крајем 2011. године други аналитичар за информатичку безбедност, бивши припадник америчког министарства одбране (који је претходно имао удела у откривању широке шпијунске мреже у сајбер простору), изјавио је да постоји веза између рачунарског црва Stuxnet и другог рачунарског црва Conficker који се ширио светом годину дана раније. Та веза се највероватније огледала у претходном омогућивању преузимање црва Stuxnet са интернета на заражени систем. Стручњаци са института за криптографију мађарског Универзитета техничких наука су 2011. године објавили информацију да постоји још један рачунарски црв, коме су дали име Duqu, који је по избору циља и начину деловања блиско повезан са рачунарским црвом Stuxnet. Све ове информације нису никада званично проверене и имале су моћ да доведу у заблуду иранску владу о начину инсталирања, функције и могућностима сајбер напада и да умање њено поверење у властите ресурсе, уговорне компаније из иностранства и безбед-

[31] Хашка конвенција IV, члан 22.

[32] Хашка конвенција IV, члан 23 (е).

[33] Хашка конвенција IV, члан 23 (б).

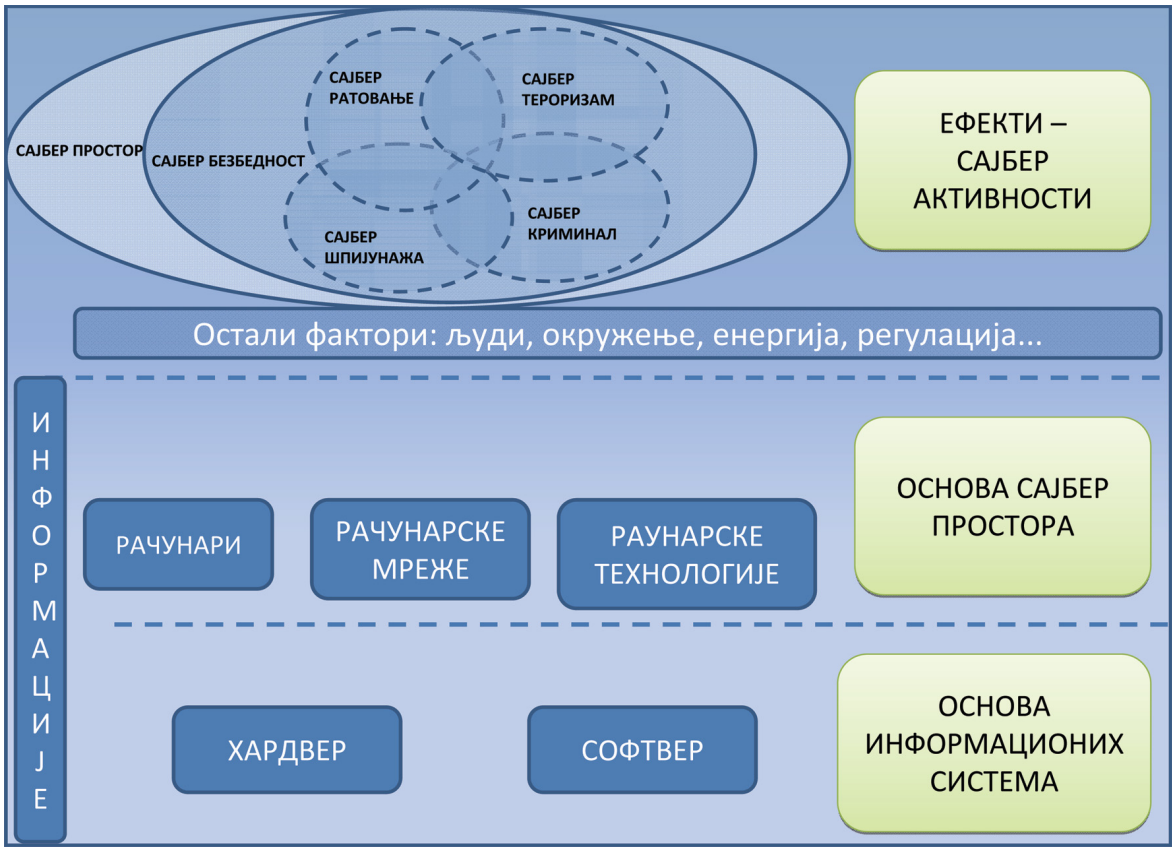
[34] Допунски протокол I, члан 37 (1).

