УДК: 341.311 ; 343.533:004

МЕЂУНАРОДНО ПРАВО И САЈБЕР РАТОВАЊЕ

Драган Д. Младеновић[*]
Генералштаб Војске Србије, Гарда
Мирјана С. Дракулић
Универзитет у Београду, Факултет организационих наука
Данко М. Јовановић
Генералштаб Војске Србије, Управа за логистику (J-4)

Сајбер безбедност је нова и специфична област националне и међународне безбедности 21. века. Њен најважнији аспект је сајбер ратовање, под којим се подразумева употреба информација, информационих система, мрежа и сајбер простора за офанзивне и дефанзивне операције на међународном нивоу.

Широм света – на државном, међудржавном и глобалном нивоу – воде се бројне дебате чији је резултат усвајање националних стратегија, војних доктрина и капацитета за вођење сајбер ратовања. Иако су принципи права оружаних сукоба универзално примењиви на све врсте сукоба, за сајбер ратовање, због комплексности, неопходна су оригинална решења, која се правилним избором и аналогијом могу извести из досадашње праксе.

У Републици Србији до сада није вођена национална дебата о сајбер ратовању ради утврђивања његове природе, односа са међународним правом и одређивања националне стратегије. Сајбер ратовање омогућава државама мале и средње величине да остваре асиметричне предности у односу на конкуренте, па чак и када је реч о великим силама. Развој капацитета и доктрине за сајбер ратовање може бити средство избора које ће јој помоћи да оствари значајан технолошки скок (прескакање целе генерације). Основни услов за то нису велика материјална средства, већ знање, а полазни услов је усклађеност властитог наступа на светској арени са међународним правом.

Циљ овог рада је утврђивање природе сајбер ратовања из технолошко-политичко-правне перспективе. У раду су обрађене специфичности и особине сајбер ратовања, анализа ситуација у којима сајбер напад постаје акт оружане агресије и могућности утврђивања државне одговорности за његово покретање. Коначно, на основу претходне анализе дат је предлог за формулисање свеобухватних принципа за утврђивање стратегије с обзиром на националне интересе и међународно право.

Кључне речи: *сајбер ратовање, сајбер рат, сајбер напад, сајбер простор, кибернетичко ратовање, међународно право, право оружаних сукоба, хуманитарно право.*

[*] dragan.mladenovic@vs.rs

Увод

Сваки облик ратовања мора бити подложан достигнутим цивилизацијским нормама савременог људског друштва. Те норме су утврђене заједнички дефинисаним и прихваћеним међународним правним актима, попут Повеље УН и оних који сачињавају међународно право оружаних сукоба. У пракси то право чини скуп међународних споразума, груписаних у Женевским конвенцијама[1] (које у начелу штите особе који не учествују или су престале да учествују у сукобима), Хашким конвенцијама[2] (које ограничавају средства и методе ратовања) и општеприхваћеним нормама обичајног права.[3] Њихов заједнички циљ је смање вероватноће избијања сукоба, а уколико се они десе – ограничавање њихових последица и своћење патње људи и материјалних разарања на најмању меру. Будући да су те норме опште и да их је прихватила целокупна међународна заједница, универзално важе за све облике и околности ратовања, укључујући и нове облике сукоба за које још увек нису усаглашена специфична правила примене, као што је сајбер ратовање. Сви актери на међународној сцени се морају уздржавати од агресивних напада и примене силе у међународним односима, осим у оправданим случајевима, попут остваривања права на оправдану самоодбрану. Право оружаних сукоба није примењиво на све случајеве примене силе, већ искључиво на међународне сукобе, тј. на оружане сукобе између субјеката међународног права (у пракси: најмање две суверене државе),[4] и у неким случајевима на немеђународне сукобе (у току којих се на подручју једне државе води борба између редовних оружаних снага и посебних наоружаних група или борба између наоружаних група са одређеним нивоом легитимитета).[5] Услов за усвајање регулатива међународног права јесте пристанак државе да део властите надлежности повери наднационалном телу, што значи да је за његов настанак неопходно успостављање консензуса свих чинилаца међународне заједнице. То значајно отежава чињеница да међу чланицама међународне за-

[1] Скуп норми којима се штите они који не учествују у борбама. Њима се штите права појединаца и имовине у току оружаног сукоба.

[2] Скуп норми којима се дефинишу правила ратовања, тј. којима се ограничавају средства и методе ратовања.

[3] У оквиру међународног права оружаних сукоба истичу се две засебне скупине правних принципа: *ius ad bellum* – односе се на легалност 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.

[4] Међународни сукоби су они оружани сукоби који се воде између две или више држава, чак и када нема објаве рата, или када је цела територија државе или њен део под окупацијом, чак и ако нема оружаног отпора окупацији, као и ратови за национално ослобођење (против колонијалне доминације, стране окупације или расистичких режима), при чему се користи право на самоопредељење без обзира на то да ли су све стране међународно признате као суверене државе или нису.

[5] Немеђународни сукоби су они који се воде између регуларних оружаних снага и наоружаних група које могу да се идентификују као засебни ентитети или између наоружаних група које се боре међусобно. Да би сукоб добио тај статус, размере борби морају достићи одређени ниво и интензитет и морају трајати одређено време. Унутрашње насиље и затегнутост (побуне), изоловани и спорадични акти насиља и остали акти сличне природе јесу акти којима се нарушава унутрашњи поредак, али нема примене међународног хуманитарног права јер нема признатог оружаног сукоба.

једнице традиционално владају супротстављени интереси. Позитивна страна спорог развоја су обезбеђивање универзалности усвојених принципа и мала зависност од историјских околности. Ипак, током историје, са развојем технологије значајно се мењао начин ратовања: увођена су нова средства и методе за које дотадашње право није знало.[6] Иако је постојеће право у основи имало капацитет да регулише настале ратне ситуације у којима су примењивана нова средства и методе, постојао је и велики број спорних ситуација чије је постојање повремено онемогућавало обезбеђивање основних принципа хуманости. Да би могло да се носи са таквим ситуацијама, међународно право је стално мењано и дограђивано, а тај процес се често одвијао уз много проблема. На пример, одмах након прве употребе авиона у оружаном конфликту сачињен је Нацрт хашких правила о ваздушном ратовању који у почетку није поштовала ниједна страна.[7] Било је потребно педесет година да се формулише потпуна забрана биолошког оружја[8] и више од двадесет година да се доврши регулисање употребе хемијског оружја.[9] С друге стране, нека правила ратовања су претходила свом времену, попут Конвенције о забрани војне или било које непријатељске употребе метода модификације животне околине из 1976. године,[10] Протокола о забрани оружја чији се делови не могу открити рендгенским зрацима из 1980. године[11] или Протокола о употреби ласерског оружја из 1995. године.[12] Ипак, и поред бројних проблема, тим специфичним прописима ратовања који се односе на употребу нових врста оружја на крају је модификовано постојеће право оружаних сукоба.[13]

Предузимање ратовања у сајбер простору војним дејством на информације, информационе системе, процесе и системе којима они управљају потпуно је нов и, по многим карактеристикама, веома специфичан начин манифестовања војне силе. Физичка основа сајбер простора налази се у свим физичким подручјима у којима је специфичним правилима дефинисана употреба силе у сврху ратовања. С друге стране, без обзира на то што почива на физичкој основи, сајбер простор се тешко може просторно-физички одредити јер се, истовремено, налази свуда и нигде, па са аспекта права није практична његова регулација на просторном принципу. Међу-

[6] Карактеристични примери су употреба ратне авијације, хемијско-биолошко ратовање, ратовање у свемиру, употреба несмртоносних оружја и други.

[7] Draft Rules of Aerial Warfare, фебруар 1923. године, http://www.dannen.com/decision/int-law.html#C, (16. 07. 2009).

[8] *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction. Opened for Signature at London, Moscow and Washington.* 10. април 1972. године, http://www.icrc.org/ihl.nsf/FULL/450?OpenDocument, (16. 07. 2009).

[9] *Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction*, Париз, 13. јануар 1993, http://www.icrc.org/ihl.nsf/FULL/553?OpenDocument, (16. 7. 2009).

[10] *Convention on the prohibition of military or any hostile use of environmental modification techniques,*10. децембар 1976, http://www.icrc.org/ihl.nsf/FULL/460?OpenDocument, (16. 7. 2009).

[11] *Protocol on Non-Detectable Fragments (Protocol I)*, Женева, 10. октобар 1980, http://www.icrc.org/ihl.nsf/FULL/505?OpenDocument, (16. 07. 2009).

[12] *Protocol on Blinding Laser Weapons (Protocol IV to the 1980 Convention)*, 13. октобар 1995, http://www.icrc.org/ihl.nsf/FULL/570?OpenDocument, (16. 7. 2009).

[13] На пример, стране у сукобима су биле способне да релативно лако прилагоде постојећа правила о копненом ратовању за ваздушно ратовање Регулативом о поштовању права и обичаја рата на копну, 1907. године, Анекс IV Конвенције о поштовању права и обичаја рата на копну, 1907. године.

тим, технолошки напредак сајбер ратовања и опште природе ратовања[14] омогућили су да се остваре физички ефекти чак и применом сајбер ратовања, па су озбиљне последице и непостојање специфичне регулативе довољни разлози за усвајање међународних стандарда за његово регулисање.[15]

Иако не постоји међународно прихваћена дефиниција сајбер ратовања, под њим се, уопштено, подразумевају сајбер дејства која су планирали, организовали или покренули државни учесници против сајбер инфраструктуре противника.[16]

Специфичности сајбер ратовања

Међународноправно регулисање сајбер ратовања отежано је због многих проблема и околности који су везани за његову специфичну природу:

– Сајбер ратовање омогућавају капацитети и активност противника, а не само нападача. Сајбер напад, за разлику од конвенционалног, нуклеарног, хемијског или биолошког ратовања, може да се предузме против неке државе само уколико њени капацитети зависе од информационих система и ако у неком подручју нису заштићени.

– Сајбер ратовање се смишљено примењује у дужем временским интервалу а ефекат дејства може да буде одложен. На пример, постојање рачунарског црва *Stuxnet* у рачунарским системима иранских нуклеарних постројења Бушер и Натанц откривено је 2010. године, а претпоставља се да су системи инфицирани 2008. године [1].

– Сајбер напади се заснивају на недостацима сајбер инфраструктуре, због чега се тешко могу спречити.

– Сајбер ратовање је истовремено изузетно ефикасан облик асиметричних и мрежноцентричних дејстава.

– Изузетно је тешко, а често и немогуће, доказати умешаност државе у покретање сајбер напада.

– Нису усаглашени облик, обим и интензитет које сајбер напад мора достићи да би се сматрао актом агресије према постојећим међународним прописима.

– У међународној заједници нема слагања око питања да ли се информационо-медијско дејство на противника сматра сајбер агресијом.

---

[14] Jason Barkham, "Information Warfare and International Law on the Use of Force", *International Law and Politics Issue 34*, New York University School of Law, 2002.

[15] У последњих десет година објављен је већи број стручних предлога за регулисање сајбер ратовања: George K. Walker, *"Information Warfare and Neutrality",* Jason Barkham, "*Information Warfare and International Law on the USe of Force*"; Yoram Dinsein, "Computer Network Attacks and Self-Defense" у *Computer Network Attack and International Law* (Michael N. Schmitt & Brian T. O'Donnell eds), 2002.; Eric Talbot Jensen, *"Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*", 2002; Michael Schmitt, *"Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework*", 1999; major David DiCenso, IW Cyberlaw: *"The Legal Issues of Information Warfare"*, 2000. године, и други.

[16] У NATO Standardization Agency дефинисан је појам Computer Network Attack (CNA) као: „Поступак предузет у циљу прекида, одбијања, нарушавања или уништења информација похрањених у рачунарским системима и мрежама или самих рачунарских система или мрежа". Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, (As Amended Throug 15 May 2011), www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (19. 5. 2011).

– Сајбер напади се често не могу локализовати само на војне циљеве. Наиме, циљеви напада су информациони системи који често имају и цивилну и војну сврху, а канали и циљеви напада (инфраструктура сајбер простора и информациони системи) већином су у приватном власништву. Технологија и инфраструктура које су потребне за сајбер ратовање у највећем броју случајева имају и цивилну и војну примену, а сајбер нападачи не морају бити припадници војске.[17]

– Индиректне последице сајбер напада на зависне системе и људе обично су веће од директних последица на рачунарске системе и податке.[18] Могу се изазвати чак и физичко уништење и смрт људи, и потенцијално изазвати последице коришћења оружја за масовно уништење [2, стр. 3].

– Крајњи исход напада је често непредвидив због накнадних, каскадних и кумулативних ефеката, који могу да достигну чак и глобални ниво.

– Сајбер напади су сложени за планирање и припрему. Могу да трају од делића секунде до неколико година, а изазивају ефекте у распону од локалних, усмерених на један рачунар, до глобалних.

– У поређењу са традиционалним војним операцијама, сајбер напади су релативно јефтини и доступни.

– Сајбер ратовање више зависи од комерцијалних него од војних потреба јер је основа његове технологије сличнија природи и карактеристикама информационе технологије и електронских комуникација него војним принципима и техникама.

– На глобалном нивоу, велики део информационо-комуникационе инфраструктуре заједнички је за све државе.

– Сајбер напади се лако могу извести прикривено, па су честе ситуације у којима се сајбер ратовање преклапа са криминалом, тероризмом и шпијунажом.

– Сајбер напад може ескалирати у сукоб ширих размера, било да је покренут у облику информационе операције или има за циљ посредно физичко уништење и смрт или повређивање људи [3, стр. 14].

– Дистрибуирана природа сајбер ратовања омогућава истовремене нападе много нападача на један циљ или једног нападача на много различитих циљева.

Иако је потпуно ново по средствима и методама, сајбер ратовање има своје доктрине, циљеве, средства, технике и специјализоване борце и команде, па се може сматрати независним подручјем ратовања.[19] Ипак, с обзиром на специфичну природу, не очекује се избијање сукоба искључиво у форми сајбер рата, већ је вероватнија интегрисана примена сајбер ратовања са свим осталим видовима ратовања [4, стр. 6].

---

[17] У свом излагању за Центар за стратегијске и међународне студије САД, директор *NSA* (*National Security Agency*) и командант Здружене сајбер команде (*U.S. Cyber Command*) навео је: „Више од 90 процената енергије за потребе наше војске је створено и дистрибуирано од стране приватног сектора, а више од 80 процената материјала наше логистике транспортују приватне компаније“, Center for Strategic and International Studies (CSIS), U.S. Cybersecurity Policy and the Role of U.S. Cybercom, speaker: gen. Keith Alexander, 3. јун 2010. године,
http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf, (7. 6. 2010).

[18] Нестанак струје у Северној Америци који је осетило више од педесет милиона људи.

[19] The Department of National Defence and the Canadian Forces, *Nature of Future Environments: Cyberspace Environment Version 1.0*, Chief of Force Development, Director of Future Security Analysis, март 2009.

Потреба за обезбеђењем властите националне инфраструктуре у сајбер простору, широк спектар прикривених дејстава и друге предности чине сајбер ратовање подједнако привлачним и за моћне и за слабије међународне чиниоце. Пошто његова широка и неконтролисана примена може да изазове непредвидиве и далекосежне последице, неопходно је да се међународноправно регулише као и ратовање у другим подручјима. Без обзира на потенцијалне предности, регулисање сајбер ратовања би морало бити у интересу целокупне међународне заједнице ради заштите државних капацитета, избегавања нарушавања властитог националног угледа у међународној заједници и политичке штете у случају да се изврши ратни злочин.

Табела 1 – *Поређење кључних карактеристика сајбер и кинетичких напада*

КАРАКТЕРИСТИКА	**КИНЕТИЧКИ НАПАД**	**САЈБЕР НАПАД**
Значај ефеката дејства	Директне последице напада су значајније од индиректних.	Индиректне последице напада су обично значајније од директних последица.
Могућност обнављања функције циља након напада	Мала. Напори на поновној изградњи инфраструктуре могу бити веома дуготрајни.	Често се веома брзо може повратити функционисање нападнутог циља.
Трошкови изградње оружја	Велики при развоју и набавци.	Углавном мали. У неким случајевима могу бити релативно високи у области развоја и истраживања.
Технолошка доступност	Ограничена у многим случајевима и подручјима.	Широко доступна у већини случајева.
Обавештајни захтеви за успешну примену	Начелно, мањи него за сајбер напад.	Начелно, већи него у случају физичког напада.
Неизвесност планирања	Начелно, мања него за сајбер нападе.	Начелно, већа него за кинетичке нападе.

На регулисање сајбер ратовања утиче његова специфична природа, по којој се разликује од ратовања у физичком домену. У том погледу, могу се издвојити четири основне врсте ситуација у којима се примењује сајбер ратовање [5, стр. 15–20]:

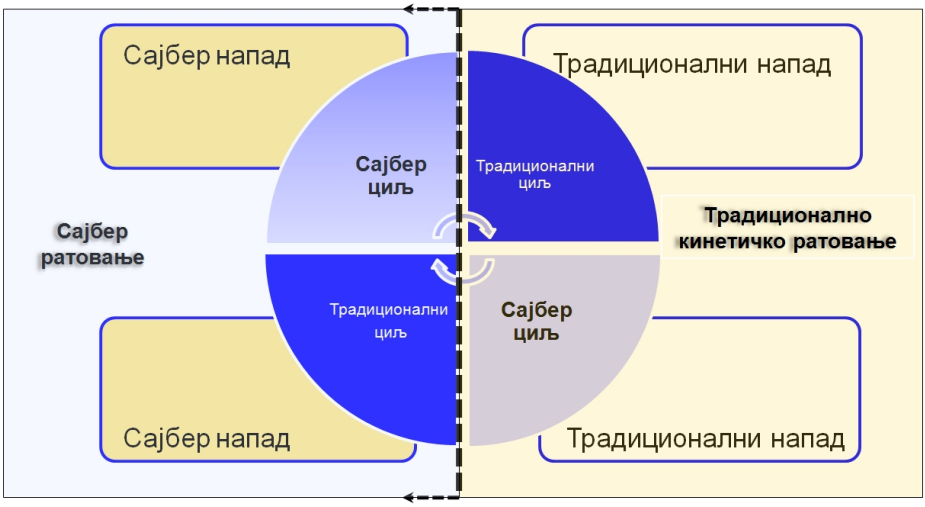
1. Примена традиционалних[20] оружја на традиционалне (не-сајбер) циљеве;[21]
2. Примена традиционалних оружја на циљеве у сајбер простору;[22]
3. Примена сајбер оружја на традиционалне циљеве;
4. Примена сајбер оружја на циљеве у сајбер простору.

[20] Кинетичког, нуклеарног, биолошког, нуклеарног, хемијског и другог „несајбер“ оружја.

[21] Они системи који су постојали пре појаве интернета и сајбер простора, односно за чије постојање више није неопходан сајбер простор. Карактерише их људски надзор и управљање и низак степен зависности од аутоматизације. Све их је мање у свету.

[22] Већина савремених циљева чије функционисање делом или у целини зависи од сајбер простора (интернета), који може на њих да оствари значајно повратно дејство. Карактерише их аутоматизовано управљање које зависи од софтвера, сензора и комуникација. Доминантна су и њихова заступљеност се повећава.

Традиционална оружја су она за која се користи сила (кинетичка, електромагнетно поље, нуклеарна енергија), средства за биолошку контаминацију или хемијски отрови за дејство на живи свет и физичко окружење. Остварују дејство одмах по упућивању на циљ, имају првенствено војну примену и нису доступна широкој популацији. Цена им варира од ниске до изузетно високе – за сложена техничка средства.



Слика 1 – *Могући случајеви сајбер ратовања зависно од врсте напада и природе циља*

Сајбер оружја, која чине примењена софтверска решења или логичке технике, упућују се на циљ путањом која је делимично или у целини у сајбер простору. 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 сајбер напади је веома често мирнодопска. Та средства су лако доступна свима и често су релативно јефтина.

Значајно је 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 облик су традиционалног ратовања које оставља последице на сајбер инфраструктуру и не сврставају се у сајбер ратовање.