[35] Допунски протокол I, члан 37. Дати су следећи примери: претварање да постоји намера да се преговара под заставом примирја или предаје; претварање да постоје озледе или болест, претварање да су особе у статусу цивила и претварање да имају заштићен статус употребом ознака, амблема или униформи Уједињених нација или државе која није учесник сукоба.

[36] FM 27-10, The Law of Land Warfare, Department of the Army Field Manual, US DoD, 15 July 1976. године, параграф 50, www.aschq.army.mil/supportingdocs/Fm27_10.pdf, (11.01.2010).

[37] Knut Dormann, „Computer network attack and international humanitarian law". Због овог проблема дошло је до разлаза између оснивача сајта Wikileaks, јер су постојала различита гледишта око потврде оригиналности достављених информација.

[38] Члан 1. Конвенције о поштовању права и дужности неутралних држава и особа у случају копненог ратовања (V Хашка конвенција), од 18. октобра 1907, каже да је „територија неутралних држава неповредива".



Слика 5. *Шематски приказ природе сајбер дејстава*

ност самог пројекта, па да изазову реакције које би имале самодеструктивно дејство на пројекат. Није познато да ли се нешто тако и остварило, али су у медијима објављене информације да је иранска влада током 2010. и 2011. године ухапсила известан број лица која су радила на развоју нуклеарног постројења. Индикативно је да су наведене информације биле опречне и да ниједна од њих није била благовремена, већ су се све појавиле у јавности након што је у потпуности остварено дејство сајбер напада.

Принцип неутралности омогућава државама које не учествују у сукобу да очувају своје мирнодопске односе са свим зараћеним странама у току сукоба. Држава која не учествује у непријатељствима, себе прогласи неутралном и понаша се у складу с тим, има потпуни имунитет од напада од стране свих зараћених страна. На основу овог принципа суверенитет неутралне државе је заштићен од напада или другог облика нарушавања.[38] Ипак, овај принцип није неограничен. Уколико неутрална страна из било ког разлога није у могућности да спречи повреду властите неутралности од стране војних снага неке од зараћених страна или спречи да јој оне повреде територију, друга зараћена страна има права да нападне те снаге на територији неутралне земље. То значи да је неутралност право, али и истовремена обавеза. По аналогији, уколико нека држава жели да задржи неутралан статус у сајбер сукобу, она не сме да покрене сајбер напад, а вероватно има и обавезу да онемогући такав напад употребом њених капацитета страни у сукобу.[39] Због недефинисане суверености држава у сајбер простору, примена овог принципа током сајбер ратовања је веома проблематична. На пример, путања сајбер напада у већини случајева не може бити предвиђена. Интернет је организован децентрализовано, па уколико неки сервер престане са радом, саоб-

[39] Jeffrey T.G. Kelsey, „Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", Michigan Law Review 1444, 2008. године.

рађај се аутоматски усмерава преко других рутера.[40] Напади могу путовати сајбер простором заједно са мирнодопским дигиталним садржајем. Већина држава света технолошки није у стању да спречи пролазак сајбер напада у домену властите јурисдикције без потпуног прекидања интернет саобраћаја. Примену система Einstein 3 за надзор интернет саобраћаја и препознавање и блокирање злонамерних програма у реалном времену тренутно развија само САД. Због тога буквална аналогија са правилима о неутралности у физичком свету није примењива на сајбер простор.

ОТЕЖАНА ИДЕНТИФИКАЦИЈА НАПАДАЧА

Право оружаних сукоба посебно је фокусирано на предузимање напада на лица – борце и неборце. Борци су сви припадници оружаних снага страна учесница у сукобу, осим медицинског и верског особља.[41] Они имају права да учествују у непријатељствима[42] и представљају „скуп организованих оружаних снага, група или јединица који се налазе под командном одговорношћу институција и лица дате државе која су одговорна за руковођење својим подређенима".[43] Борци имају обавезу да се „разликују од цивилне популације док су укључени у борбена дејства или се налазе у стању припрема за напад".[44] Право оружаних сукоба забрањује директан напад на неборце, а дозвољава нападе на борце уз поштовање принципа хуманитарног права. Са аспекта сајбер ратовања ово је кључно правило, с обзиром на то да су већину досадашњих случајева сајбер напада покренули цивили. Разликовање бораца и цивила у току сајбер сукоба је веома тешко, а у многим ситуацијама и немогуће у току сајбер ратовања. Ситуација се посебно компликује у случају високотехнолошких аутоматизованих борбених средстава и техника, код којих је ратно дејство у потпуности аутоматизовано.