Да би се у потпуности могла разматрати област сајбер ратовања, поред неопходног одређења природе самог акта напада неопходно је одговорити на два кључна питања:

1. Да ли је неки сајбер напад акт агресије у духу међународног права?
2. Да ли се може утврдити порекло сајбер напада и одговорност државе нападача?

Од одговора на та питања зависе могућност и начин примене међународног права на сајбер ратовање.

Сајбер напад као акт примене оружане силе и агресије

Без обзира на врсту и природу средстава сајбер напада, њихова заједничка карактеристика је да су усмерени на сајбер инфраструктуру противника и да су их планирали, организовали и покренули државни актери, што значи да за напад постоји **одговорност неке државе**. Треба имати на уму да се у савременом контексту веб-окружења, опште дигитализације садржаја, сервиса и просеца и развоја свеприсутног рачунарства сајбер инфраструктура мора посматрати у ширем друштвеном контексту. Њу не чине само рачунари и рачунарске мреже које граде сајбер простор, већ сви друштвени сегменти који утичу на њено постојање и дају јој значај у правном поретку.[23] Начелно, сајбер инфраструктуру чини скуп људи, процеса и система који сачињавају сајбер простор [6].

Основни међународни акти којима се регулише употреба силе, Повеља Уједињених нација и међународно право оружаних сукоба садрже принципе апсолутне забране државне употребе силе, осим у случају легитимних ситуација, попут самоодбране.[24] Ипак, то право се у пракси често слободно тумачи, па га често и војне силе злоупотребљавају као изговор у случају агресије ради остварења националних циљева. Већина у међународној заједници сматра да се превентивни напади не могу оправдати правом на самоодбрану, уз позивање на тзв. безбедносни принцип очувања суверенитета било које државе. Међутим, такве ситуације се могу очекивати нарочито у области војних дејстава у сајбер простору. Поред тога, због природе сајбер ратовања неопходна је, као приоритетна, примена војног одвраћања и превентивних акција, јер није могуће одбранити властите капацитете пасивном одбраном противника. Сајбер ратовање је могуће због многобројних недостатака и несавршености сајбер инфраструктуре, при чему страна која прва открије те недостатке остварује могућност првог напада на противника (*zero day attack*). Када се начини напада јавно објаве, велика је могућност да угрожена страна преузме мере да их онемогући у будућности. Суштина методе сајбер ратовања огледа се у сталном изналажењу нових могућности предузимања напада на противника који није против њих осигуран. Чак ни потпуна изолованост неког информационог система од глобалне мреже не омогућава сигурну заштиту, јер се недостаци који омогућавају сајбер ратовање не налазе искључиво у софтверу и хардверу, већ у свим елементима сајбер инфраструктуре (архитектура мреже, физичка основа сајбер простора, садржаји, правни система којим се регулишу активности и односи у сајбер простору, људи и дистрибуираној природи сајбер простора). Као пример за ту

[23] У ширем контексту, сајбер инфраструктура се састоји од следећих основних целина: *физичког окружења* (објекти, локалитети земаљских станица, свемирски простор у којем се крећу сателити, морско дно по којем се простиру подводни каблови и слично), *енергије* (извора-електричне, генератори, батерије и слично), *хардвера* (полупроводнички процесори, електронске картице, бакарни и оптички каблови и слично), *софтвера* (дигитални код, програми, базе података), *мрежа* (чворови, везе, топологије и слично), *садржаја* (информације, протоколи, прекиди или измене у току информација), *људи* (програмери, оператери, особље за одржавање и други) и **регулативе** (споразуми, стандарди итд.). Све већи обим светске инфраструктуре зависи од сајбер простора.Karl, F. Rauscher, „Protecting Communications Infrastructure“, Bell Labs Technical Journal, Special Issue: Homeland Security,Volume 9, Issue2, 2004.

[24] Повеља УН, члан 51. Поступак оправдане употребе силе подробније је дефинисан у члановима 37–51.

тврдњу могу послужити бројни познати случајеви, попут отуђења великог броја поверљивих Владиних докумената са војне *SIPRNET* мреже америчке војске (случај *Wikileaks*) или убацивање рачунарског црва *Stuxnet* у изоловани систем управљања иранских нуклеарних постројења Бушер и Натанц. У савременим националним стратегијама великих сила за војна дејства у сајбер простору узете су у обзир те околности, па је чест случај позивања на право на самоодбрану ради превентивне самоодбране и одвраћања противника, при чему се лако могу уочити двоструки стандарди за примену сајбер ратовања [7]. Такво тумачење права на самоодбрану не може се сматрати оправданим у контексту међународног права јер је нужан услов за остваривање права на самоодбрану постојање претходне агресије. Зато се поставља једно од основних питања у подручју сајбер ратовања: *да ли, и у којим случајевима, неки сајбер напад има карактер агресије?* У вези с одговором на то питање у свету постоје две различите групе мишљења.

Русија је предводник велике групе држава[25] које сматрају да је информационо ратовање у сајбер простору облик агресије на политички и друштвени систем нападнуте државе и да, као такво, подлеже међународној регулацији као и оружани сукоби. По том схватању, информациона безбедност се састоји од људског, друштвеног, духовног и техничког (сајбер) подручја,[26] па се у међудржавним односима, укључујући и сукобе, мора посматрати свеукупност информационог деловања, а не само технолошко-технички аспект сајбер ратовања. У сајбер простору се могу предузети технолошки сајбер напади, али се могу ширити и дезинформације и стварати лажна слика у медијима извртањем истине, дезоријентисањем, утицајем на вољу становништва и другим облицима манипулације ради подривања државног, економског и друштвеног система, са крајњим циљем дестабилизације друштва и власти [8, 9]. Такво објашњење је у сагласности са важећом теоријом „пет прстенова“, која је послужила као основа за савремени концепта мрежноцентричног ратовања који је заступљен у америчкој војној доктрини. Пошто се оружани напади на цивилну популацију и инфраструктуру тешко могу оправдати војном потребом и пропорционалношћу [10, 11], ти посредни и прикривени начини могу да буду веома ефикасни у међународним односима. Уколико су успешни, остварују исти резултат: изазивање отпора становништва према властитом руководству ради дестабилизације и свргавања власти противничке државе без борбе [12]. Та неоружана дејства на противника могу да се изводе на више равни (санкције, блокада комуникација, изоловање руководства и психолошка дејства на становништво), а захваљујући успешном ширењу интернета у свету и његовој природи све чешће се изводе употребом онлајн друштвених мрежа (Иран и Бурма).[27] Стога не чуди чињеница да је у великом броју држава које су политички и економски конфронтиране са САД и које имају унутрашње политичке проблеме за-

[25] Кине, Индије, великог броја држава Трећег света, несврстаних држава и дела европских и латиноамеричких држава.

[26] Скуп тих елемената информационог простора чини критични информациони простор, који је дефинисан у националном законодавству и одговарајућим међународним споразумима.

Доктрина информационой безопасности Российской Федерации (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895), http://www.scrf.gov.ru/documents/5.html, (18. 4. 2011).

[27] “Editorial: Iran’s Twitter revolution”, The Washington Times, 16. јун 2009, http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/ (2. 6. 2010).

брањена њихова употреба.[28] Пошто је сајбер простор најдецентрализованији облик медија, са великом стопом раста, изузетно је погодан за превазилажење медијске цензуре. У сарадњи са академским и невладиним институцијама, влада САД развија велики број пројеката помоћу којих се превазилазе контрола и блокирање интернет саобраћаја од стране домаћих влада.[29] Тиме сајбер простор постаје област у којој суверенитет не остварује страна која има право, већ она која има објективну моћ да га оствари. У таквим ситуацијама, (зло)употреба сајбер простора у комбинацији са позивањем на опште цивилизацијске вредности, попут људских права и демократије, може буде политичко средство избора за утицај на страну владу. Такав начин организовања је имао велики одјек међу млађом опозиционом популацијом у Ирану у периоду од 2007. године до данас и значајно је утицао на интензивирање масовних опозиционих протеста након председничких избора, упркос чињеници да је у том периоду у Ирану популарност друштвених мрежа на интернету била готово занемарљива (у време протеста било је само око 20.000 регистрованих корисника *Twittera*) [13]. Ипак, социјалне мреже на интернету не могу да се сматрају „оружјем" из сајбер света, јер оружје не подлеже принципима људских права или етичности, нити има политичку вољу, већ је подједнако ефикасно против сваког циља. Такав вид употребе сајбер простора није свемогућ, јер су за њега неопходни и други, доминантнији, друштвени услови, попут унутрашње политичке, социјалне и економске нестабилности, ограничене слободе и независности медија, ауторитативног режима и специфичних друштвених односа између власти и становништва. За такав вид пропагандног политичког дејства посебно су погодна друштва са строгим традиционалним нормама и великим процентом незадовољне млађе популације која има могућност да користи интернет и прати медије економски развијених држава (као што су, на пример, све државе арапског поднебља). Потврда за то су, на пример, неуспешни покушаји самоорганизовања политичких протеста у Хрватској, Црној Гори, Србији и Шпанији током пролећа 2011. године. Наиме, били су неуспешни, уз мали одзив, јер осим колективног незадовољства властима нису имали организовану политичку позадину. С обзиром на то, може се закључити да интернет није нужан услов за ширење идеја или пропаганде, већ је погоднији од других медија због брзог ширења употребе, лаке доступности информација и најнижем степену цензуре у односу на друге медије.

За Русију, због наведених околности, информационо деловање у сајбер простору има примаран значај. У руској војној доктрини се не користе изрази *сајбер ратовање* или *операција*, већ искључиво *информационо ратовање*, док је безбедност у сајбер простору део информационе безбедности.[30] Русија сматра да се у међународним односима свако намерно ширење информације на интернету од стране неке стране владе ради подривања или рушења владе друге државе мора квалификовати као агресија и сматрати незаконитом у духу Повеље УН, при чему „*било који праведни циљ, попут промовисања демократије, не може бити употребљен као*

[28] Кина, Иран, Вијетнам, Узбекистан, Пакистан, Сирија и Бангладеш.

[29] Psiphon, Tor, UltraSurf, FreeGate, Gtunnel, FirePhoenix и други.

[30] У фебруару 2010, Русија је званично објавила нову војну доктрину за наредну декаду. Иако се у њој не помињу директно сајбер безбедност или интернет, обухваћен је аспект информационе безбедности, који по руској доктрини обухвата интернет, медије и сајбер безбедност. *Военная доктрина Российской Федерации*, 5. фебруара 2010, http://news.kremlin.ru/ref_notes/461, (17. 5. 2010).

оправдање за такве акције" [14]. Међутим, тај став је технолошки неодржив, јер се подразумева апсолутна медијска контрола сајбер простора, самоизоловање и деловање у супротности са позитивним препорукама међународних органа о слободи приступа информацијама. Зато у домену сајбер простора већ дуго трају два велика концепцијска сукоба: за и против неутралности интернета на унутрашњем и економском пољу и борба за јачање националног суверенитета над властитим сајбер простором на националном и међународном нивоу.

Сасвим супротан став промовишу САД и државе окупљене око НАТО-а. Оне негирају право на сваки покушај успостављања државне цензуре над идејама и информацијама на интернету, што образлажу универзалним принципом заштите људских права и демократије [15, 16]. Упориште за то имају у ставовима познатих међународних невладиних организација за заштиту људских права [17]. Стога САД константно врше притисак на Кину, Иран, Бурму, Кубу, Сирију и друге државе, настојећи да подстакну јавно неповерење локалног становништва у институције њихових влада, посебно у односима који се тичу остваривања људских права.[31] Са америчког становишта, информационо деловање не може да буде облик оружане агресије на неку државу онако како га препознаје међународно право. Сједињене Државе подразумевају да сајбер напад чини искључиво офанзивна употреба сајбер оружја, срачуната на наношење штете (привременим или трајним нарушавањем или онеспособљавањем функције) одређеном циљу који зависи од информација и информационих система који су директан објекат напада, односно напад чија се природа манифестује кроз технички аспект сајбер ратовања.

У ситуацији када не постоје заједнички међународни став и усвојена терминологија у области сајбер ратовања, неопходно је да се као полазна основа у разматрању узме једини општи систем вредности, који је представљен у међународном јавном праву. Јер, иако се у међународном праву нигде експлицитно не помиње сајбер ратовање, његови прописи се у општем случају могу применити и на тај облик сукоба. На пример, основни међународни уговор, Повеља УН, обавезује све чланице УН да: „решавају своје међународне спорове мирним путем, тако да мир у свету, безбедност и правда не буду повређени".[32] Приликом оснивања Уједињених нација, примарни циљеви те најшире међународне организације били су очување светског мира и безбедности,[33] па Повеља УН и међународно право садрже принцип апсолутне забране употребе силе државама, осим у случају легитимних ситуација попут самоодбране.[34] Чланом 51 Повеље постављен је императив да се све чланице „у својим међународним односима суздржавају од претњи силом или употребе силе против територијалног интегритета или политичке независности било које државе, те од употребе силе на било који други начин који није сагласан са циљевима УН".[35] Иако се Повељом УН забрањује примена силе, држави су дозвољене акције које су разумно неопходне ра-

[31] Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China* 103-34, Stanford University Press, 2008. година. Зенг закључује да је интернет „одиграо важну улогу у успостављању политичке либерализације у различитим аспектима као што су политичка отвореност, транспарентност и одговорност".

[32] Повеља УН, чл. 2, ст. 3.

[33] Sean Murphy, *Principles of International Law*, Concise Hornbooks, Thompson West, 2006. године, стр. 439.

[34] Повеља УН, чл. 51.

[35] Повеља УН, чл. 5, ст. 4.

ди самоодбране у случају када је суочена са опасношћу оружаног напада,[36] и то све док међународна заједница не предузме мере да организовано заустави почетни напад.[37] Пошто су принципи међународног права исказани у Повељи УН универзални, јасно је да је та формулација примењива и на акте агресије изазване сајбер нападима. У концепту права на самоодбрану кључни појмови су *оружани напад* и *агресија*. *Оружани напад* је дефинисан у члану 51 Повеље УН, у којем су наведени изузеци за оправдану употребу силе од стране било које државе чланице УН који не подлежу санкцијама Савета безбедности УН.[38] Међутим, Повељом УН није прецизно дефинисано која акција представља употребу силе. Та чињеница је била повод за недоумице и спорења између разних држава, а поново је постала актуелна у случају информационог и сајбер ратовања. У време настанка Повеље и одговарајућих конвенција права оружаних сукоба доминантан облик агресије у међународним односима била је примена физичке силе (оружје с кинетичким дејством). За разлику од њих, савремене сукобе карактерише примене суптилнијих, неоружаних метода утицаја на противничку страну (у подручју дипломатије, права, економије и информација) које нису нужно повезане с војним дејствима [18]. Питање природе агресије детаљније је објашњено у Резолуцији Генералне скупштине УН бр. 3314 о дефинисању агресије, из 1974. године.[39] У чл. 1 те резолуције наведено је: „Агресија је употреба *оружане силе* од стране неке *државе* усмерена против *суверенитета, територијалног интегритета* или *политичке независности друге државе* или која је *на било који начин несагласна са Повељом УН*, на начин како је наведено у овој дефиницији".[40] Члан 3 Резолуције садржи списак дела која се могу квалификовати као агресија (инвазија или напад оружаним снагама, бомбардовање, блокада лука и обала, употреба оружаних снага на територији друге државе супротно споразуму, допуштање злоупотребе вла-

[36] Ian Brownlie, *International Law and the Use of Force by States*, Oxford, Clarendon Press, 1963, стр. 432–433. Професор Јан Браунли је категорисао неколико изузетака у вези са ограничавањем употребе силе према чл. 51. Повеље УН:

1. акт самоодбране;
2. акт колективне самоодбране;
3. акције одобрене од компетентног органа (на пример, Савет безбедности УН);
4. када према међународним споразумима постоји право на интервенцију у случају ад хок захтева неке стране или када је та интервенција оправдана по принципу територијалног суверенитета;
5. у случају потребе за прекидањем злочина;
6. у случају потребе због природне катастрофе и
7. због предузимања мера ради заштите живота и власништва властитих држављана на страној територији.

[37] Повеља УН, чл. 42 („Савет може да предузме акцију која је потребна ради одржавања или успостављања мира и безбедности у свету ваздухопловним, поморским или пешадијским снагама. Таква акција може укључивати и демонстрације, блокаде или друге операције ваздухопловних, поморских или пешадијских снага чланица Уједињених нација") и чл. 43, ст. 1 („Да би допринели одржању мира и безбедности у свету, све чланице Уједињених нација се обавезују да своје оружане снаге, помоћ и олакшице, укључујући и право пролаза, ставе на располагање Савету безбедности и то на захтев Савета и у складу са посебним споразумом или споразумима ради одржавања мира и безбедности у свету").

[38] *Исто*, чл. 51.

[39] Дефиниција агресије, Резолуција Генералне скупштине 3314 (XXIX), чл. 1, 14. децембар 1974, http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/3314(XXIX)&Lang=E&Area=RESOLUTION, (20. 5. 2010)

[40] *Исто*, у чл, 3. те резолуције наведено је седам чинова који се сматрају агресијом, а у чл. 4 каже се да агресија није ограничена на тих седам чинова.

стите територије за напад на трећу страну, ангажовање нерегуларних група да користе оружану силу), а у чл. 4 речено је да та листа није коначна. Међу наведеним делима се не помиње сајбер ратовање, што је и разумљиво, јер је Резолуција претходила времену његовог настанка, али је предвиђена могућност да се списак дела прошири напоменом да није коначан.[41] Ни сам појам *сила* се није једнако схватао током историје, већ је различито интерпретиран у различитим околностима, што ће се вероватно наставити и у будућности. Основ за такву тврдњу је Бечка конвенција о уговорном праву:[42] „Споразум ће бити интерпретиран у доброј вери у складу са уобичајеним значењем које је садржано у изразима уговора у њиховом контексту и у светлу њиховог предмета и сврхе".[43] Из претходног става се намеће питање које је то уобичајено значење појма *сила*, односно да ли се подразумева да се он односи на оружану силу или и на друге облике присиле, попут манифестације силе унутар или кроз сајбер простор.[44] Иако је то дискутабилно питање, у међународној јавности је у прошлости преовладавао став да се појам *сила* наведен у Повељи УН не односи искључиво на оружану силу, већ да има шире значење,[45] као што је, на пример, примена биолошког и хемијског оружја.

Римским статутом Међународног кривичног суда, нарочито чл. 5, регулише се надлежност тог суда за најозбиљнија кривична дела, која је као таква прогласила целокупна међународна заједница, попут геноцида, злочина против човечности, ратних злочина и агресије.[46] У њему је наведено и да дефинисање појма *агресија* није окончано од стране међународне заједнице.[47] Тиме је омогућено међународној заједници да дефинише нове облике агресије, попут сајбер напада, који би тако потпали под надлежност Међународног суда правде.

То питање има изузетну важност за целокупни концепт сајбер ратовања. Право државе на самоодбрану као одговор на претходни сајбер напад постоји једино у случају када тај напад достигне ниво оружаног напада. Међутим, досадашња пракса у примени силе у сајбер простору показује неусаглашеност међународних ставова. Током сајбер

[41] *Исто*.

[42] Vienna Convention on the Law of Treaties, 1969. година (ступила на снагу 1980. године). http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf, (20. 5. 2010).

[43] Vienna Convention on the Law of Treaties, чл. н 31, ст. 1.

[44] Детаљнију анализу значења појма *сила* и *оружана сила* у контексту Повеље УН, у чл. 2, ст. 4, видети у: Michael N. Schmitt, „Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", страна 13. Рад је објављен у ревији *The Columbia Journal of Transnational Law*, Vol. 37, 1999, стр. 885–937.
http://www.google.com/url?sa=t&source=web&ct=res&cd=2&ved=0CA0QFjAB&url=http%3A%2F%2Fww.usafa.edu%2Fdf%2Fiita%2FPublications%2FComputer%2520Network%2520Attack%2520and%2520the%2520Use%2520of%2520Force%2520in%2520International%2520Law.pdf&ei=fhDySs_wAYOnsAa46LWjDw&usg=AFQjCNFauYdszo2qE3c7zgi-F7CjH6w9Lw&sig2=a9x3zjTn5sl9el5FOCkUqg, (20. 5. 2010).