На пример, нови модел беспилотне летелице Војске САД X-47B, произвођача Northrop Grumman, која је потпуно аутономна и нема пилота ни у летелици, ни за командама даљинског управљача, јер је опремљена аутоматизованим рачунарским системом и програмима који самостално обављају војну акцију.[46] У таквим случајевима примене роботизованих ратних средстава, али и већине софтверских програма способних да открију циљ, прате његов рад и преузму дејство у погодном тренутку (попут поменутог рачунарског црва Stuxnet), питање одговорности за предузети напад постаје веома сложено. Ко је одговоран за последице њиховог дејства? Командант јединице у чијем су саставу? Државни представник који је одобрио њихову употребу? Представник Војске који их је поручио? Произвођач или програмер? Без обзира на сложеност оваквих питања услед немогућности постојећег права оружаних сукоба да недвосмислено регулишу употребу будућих средстава за вођење рата, бу-

Слика 6. *Нови модел беспилотне летелице Војске САД X-47B произвођача Northrop Grumman, која је потпуно аутономна и нема пилота ни у летелици, ни за командама даљинског управљача*[45]

[40] Davis Brown, „A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict", Harvard International Law Journal 179, 2006.

[41] Допунски протокол I, члан 43 (2).

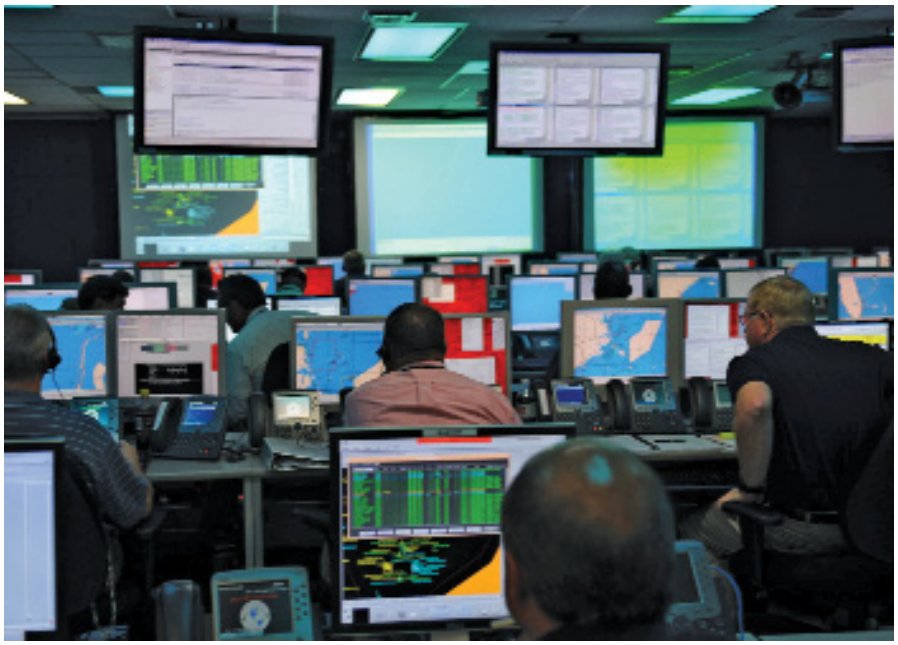
[42] Допунски протокол I, члан 43.

[43] Исто, члан 43 (1).

[44] Исто, члан 44 (3).

[45] http://www.thelivingmoon.com/45jack_files/03files/Black_Aircraft_Navy_Triangles.html (26. 12. 2012).