[45] *Исто*, стр. 10–22.

[46] http://untreaty.un.org/cod/icc/statute/romefra.htm, (16. 05. 2010).

[47] Римски статут међународног кривичног суда, „Службени лист РСЈ" – Међународни уговори, бр. 5/2001, чл. 5, ст. 2. „Суд је надлежан за кривично дело агресије након што се прописима донетим у смислу чланова 121. и 123. установе елементи бића овог кривичног дела, и тако испуне претходни услови за установљење надлежности Суда. Ти прописи морају бити у складу са одговарајућим одредбама Повеље Уједињених нација".

инцидената у Естонији, 2007. године, и Грузији, 2008. године, непознати нападачи су у синхронизованим серијама *DDoS* напада[48] извесно време блокирали рад неколико интернет сајтова владиних, медијских и финансијских институција.[49] Естонски министар одбране је тада јавно упоредио насталу ситуацију с блокирањем морских лука,[50] што је према наведеној резолуцији Генералне скупштине УН о агресији[51] акт агресије.[52] У другом случају, председник Грузије је чак тражио интервенцију страних влада, али је је, уместо ње, добио технолошку помоћ водећих америчких приватних интернет компанија. Наиме, према међународном праву наведене акције се не сматрају актима агресије. У чл. 41 Повеље УН наведено је да „...потпун или делимичан прекид економских веза или железничких, ваздушних, поштанских, *телеграфских, радио* и *других линија комуникације*...“ не представља употребу мера оружане силе.[53]

Један од основних принципа права оружаних сукоба је *пропорционалност*, што значи да легитимна самоодбрана неке државе постоји само у случају да је претходно угрожена актом агресије који јој даје право на реципрочан одговор.[54] То значи да превентивна примена сајбер напада или прекомерно агресивна одбрана (на пример, авио-бомбардовање нападача као одговор на сајбер напад ограниченог дејства) не би била легална реакција. У Националној војној стратегији за сајбер операције из 2006. године администрација САД навела је да ће Министарство одбране САД водити офанзивне и дефанзивне акције са применом физичке (кинетичке) силе ради очувања слободе акција и постизање оптималних војних ефеката и стратегијске предности у сајбер простору [19]. У најави нове војне сајбер стратегије, америчка војска је увела категорију „еквивалентности“ напада од које зависи врста војног одговора. Уко-

[48] *Distributed Denial of Service Attack*, врста напада у којем нападач слањем лажних масовних порука блокира ресурсе нападнутог система и чини га недоступним за нормално функционисање његовим корисницима. У Великој Британији, САД и више дугих држава такав напад је проглашен незаконитим делом за које је предвиђена озбиља затворска казна.

[49] Maricelle Ruiz, “Internet Law - Should We Go to War Over a Massive Cyber Attack?”, *Internet Business Law Services*, 23. мај 2007.
http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1762, (20. 5. 2010).

[50] Mark Landler & John Markoff, “Digital Fears Emerge after Data Siege in Estonia”, Valentinas Mite, „Estonia: Attacks Seen As First Case of ‘Cyberwar’“, 30. мај 2007. године, Radio Free Europe,
http://www.rferl.org/content/Article/1076805.html, (17. 7. 2009).

[51] Дефиниција агресије, Резолуција Генералне скупштине 3314, чл. 3 (ц),
http://www.un-documents.net/a29r3314.htm, (20. 5. 2010).

[52] Johnny Ryan, “Growing Dangers: Emerging and Developing Security Threats”, *NATO Review*, 2007,
http://www.nato.int/docu/review/2007/issue4/english/analysis2.html, (20. 5. 2010).

[53] Повеља УН, чл. 41.

[54] У Повељи УН, чл. 2, параграф 4, државама се указује да треба да се: „...уздржавају од претње силом или употребе силе против територијалног интегритета или политичке независности сваке државе, или на други начин несагласан са циљевима Уједињених нација“. У чл. 51 наводи се: „Ништа у овој Повељи не умањује природно право на индивидуалну или колективну одбрану у случају оружаног напада на члана Уједињених нација док Савет безбедности не предузме мере потребне за очување мира и безбедности у свету. О мерама које предузму чланови користећи се овим правом на самоодбрану биће одмах обавештен Савет безбедности и ове мере ни на који начин неће довести у питање овласти и одговорности Савета да у складу са овом Повељом предузме у свако доба акцију коју сматра нужном у циљу обезбеђивања и одржања мира и безбедности у свету“,
http://www.bgcentar.org.yu/documents/Povelja%20Ujedinjenih%20nacija.htm, (20. 05. 2010).

лико сајбер напад изазове смрт лица или материјална уништења еквивалентна нападу кинетичком силом, одговор војном физичком силом ће се узети у разматрање.[55] У студији Националне академије наука САД наведена је изјава званичника америчке војске да није одбачена чак ни могућност нуклеарног одговора на сајбер напад.[56] Није легално ни коришћење сајбер простора за подстицање немира или побуна против легалне политичке власти у сувереним државама (тзв. *Twitter* или *Facebook* револуције), што је вероватно био случај током протеста у Ирану, Бурми, Сирији и Либији. Према Резолуцији Генералне скупштине УН бр. 2625, ратна агресија се сматра „*злочином против мира* и државе чланице се опомињу да се уздрже од „аката одмазде које укључују употребу силе и од *организовања, подстицања, асистирања* и *учествовања у цивилним сукобима или терористичким нападима у другој држави*".[57]

Логичан пут за дефинисање природе сајбер напада јесте упоређивање последица које примена силе остави на циљ. У већини досадашњих сајбер напада на националну сајбер инфраструктуру (попут случајева у Естонији, Грузији, Киргистану или САД) подразумевала се примена неинвазивних метода с привременим последицама слабог интензитета, попут *DDoS* напада. У скоро свим досадашњим случајевима сајбер ратовања основна правна препрека за закониту примену начела самоодбране била је немогућност доказивања да је, по последицама, сајбер напад достигао ниво напада кинетичком силом. Ипак, такав начин не може бити ефикасан у свим случајевима, посебно због немогућности превенције напада који нису у складу са правом и у случају неефикасне примене силе са намером изазивања таквих последица.

Проблем одређивања последица остварене силе јавља се и у случају сајбер шпијунаже, као честе активности која се одвија између држава у сајбер простору. У начелу, сајбер шпијунажа се не сматра актом ратовања, али је дискутабилно како би такав акт, у случају откривања, окарактерисале угрожене државе.[58] Утолико пре јер су у примени сајбер шпијунаже и ратовања готово идентичне технике, методе и средства, а сајбер шпијунажа би се, у принципу, најтеже могла окарактерисати као акт агресије. Пример за то је одлука Савета безбедности[59] у вези с познатим инци-

[55] Siobhan Gorman, Julian E. Barnes, „Cyber Combat: Act of War", The Wall Street Journal, 31. мај 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=googlenews-_wsj#printMode, (31. 5. 2011).

[56] William, A., Owens, Kenneth, W. Dam, and Herbert S. Lin, „Technology, Policy, Law, and Ethics regarding U.S. Acquisition and Use of Cyberattack Capabilities", National Academy of Sciences, 2009, ISBN 976-0-309-13850-5.

[57] Резолуција Генералне скупштине УН 2625, Декларација о принципима међународног права који се односе на пријатељске односе и сарадњу међу државама у складу са Повељом УН, 24. октобра 1970, http://www.yudikorsou.com/download/UN%20GENERAL%20ASSEMBLY%20RESOLUTION%202625.doc, (20. 5. 2010)

[58] Досадашњи случајеви, попут велике шпијунске мреже *GhostNe,t* која је пратила канцеларије тибетанског Далај Ламе и била раширена у многим државама света, углавном на рачунарима амбасада и конзуларних представништва многих држава, укључујући и амбасаду Индије у Београду, нису били ни у једном случају означени као акти агресије.

[59] Заседања Савета безбедности УН 857, 858, 859 и 860:
http://www.undemocracy.com/S-PV-857, (20. 5. 2010);
http://www.undemocracy.com/meeting/S-PV-858, (20. 5. 2010);
http://www.undemocracy.com/meeting/S-PV-859, (20. 5. 2010);
http://www.undemocracy.com/meeting/S-PV-860, (20. 5. 2010);
http://www.undemocracy.com/S-PV-860/page_17/rect_142,1005_509,1200, (20. 5. 2010);
http://www.undemocracy.com/S-4321, (20. 5. 2010).

дентом из времена „хладног рата“ у којем је СССР, 1960. године, изнад властите територије оборио амерички шпијунски авион У-2, „црна птица“, који се налазио у неовлашћеној шпијунској мисији.[60] Тада се Савет безбедности УН није сложио са тврдњом СССР-а да је та акција чин агресије САД и донео је одлуку да тај акт није значио незакониту употребу силе, без обзира на очигледну повреду ваздушног простора Совјетског Савеза. Аналогно томе, може се сматрати да ни шпијунски сајбер упад у информационе мреже неке земље није акт незаконите примене силе [20]. Међутим, у таквом случају допуштене су акције самоодбране земље чији је простор повређен (копно, ваздушни, сајбер или било који други простор), јер ни у једној држави, према националном праву, шпијунажа није дозвољена.[61] Ситуација је много сложенија у случају сајбер упада у информационе системе неке државе којима се онеспособљавају њени информациони капацитети, чиме се, директно или посредно, наноси штета њеној способности да се брани, материјалним и финансијским ресурсима или целокупном становништву.

Сајбер напади могу имати широк распон дејстава на различите циљеве и последица, па се приликом оцене њихове природе тешко може применити исти критеријум. То потврђује неколико карактеристичних сајбер напада. На пример, израелска војска је 2007. године, током комбиноване диверзантско-обавештајно-ваздухопловне акције „Воћњак“, уништила нуклеарно постројење у изградњи[62] у Сирији. При томе је највероватније применила комбинацију операција у електромагнетном спектру и сајбер простору ради онеспособљавања сиријског радарског система у време ваздухопловног напада израелске војске на наведени циљ.[63] Тај инцидент је могао да прерасте у много шири војни сукоб између те две државе, које су формално у стању рата од 1967. године, након што је Израел окупирао део сиријске територије. Сам напад није био анониман, али је изведен тајно, без објаве рата или упозорења.

Велики део међународне јавности сумња да је Израел умешан и у подметање рачунарског вируса *Stuxnet* у нуклеарна постројења Бушер и Натанц у Ирану. Тај злонамерни код је откривен 2010. године, након што је изазвао квар система аутоматизоване контроле рада нуклеарних постројења. Такав напад на нуклеарно постројење у којем се обогаћује уранијум могао је да има опасне последице по становништво и природну средину и представља озбиљно кршење права оружаних су-

[60] Arie. J. Schaap, “Cyber warfare operations: Development and use under international Law”, *The Air Force Law Review*, Cyberlaw Edition, Vol. 64, 2009, стр. 143.
http://www.thefreelibrary.com/Cyber+warfare+operations:+development+and+use+under+international+law.-a0212035712, (20. 5. 2010).
Видети: U.S. Department of State, Foreign Relations of the United States: 1958-60: E. Europe Region; Soviet Union; Cyprus,
http://dosfan.lib.uic.edu/ERC/frus/frus58-60x1/13soviet7.html, (20. 5. 2010).

[61] У начелу, шпијунажа је дозвољена у међународном, али не и у националним законодавствима.

[62] Erich Follath, Holger Stark, „How Israel Destroyed Syria’s Al Kibar Nuclear Reactor“, Spiegel Online International, 02. новембар 2009. године,
http://www.spiegel.de/international/world/0,1518,658663,00.html, (13. 8. 2010).

[63] „IAEA reports Syria over undeclared reactor“, World Nuclear News, 10. јун 2011. године,
http://www.world-nuclear-news.org/NP-IAEA_reports_Syria_over_undeclared_reactor-1006117.html, (15. 6. 2011).
Richard Clarke, „Cyber War“ 2010, HarperCollins, ISBN: 987-0-06-199239-1, стр. 13–19.

коба.[64] Међутим, без обзира на константно стање непријатељства између Ирана и Израела, између те две државе не постоји формално стање рата, нити оружаног сукоба, и мала је вероватноћа да се докажу порекло наведеног напада и одговорност нападача.

Пред сам почетак Другог заливског рата, 2003. године, војска САД извела је пробој у комуникациони систем електронских порука ирачке војске кроз који је послала позиве ирачким официрима на предају. Тим сајбер нападом није изазвана никаква физичка штета, већ је представљао пропагандно-информационо дејство. Десио се у припремној фази оружаног рата између две државе и није супротан одредбама постојећег права које се односи на оружане сукобе.

Обимни *DDoS* напади су честа појава у сајбер простору и неки од њих су имали карактер неформалног међудржавног сукоба, попут напада на Естонију 2007. године, Грузију 2008. године и Киргистан, САД и Јужну Кореју 2009. године. Сви ти напади су изведени техником која у редовном интензитету представља легитимну активност према неком серверу (слање захтева за информацијама), али с неуобичајеном великом фреквенцијом понављања активности. То значи да напад није везан за избор сајбер средства, већ за начин (метода) његове примене. Међу државама жртвама и могућим нападачима није постојао сукоб, али је било политичких несугласица. Нападе су предузимале самоорганизоване групе, највероватније без контроле руске државе. Изузетак је напад на Грузију, који се десио готово паралелно са оружаним војним сукобом између Русије и Грузије. Ипак, порекло сајбер напада није утврђено. Ти *DDoS* напади јесу привремено онемогућили рад појединих државних информационих система, али нису оставили последице које су могле да се окарактеришу као акти агресије, чак ни у случају да се могла доказати умешаност државе нападача. Ипак, без обзира на квалификацију нивоа агресије, све наведене ситуације су могле да прерасту у шире сукобе, будући да су Естонија и САД чланице НАТО-а, Грузија – чланица „Партнерства за мир“, а Јужна Кореја је контактна чланица и један од најважнијих савезника Сједињених Држава. У току сукоба је покренуто и питање неутралности, јер су приватне компаније из САД и других држава понудиле нападнутим државама, као помоћ, властите капацитете.

Без обзира на то што *DDoS* напади, шпијунске акције, подметање рачунарских вируса и црва и слични облици нарушавања рада информационих и зависних система остављају последице на мету напада, у већини случајева се не могу доказати њихово порекло и одговорност државе нападача, а ефекти им се углавном своде на привремено ускраћивање располагања информационим ресурсима и изазивање непријатности. Стога је општи став јавности да се они не могу квалификовати као дела којима се крше ставови из Повеље УН о употреби силе.[65] Према скоро

[64] „Фабрике или постројења која у себи садрже опасне силе, попут брана, насипа или електричних централа не смеју бити циљ напада, чак и када су такви објекти војни циљеви, уколико такав напад може изазвати ослобађање опасних сила и изазвати озбиљне последице међу цивилним становништвом“, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 (Допунски протокол I), чл. 56 (1). Та забрана престаје да важи када се ти објекти и објекти у њиховој непосредној околини не користе за предвиђену намену, већ за редовну, значајну и директну подршку војним операцијама и уколико је војни напад једини начин да се таква подршка оконча.

[65] Stephen W. Korns and Joshua E. Kastenberg, “Georgia's Cyber Left Hook”, *Parameters - U.S. Army War College Quarterly,* Vo1. XXXVIII, No. 4 (Winter 2008-2009).

свим стручним ставовима у вези с карактером сајбер напада на Естонију, чланицу НАТО-а, реч је била о сајбер криминалу или тероризму, без обзира на политичку позадину сукоба.[66] Правни тим Здруженог центра за сајбер одбрану НАТО-а[67] имао је идентичан став о непостојању основе за проглашење државне одговорности Русије за нападе у Грузији: „Веома је проблематична примена права оружаног сукоба на случај сајбер напада у Грузији због објективне чињенице да је случај толико нејасан да се не могу применити неопходни критеријуми за одлучивање о директној умешаности руске државе у случај, чак ни да су ефекти напада ишли у њену корист".[68] Међутим, последице сајбер напада могу имати много озбиљнији интензитет, посебно у случају физичког уништења система који зависе од функције информационе технологије. Иако се сајбер нападима не може остварити директно дејство на физички свет, нарушавањем рада информационих система и процеса у њима могу посредно да се изазову последице по техничке системе чији рад зависи од тих информација, система и процеса.

Иако је сајбер ратовање релативно ново, у историји „хладног рата" постоје примери који упућују на то да је информациона технологија и раније коришћена у такве сврхе. На пример, савремена Русија је енергетска сила захваљујући великим резервама нафте и природног гаса, што све чешће користи и као политичко средство у међународним односима. Када је њен претходник, бивши СССР, почетком осамдесетих година 20. века започео програм развоја енергетске инфраструктуре, совјетска власт је покренула широку акцију индустријске шпијунаже ради прибављања развијених западних технологија у тој области. Када је америчка страна сазнала за та настојања, започела је програм модификовања технологија за које су Совјети били заинтересовани ради његовог подметања. Наиме, америчке обавештајне службе су у систем контроле рада гасовода намерно уградиле озбиљну грешку и потом га подметнуле совјетским агентима за индустријску шпијунажу. Постоје тврдње да је подметнути софтвер употребљен у току изградње великог Транссибирског гасовода у СССР-у [21 стр. 81–82] и да је неко време радио без сметњи, а потом је изазвао поремећај у функционисању гасовода затварањем вентила на једној и изазивањем максималног притиска на другој страни. То је довело до велике експлозије, за коју поједини стручњаци сматрају да је била најјача експлозија ненуклеарног порекла која је икада измерена на планети – укупне јачине око три килотона.[69]

Такав сценарио је актуелан и у садашње време. Влада САД покренула је 2007. године серију тестова под називом *Aurora Generator Test*[70] да би оценила могућност физичких последица сајбер напада по државни електроенергетски систем. У њима је реално демонстрано могуће уништење делова система преузимањем контроле над

[66] *Исто*, стр. 71.

[67] Cooperative Cyber Defense Center of Exellence, Tallinn, Estonia, http://www.ccdcoe.org/.

[68] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook".

[69] Gus W. Weiss, „The Farewell Dossier", Central Intelligence Agency, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm, (25. 3. 2010);
John Markof, „Old Trick Threatens the Newest Weapons", *The New York Times*, 26. октобар 2009, http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=1&ref=science&pagewanted=all, (25. 3. 2010).

[70] Ted Bridis & Eileen Sullivan, "US Video Shows Hacker Hit on Power Grid", *SFGATE.COM* , 27. септембар 2007, http://www.sfgate.com/cgibin/article.cgi?f=/n/a/2007/09/26/national/w165704D09.DTL&type=politics, (15. 4. 2010).

системом електричног снабдевања и изазивањем поремећаја рада електричних централа уништењем електрогенератора.[71] Резултати експеримента су довели до тога да је америчка савезна електрорегулаторна комисија[72] 2008. године донела прописе којима је све електроенергетске компаније обавезала да примене специфичне мере сајбер безбедности, уз могућу казну од милион долара дневно за њихово непоштовање.[73] Могућност сајбер напада на електроенергетске мреже се све више повећава због све већег степеном зависности од умрежених информационих система. У циљу повећања ефикасности електричне мреже у САД, америчка државна администрација је донела одлуку о изградњи „Паметне мреже"[74] – информационог система за оптимизацију производње и утрошка електричне енергије, док је Европска унија усвојила одлуку о покретању сличног пројекта под називом *Super Smart Grid.*[75] Америчка агенција *CIA*, почетком 2008. године, издала је јавно саопштење о поседовању информација да су сајбер напади већ изазвали пад електричне мреже у неколико региона у свету ван Сједињених Држава,[76] а у америчкој јавности се већ дуже време спекулише о могућности да се исто деси и са њиховим капацитетима.[77] Такви напади могу имати несагледиве последице, пошто је веома реална могућност сајбер напада и на нуклеарна постројења.[78] Сви ти напади би имали статус ратног злочина, под условом да се може доказати одговорност државе нападача. Међутим, последице сајбер напада нису довољан критеријум за одређивање њихове природе и легалности. Оне могу да настану и случајно, грешком или као изоловани акт неког појединца, па у међународној заједници постоје различити ставови око тога шта је сајбер напад.