[46] W.J. Hennigan, „New drone has no pilot anywhere, so who's accountable?", Los Angeles Times, 26 January 2012, http://articles.latimes.com/2012/jan/26/business/la-fi-auto-drone-20120126, (26. 12. 2012).



дућност њихове употребе је недвосмислено очекивана.

Може се очекивати да ће будуће сајбер нападе предузимати цивилни стручњаци подједнако као и посебно обучени припадници војске. Они могу бити прикључени војним јединицама страна у сукобу, али то у пракси није неопходно. За сајбер нападе је небитно ко их покреће и да ли има униформу и ознаке војне јединице, иако то представља кршење правила ратовања.[47] Практичан проблем у ситуацијама сајбер ратовања представља и нејасноћа како би се, чак и да то жели, нападач могао идентификовати као легитиман борац. Стриктним поштовањем правила ратовања и обавезе самоидентификовања бораца у току сукоба дошло би се до закључка да је сајбер ратовање нелегално, јер током њега не постоји начин, нити смисао идентификације лица која припремају, покрећу и воде сајбер нападе.

У неким случајевима сајбер напада, идентификација није могућа због масовности нападача. За неке досадашње облике сајбер напада, попут DDoS[48] напада, била је карактеристична једна група самоорганизујућих грађана, такозвани levee en masse,[49] облик грађанске војске, добровољачких одреда, организованих покрета отпора и скоро било који други облик неконвенционалних бораца који се сами и неформално окупљају и организују. Шира група спонтано организованих руских цивила била је директно укључена у нападе на Естонију, Грузију и Киргистан током периода 2007–2009. године, али не као одговор на напад, већ у функцији претходне агресије на неку државу. Пример за овакво ангажовање цивила у сајбер сукобима могу бити сви случајеви у којима припадници једне нације предузимају дејства против непријатељске нације, попут акције српских и кинеских патриота против НАТО сервера током 1999. године, честа организована међусобна дејства хакера у српско-албанском, палестинско-израелском или индијско-пакистанском сукобу. Војно ангажовање цивила у сукобу није легално и представља кршење права оружаних сукоба, док би напад на њих у смислу одговора на њихово дејство био оправдан. Пошто цивилима међународно право не даје статус бораца, њихово учешће у борбама може бити и кривично дело.[50] Такво објашњење важи за свако учешће у борби, укључујући и сајбер ратовање. Ипак, чињеница је да је у сајбер ратовању често ангажовање цивила за припрему и вођење војних дејстава. Учешће цивила у борбама на некој од зараћених страна представља индивидуални ратни злочин по међународном праву, али и колективни, уколико те цивиле ангажује држава. Овај принцип је применила

[47] Commentary on the Additional Protocols of 8 June, 1977 to the Geneva Conventions of 12 August 1949, члан 44.8

[48] Distributed Denial of Service Attack је врста рачунарског напада којим се рачунарски и мрежни ресурси чине недоступним њиховим корисницима. Користе уобичајен поступак захтева за информацијама, али на неуобичајен и смишљен начин ради онемогућивања нападнутих система.

[49] Ова категорија била је директно укључена у сајбер нападе руске стране на Естонију, Грузију и Киргистан у периоду 2007–2009. године.

[50] Ово је чест случај у савременим ратним активностима САД у Ираку и Авганистану.

Влада САД када је по одредби Акта о војним судовима из 2006. године оптужила Канађанина ухваћеног у Авганистану који је учествовао у борбама на противзаконит начин[51]. Овај тренд ангажовања специфичних приватних армија за потребе војске у ратним жариштима је у изразитом порасту,[52] иако је Генерална скупштина Уједињених нација 1989. године на пленарном заседању усвојила резолуцију број 44/34, Међународну конвенцију против регрутовања, употребе, финансирања и обуке најамника. Члан 5 ове Резолуције наводи: „Државе учеснице неће регрутовати, користити, финансирати или обучавати најамнике и забраниће такве активности у складу са одредбама ове Конвенције"[53]. Регулисање статуса цивила пружа им заштиту у току ратних сукоба, али и ограничава активности држава које користе цивиле у току сукоба. Ово питање је значајно за сајбер ратовање, у којем је очекивано ангажовање цивила за војне активности вероватно највеће од свих облика ратовања. Много је лакше ангажовати цивилне програмере за креирање вируса, шпијунских програма или акције сајбер напада на противничке системе него обучавати постојећи војни персонал. О томе сведоче бојни позиви и пројекти америчког министарства одбране, научноистраживачке агенције DARPA[54] и обавештајне агенције NSA[55] упућени хакерима и студентима за узимање активног учешћа у развоју техника и средстава за сајбер ратовање.[56] Не постоје никаква техничка ограничења да се тако унајмљени цивили употребе за непосредно извршење борбених сајбер дејстава на противнике. Ношење униформе и војних ознака хиљадама километара далеко од бојног поља представља формализам и губи смисао, јер такво буквално поштовање правила ратовања нико не би могао да провери нити контролише. Ангажовање цивила на предузимању војних акција и наношењу људских жртава и материјалних разарања треба да представља кривично дело код свих облика ратовања, па и сајбер ратовања.