Мајкл Шмит, декан и професор међународног права у Европском центру за безбедносне студије „Џорџ К. Маршал"[79] сматра да неки сајбер напад може бити дефинисан као оружани напад уколико *има за циљ* изазивање повређивања или смрти људи, оштећење или уништење имовине, или у случају да су такве *последице* напада очекиване.[80] Иако се из постојећег међународног права не може извести закључак

[71] Richard Clarke, *Cyber War*, стр. 88.

[72] Federal Energy Regulatory Commission, www.ferc.gov.

[73] Federal Energy Regulatopy Commision, *The Strategic Plan*, http://www.ferc.gov/about/strat-docs/FY-09-14-strat-plan-print.pdf, (22. 3. 2010).

[74] John Carey, „Obama's smart grid game plan", *Bloomberg Business Week*, 27. октобар 2009, http://www.businessweek.com/technology/content/oct2009/tc20091027_594339.htm, (22. 3. 2010).

[75] A. Battaglini, J. Lilliestam, C. Bals, A Haas, „The SuperSmart Grid, Potsdam Institute for Climate Impact Research", *European Climate Forum* ,18. јун 2008. године, http://www.supersmartgrid.net/wp-content/uploads-/2008/06/battaglini-lilliestam-2008-supersmart-grid-tallberg1.pdf, (22. 3. 2010).

[76] Tom Spiner, „CIA: Cyberattack caused multiple-city blackout", *CNET News*, 22. јануар 2008, http://news.cnet.com/CIA-Cyberattack-caused-multiple-city-blackout/2100-7349_3-6227090.html, (15. 4. 2010). У изјави је наведено да *CIA* не поседује информације о томе ко су нападачи или каква је била сврха напада, али да су изведени путем упада са интернета.

[77] Anne Broache, "Will cyberintrusions crash U.S. electrical grid?", *CNET News*, 17. октобар 2007, http://news.cnet.com/8301-10784_3-9799403-7.html, (15. 4. 2010).

[78] „Russia says Stuxnet could have caused new Chernibyl", Reuters, 26. јануар 2011, http://www.reuters.com/article/2011/01/26/us-iran-nuclear-russia-idUSTRE70P6WS20110126, (13. 5. 2011).

[79] Michael N. Schmitt, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany.

[80] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello", *International Review of the Red Cross*, јун 2002.

да се сајбер напади могу изједначити са недозвољеном употребом силе или оружаним нападима, том Шмитовом дефиницијом уводи се нови елемент. На основу њега, сајбер напади се карактеришу као оружани напади не само ако се остваре последице оружаног напада (повређивање или смрт људи, или оштећење или уништење имовине) већ и у случају да постоји циљ (намера, потенцијал) да се оне изазову. Прихватањем таквог стандарда, сви сајбер напади усмерени на системе битне државне инфраструктуре могу да се прогласе оружаним нападом. У том случају, може се применити право сваке државе на самоодбрану против таквог напада у складу са чл. 51 Повеље УН, при чему остаје обавеза избора пропорционалног одговора, о чему такође постоје несугласице због различите процене држава шта је пропорционалан акт. На пример, након терористичког напада 2001. године, САД објавиле су тзв. рат терору и предузеле ратни поход на Авганистан. То је било последица снажног настојања Владе САД (Бушова доктрина)[81] да убеди међународну јавност у амерички став да не треба правити разлику између терористичких организација и влада држава које им пружају заштиту. Многе државе света критиковале су такав став САД као потпору настојању да осигурају право да изводе војне акције било када и било где у свету.

Једина ограничења за самосталну процену врсте и интензитета војног одговора на претходни сајбер напад јесу поштовање принципа неопходности за одбрану и принципа пропорционалности у односу на почетни напад.[82] Тај стандард је у међународном праву током историје више пута потврђен, као у случају пресуде Међународног суда правде у случају Никарагва против САД[83] или у саветодавног мишљења Међународног суда правде о легалности претње или употребе нуклеарног оружја:[84] „...примена права на самоодбрану које подлеже условима неопходности и пропорционалности представља правило обичајног међународног права" и „...ова два услова се равноправно примењују са чланом 51. Повеље УН, без обзира на врсту примењене силе".[85] Према томе, одговор неке државе на напад није ограничен на специфичну врсту оружја или тип војног одговора све док је тај одговор у складу са принципима наведеним у Повељи УН да је неопходан и пропорционалан претходном нападу. То ограничење је изузетно важно, јер се у војним доктринама САД и Русије, највећих нуклеарних сила на свету, не постављају ограничења за врсту одговора на напад предузет на њихове државе.

На основу наведеног, може се закључити да је за сајбер напад, да би достигао ниво агресије, неопходно утврдити природу и врсту, обим и садржај последице и намену напада и намеру нападача. Иако је у сукобима у физичком свету често те-

[81] "National Security Strategy of the United States," септембар 2002, http://www.globalsecurity.org/military/library/policy/national/nss-020920.pdf, (04. 3. 2010).

[82] Та правила су уведена у обичаје међународног права након става државног секретара САД Данијела Вебстера у одговору Британцима на њихово позивање на самоодбрану у познатом Каролиншком инциденту. Michael C. Bonafede, "Here, There, and Everywhere: Assessing the Proportionality Doctrine and U.S. Use of Force in Response to Terrorism After September 11 Attacks", *Cornel Law Review*, 2002. година.

[83] Видети: Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. USA), 1986 International Court of Justice, 1986. godina, http://www.icj-cij.org/docket/index.php?p1=3&p2=3&code=nus&case=70&k=66 (13. 11. 2009).

[84] International Court of Justice, *Legality of the threat or Use of Nuclear Weapons*, 1996, стр. 226, параграф 41, http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&case=95&code=unan&p3=4, (03. 3. 2010).

[85] *Исто*, параграф 41, стр. 226.

шко утврдити наведене карактеристике, у сајбер простору је то вишеструко сложеније. Да би да нека држава остварила право на самоодбрану, неопходно је да је испуњен и други нужан услов: да је познат нападач и да он има државни субјективитет. Иако би било тешко доказати обе те чињенице, садашњи технички ниво сајбер простора чини да је државна одговорност за напад много теже доказива од тога да су последице сајбер напада достигле ниво напада кинетичким дејством.

Утврђивање државне одговорности за сајбер напад

За регулисање сајбер ратовања кључно је питање могућност идентификовања нападача и утврђивања одговорности државе за сајбер напад. Према праву оружаних сукоба, подразумева се да су у стању сукоба налазе субјекти међународног права,[86] али се то изузетно тешко може проценити. Наиме, сајбер нападе могу да покрену појединци са територије треће државе, а они могу имати одложено дејство, могу бити преусмерени на сервере других држава и могу да буду дистрибуирано покренути истовремено са више различитих позиција. Због тога је за утврђивање порекла напада, поред сајбер форензике, потребно да се примене и друге међународно прихватљиве методе доказивања одговорности неке државе. У том погледу погодан је пример правног преседана из праксе Уједињених нација у вези с одлуком о бомбардовању Либије, 1986. године, које су извеле САД као санкцију за претходни терористички напад на америчке војнике у једној немачкој дискотеци.[87]

Генерална скупштина УН изгласала је Резолуцију бр. 41/38[88] којом је потврдила да напад на неку државу на основу претпоставке или оптужбе да је пружила уточиште терористичкој организацији која је извршила напад или да је помогла у организовању терористичког напада није у складу са Повељом Уједињених нација. Донедавно, у свету је преовладавало мишљење да је међународно право засновано на односима међу државама са истим правима.[89] У том духу, самоодбрана је средство које омогућава једној држави да се сама заштити од оружаног напада друге државе, док је насиље које предузму недржавни субјекти према некој држави, њеним грађанима или имовини у надлежности криминалног права.[90] Међутим, међународне околности су се умногоме измениле. У вези с тим, карактеристичан је случај проглашења „рата терору“ од стране америчке администрације након терористичког напада на САД 2001. године. Он је послужио као основа за одлуку о покретању војне акције у Авгани-

[86] III Хашка конвенција о започињању непријатељстава из 1907. године, http://www.icrc.org/ihl.nsf/FULL/190, (9. 1. 2010).

[87] Након обавештајних активности, САД дошле су до сазнања да су за напад одговорна лица која су била сарадници либијских безбедносних агенција, што међународна заједница није потврдила.

[88] Резолуција Генералне скупштине УН бр. 41/38 (Doc. A/RES/41/38) од 20. новембра 1986, http://www.un.org/documents/ga/res/41/a41r038.htm, (3. 3. 2010).

[89] Michael N. Schmitt, „21st Century Conflict: Can the Law Survive?“, 8(2) *Melbourn Journal of International Law* 24, 2007, http://www.austlii.edu.au/au/journals/MelbJIL/2007/24.html, (3. 3. 2010).

[90] Antonio Cassese, “Terrorism Is Also Disrupting Some Crucial Legal Categories of International Law”, *European Journal of International Law*, Vol 12, No.5, стр. 993–1001, https://www.unodc.org/tldb/bibliography/Biblio_Internat_law_Cassese_2001.pdf, (3. 3. 2 010).

стану против власти талибана, уз образложење да су пружили уточиште и подршку терористичкој организацији Ал Каида, која је извела терористички напад. Иако је председница Националног удружења правника САД Марџори Кон[91] оценила је да је та војна операција, која непрекидно траје од 2001. године, међународноправно нелегитимна,[92] у међународној заједници о том проблему постоје супротна тумачења.

Према мишљењу многих стручњака, усвајање Нацрта прописа о одговорности држава за међународно противправна дела, 2001. године, од стране Комисије УН за међународно право био је преломни тренутак у историји међународног права.[93] У том нацрту дата је основа за опште правило у међународним односима у току сукоба да ће „понашање било ког државног органа бити сматрано актом те државе у сагласности са домаћим законом државе".[94] Према Комисији, државни орган представља „било коју особу или ентитет који има тај статус у складу са домаћим законима државе",[95] па неки државни орган не може избећи одговорности тврдећи да су одређени учесници прекорачили властите надлежности.[96] Међутим, иако се тим правилом ограничава могућност терористичких активности уз одобрење или знање државних органа, у духу савремених безбедносних изазова и технолошког развоја, посебно у области сајбер ратовања, јавља се потреба редефинисања постојеће интерпретације употребе силе у међународним односима, посебно у случајевима нарушавања државног суверенитета. Транснационалним активностима држава у сајбер простору које се тичу њихових унутрашњих послова лако може да се изазове кршење међународноправних принципа поштовања суверенитета држава и немешања у њихове унутрашње послове.[97] Иако наведени нацрт прописа није постао међународно обавезујући,[98] он се сматра битним показатељем стања међународ-

[91] Марџори Кон је професорка права на Правном факултету „Томас Џеферсон" у САД и председник Националног удружења правника Сједињених Америчких Држава.