Закључак

Основни проблем у вези с међународним правним регулисањем сајбер ратовања огледа се у његовој специфичној природи, нејасној разлици између криминала, тероризма, обавештајних активности и ратовања и чињеници да оно често није селективно у односу на војне и цивилне циљеве, као и да се брише разлика између бораца и цивила који покрећу сајбер нападе. Недостатак специфичних прописа ратовања за ово подручје има за последицу да нема ни прекршилаца тих правила. Недостатак регулативе ратовања може изазвати несагледиве последице по светску безбедност и у супротности је са достигнутим стандардима међународне заједнице. Ипак, њено непостојање не значи да је дозвољена неограничена и неселективна примена сајбер ратовања. Све државе су обавезне да се понашају у складу са постојећим међународним правом приликом покретања сајбер напада. На оперативном и тактичком нивоу ти напади морају поштовати све принципе међународног права оружаних сукоба, који су општеприхваћени у међународној заједници у толикој мери да су постали део обичајног права. Стога ниједна национална стратегија и војна доктрина за област сајбер ратовања не сме бити у супротности са наведеним начелима. Међутим, њихова имплементација није лака и једноставна, посебно уколико се имају у виду многобројне специфичности сајбер ратовања. Поред тога, додатни изазов представља динамична брзина развоја сајбер ратовања. Државе морају остварити право на одбрану националне безбедности, али морају испунити и обавезе према међународној заједници. Нужан услов на међународном нивоу је дефинисање основних

[51] Видети: Сједињене Државе против Кадра (US v. Khadr). Омар Кадр је у Авганистану наводно ручном бомбом напао америчке снаге. Кадр није користио незаконито оружје, ограничио је ефекте свог напада на непријатељске снаге и није се представљао као заштићени цивил док се припремао за напад. Стога је једино дело за које је могао бити оптужен по ратном праву само учешће у борби.

[52] Borozo Daragahi, „In Iraq, private firms train Iraqi soldiers, provide security and much more" Post-gazete.com, 15. јун 2010. године, http://www.sandline.com/hotlinks/Post-Gaz_priv-contractors.html, (22. 02. 2010).

[53] United Nations, General Assembly, A/RES/44/34, International Convention against the Recruitment, Use, Financing and Training of Mercenaries, 4. децембра 1989. године, http://www.un.org/documents/ga/res/44/a44r034.htm, (22. 02. 2010).

[54] Defence Advanced Research Project Agency

[55] National Security Agency

[56] Kevin Fogarty, DARPA, NSA, DoD launch cyber security effort: Operation Schmooze Hackers", IT World, 08 November 2011, http://www.itworld.com/security/222273/darpa-nsa-dod-launch-new-cybersecurity-effort-operation-schmooze-hackers (15. 11. 2011).

категорија и појмова у наведеној области и усвајање заједничких циљева. Кључни проблем јесте утврђивање одговорности државе за предузети напад и околности под којима се сајбер напад може сматрати актом оружане агресије.

У одсуству техничких могућности идентификовања стварног нападача и доказивања одговорности државних органа за напад, неопходно је усвојити нове принципе одговорности држава за активности у сајбер простору, који ће посредно омогућити примену универзалних принципа права оружаних сукоба. Док се то не учини, а у складу са реалним интересима националне безбедности, неопходно је наставити са развојем националних капацитета за сајбер ратовање у Војсци, али и другим државним институцијама, пошто противнички сајбер напади нису ограничени само на војне системе.

По својој природи, сајбер ратовање је најближе обавештајним операцијама, које по међународном праву нису забрањене, а чак су и неопходне ради правилне припреме свих операција. Такав модел већ је усвојило више држава света које технолошки и организационо предњаче у области сајбер ратовања. Специфичне међународне околности у којима се налази Република Србија дају прилог ставу да за успешну одбрану властитих капацитета Србија мора војно развијати офанзивне капацитете у области сајбер ратовања и предузимати проактивну одбрану свих националних ресурса у сајбер простору. Једино ограничење за развој капацитета и доктрине сајбер безбедности представљају ефекти властитих сајбер дејстава и њихова усклађеност са принципима права оружаних сукоба

Литература

1. Rauscher, K., Protecting communications infrastructure, Issue 2, s.l. : Wiley InterScience, Summer 2004, Bell Labs Technical Journal –Special Issue: Homeland Security, T. Volume 9, стр. 1–4.

2. Rho, J., Blackbeards of the Twenty-first Century: Holding Cybercriminals Liable Under the Alien Tort Statue, Chicago, 2007, Chicago Journal of International Law, Vol. 7, Number 2, Winter 2007 (8 Chi J Intl L 695), стр. 695– 718.

3. International Strategy For Cyberspace, The White House,http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf, May 2011, [цитирано: 20. мај 2011].

4. Sommer, P., Brown, I., Recuding Systemic Cybersecurity Risk, OECD/IFP Project on „Fututre Global Shocks", 4 January 2011, http://www.oecd.org/dataoecd/57/44/46889922.pdf, [цитирано: 5. јануар 2011].

5. Rauscher, F., Korotkov, A., Working Towards Rules for Governing Cyber Conflict, Russia-U.S. Bilateral on Critical Infrastructure Protection, The EastWest Institute, January 2011, http://www.ewi.info/working-towards-rules-governing-cyber-conflict, [цитирано: 28. јануар 2011].

6. Rausher, F., Yaschenko, V., Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations, The EastWest Institute, 26 April 2011, http://www.ewi.info/russia-us-bilateral-cybersecurity-critical-terminology-foundations, [цитирано: 28. април 2011].

7. Streltsov, A., International information security: description and legal aspects, 2007, http://www.unidir.org/pdf/articles/pdf-art2642, [цитирано: 13. мај 2011].

8. Department of Defense, USA, The National Military Strategy For Cyberspace Operations (U). http://www.carlisle.army.mil/DIME/documents/National%20Military%20Strategy%20for%20Cyberspace%20Operations.pdf, 2006, [цитирано: 14. март 2010].

9. Schaap, A., Cyber warfare operations: Development and use under international Law, The Air Force Law Review, Cyberwar Edition, 2009, T. 64, Winter, 2009, стр. 121-174.

10. Clarke, R., Cyber War: The Next Threat to National Security and What to Do About It. New York : Ecco, Harper Collins, 2010, ISBN 0061962236.

11. Dictionary of Military and Associated Terms, US Department of Defense, www.dtic.mil, 8 November 2010, www.dtic.mil/doctrine/dod_dictionary/ [citirano: 15. maj 2011].

12. International Strategy For Cyberspace, The White House, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, [цитирано: 20. мај 2011].

13. Strategy for Operating in Cyberspace, US Department of Defense, July 2011, http://www.defense.gov/news/d20110714cyber.pdf, [цитирано: 14. јул 2011].

14. Военная доктрина Российской Федерации, Президент России, www.kremlin.ru, 5 февраля 2010, http://news.kremlin.ru/ref_notes/461, [цитирано: 4. март 2011].

15.Доктрина информационной безопасности Российской Федерации, № Pr-1895, Совет Безопасности Российской Федерации, www.scrf.gov.ru, 9 сентября 2000, http://www.scrf.gov.ru/documents/5.html, [цитирано: 1 јун 2011].

16. Faillere, N., O Murchy, L., Chien, E., W32. Stuxnet Dossier, symantec.com. february 2011.

17. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [цитирано: 28. март 2011].