[92] „Све државе имају обавезу да решавају међусобне спорове мирним путем и да ни једна нација нема право да користи војну силу сем у случају права на самоодбрану како је оно регулисано Повељом УН или посебном резолуцијом Савета безбедности". Инвазија на Авганистан није била легитимна самоодбрана на основу Повеље УН, јер је терористички напад био криминални акт, а не војни напад на другу државу. Авганистан није напао САД… Даље, није постојала евидентна претња за САД након напада 11. септембра 2001. године…неопходност самоодбране мора бити тренутна, потпуна, не остављајући прилику за премишљање о средству и тренутку примена", Marjorie Cohn, „Afganistan: The Other Illegal War", *AlterNet*, 1. август 2008, http://www.alternet.org/world/93473/afghanistan:_the_other_illegal_war/, (4. 3. 2010).

[93] Нацрт прописа о одговорности држава за међународно противправна дела (*Draft Articles on the Responsibility of States for Internationally Wrongful Acts),* усвојен од стране Комисије за међународно право (*International Law Commision)* UN, http://www.un.org/law/ilc/. Прописима о одговорности држава регулише се када и како су државе одговорне када прекрше неку међународну обавезу, http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, (10. 1. 2010).

[94] Нацрт прописа о одговорности држава за међународно незаконита дела, чл. 4, ст. 1.

[95] *Исто*, чл. 4, ст. 2.

[96] *Исто*, чл. 7.

[97] Декларација о принципима у међународном праву из 1970. године, (http://daccessdds.un.org/doc/RESOLUTION/GEN/NR0/348/90/IMG/NR034890.pdf?OpenElement) и Декларација о неприхватљивости мешања у унутрашње послове државе из 1965. године (http://www.un.org/documents/ga/res/36/a36r103.htm, 10. 1. 2010).

[98] Нацрт је представљен у Резолуцији Генералне скупштине УН бр. 56/83, без прејудицирања за касније усвајање у форми међународног споразума.

ног права. На њега се ослонио и Међународни суд правде, који је до сада неколико пута доносио одлуку о утицају државних органа на неки сукоб, приликом доношења пресуде у случају тужбе за геноцид БиХ против Србије.[99] Међутим, будући да је природа сајбер напада специфична, доказивање одговорности државе је сложен проблем, Иако би сваки сајбер напад који је покренула нека држава или који је изведен уз сагласност неке државе морао да подлеже правним последицама које проистичу из чл. 4 Повеље УН[100] уколико по природи и интензитету достигне ниво оружаног напада. Та околност отежава примену постојећег међународног права и подручје сајбер ратовања оставља нерегулисаним, па је једини могући пут у будућности изградња специфичних међународних прописа којим ће се дефинисати елементи сајбер ратовања и, у току њега, принципи државне одговорности. Регулисање сајбер ратовања и изградњу нових правила захтевају и најутицајнији фактори међународне заједнице [22]. При томе, неопходно је да ти прописи буду усклађени са постојећим међународним правом а опште правне претпоставке за владање у току сајбер ратовања могу да се изведу из досадашње међународне праксе у сличним ситуацијама. За утврђивање везе између државе и појединца у току сукоба у пракси међународног права постоје два карактеристична случаја на основу којих су настали стандарди за процене степена умешаности државе у неки сукоб. То су *начело потпуне контроле* и *начело ефективне контроле*.[101]

Тест „потпуне контроле“ или „први никарагвански тест“. Према одредбама чл. 4 Нацрта правила о одговорности држава за међународно противправна дела главна околност за утврђивање одговорности неке државе јесте деловање њених формалних, *de iure*[102] органа. Међутим, у пракси се ретко дешава да нека држава отворено противправно делује у сукобу тако што користи своје званичне органе. У тим приликама обично је реч о неформалним снагама под контролом државе, попут плаћеничких или паравојних снага.[103] Таква ситуација је вероватна и у сајбер ратовању, у којем се, због могућности прикривања стварног нападача, очекује ангажовање неформалних, националистичких или политичких група, или приватних компанија, па чак и *outsourcing* у друге државе. Ти *de facto*[104] државни органи не смеју да се игнори-

[99] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), International Court of Justice, http://www.icj-cij.org/docket/index.php?p1=3&k=f4&p3=4&case=91 (18. 3. 2010).

[100] Joyner i Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework".

[101] Antonio Cassese, „The Nicaraqua and Tadić Test Revisited in light of the ICJ Judgment on Genocide in Bosnia“, The European Journal of International Law, Vol. 18 no. 4, 2007, www.ejil.org/pdfs/18/4/233.pdf *, (13. 05. 2010).* Scott J. Shackelford, "State Responsibility For Cyber Attacks: Competing Standards For A Growing Problem"; Derek Jinks, „State Responsibility for the Acts of Private Armed Groups“, *Chicago Journal of International Law*, Vol. 4, 2003, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=391641, (12. 1. 2010).

[102] Израз *de iure* значи заснован на закону, с обзиром на прописани закон, и често је у супротности са стварном ситуацијом – *de facto.*

[103] *Blackwater Worldwide* (нови назив од 2009. године је „Xe Services“), америчка приватна компанија, представља највећу светску плаћеничку војску која је у блиским везама са десничарским естаблишментом у САД. Специјализована је за ратни *outsourcing*. James Risen, Mark Mazeti, „Blackwater Guards Tied to Secret C.I.A. Raids“, The New York Times, 10. децембар 2009, http://www.nytimes.com/2009/12/11/us/politics/11blackwater.html?_r=1&hp¸ (12. 1. 2010).

[104] Стварни, заснован на чињеницама, у пракси.

шу, јер би у том случају државе које их ангажују избегле одговорност за учешће у сукобима уз оправдање да они немају легалан статус у складу са домаћим правом. У ствари, основни проблем је правне и техничке природе – немогућност утврђивања ко су нападачи. Тест „потпуне контроле“ или „први никарагвански тест“ формулисао је Међународни суд правде у случају Никарагва против САД,[105] посебно параграфе 109 и 110 пресуде, приликом одлучивања о томе да ли се и под којим условима може приписати одговорност властима САД за деловање паравојне скупине „контраша“ током којег је дошло до тешких повреда хуманитарног права у Никарагви.[106] У тесту се разматра како се групе које нису органи неке државе по њеном унутрашњем праву *de facto* могу изједначити са њима јер, у суштини, потпуно зависе од те државе: не одлучују самостално и делују као њен инструмент.[107] Кључна питања у том тесту су:

– Да ли је нека држава формирала дотичну групу?

– Да ли постоји однос потпуне зависности те групе од државе и потпуно одсуство могућности самосталног деловања групе?

– Користи ли држава тај однос зависности и контроле?

– Да ли је држава одабрала и поставила политичке вође дотичне групе?

Уколико је држава основала неку групу, суштински је контролисала, одабрала и поставила њене вође и усмеравала јој активности, и ако су припадници те групе починили недозвољена дела, онда је, у комбинацији са принципом командне одговорности, та држава одговорна за последице напада који је предузела та група, чак и уколико државно руководство није имало намеру да изазове те последице, ни сазнања о постојању намере.[108] Тај стандард се односи на одговорност државе за властите органе или неку групу и поистовећује их са државом у погледу последица дејстава. Док год је деловање *de iure* и *de facto* органа службеног карактера, оно се аутоматски приписује држави, чак и ако је почињено при прекорачењу овлашћења или супротно датим упутствима.[109] Примена тог принципа повећава вероватноћу утврђивања државне одговорности у случају сајбер ратовања, али се тиме не решавају сви проблеми, јер се организовање борбених група суштински разликује од ангажовања сајбер нападача.

Тест „ефективне или оперативне контроле“ или „други никарагвански тест“. Према том тесту, за утврђивање државне одговорности за напад довољно је да се докаже да недржавни субјекти (појединци или групе) делују по смерницама неке државе или да се на било који начин налазе под њеном контролом.[110] У случају најте-

[105] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), параграфи 109 и 110, http://www.icj-cij.org/docket/files/70/6503.pdf?PHPSESSID=05fad554ae9feec6f32e8fcea282db53, (20.05.2010). Извештај Међународног суда правде: http://www.icj-cij.org/docket/index.php?p1=3&p2=3&k=66&case=70&code=nus&p3=4, пресуда: http://www.icj-cij.org/docket/files/70/6503.pdf, (12. 1. 2010).

[106] Суд је пресудио да су САД повредиле међународно право подршком побуњеничкој герили, вођењем психолошких операција против легалне владе у Никарагви и постављањем мина у њеним водама. Извршење пресуда блокирале су САД у Свету безбедности УН. Видети: http://www.unhcr.org/refworld/publisher,HRW,,NIC,467fca491e,0.html, (20. 5. 2010).

[107] Пресуда Босна против Србије, Међународни суд правде, стр. 140–141, параграфи 391–393; Пресуда Никарагва против САД, стр. 43–64, параграфи 93–114.

[108] Shackelford, S., “State Responsibility For Cyber Attacks: Competing Standards For A Growing Problem”.

[109] Пресуда Босна против Србије, стр. 142, параграф 398; Пресуда Никарагва против САД, стр. 36–40, параграфи 75–86; Нацрт прописа о одговорности држава за међународно противправна дела, стр. 45, чл. 7.

[110] Нацрт прописа о одговорности држава за међународно противправна дела, стр. 47, чл. 8.

жих повреда хуманитарног права неопходно је доказати постојање намере државног руководства и директних налога да се учине таква дела.[111] Тест је дефинисао Међународни суд правде параграфом 115 пресуде у суђењу Никарагва против Сједињених Америчких Држава.[112] Тај однос ефективне контроле постоји у ситуацији када нека држава финансира неку групу, координира и контролише њено деловање и издаје јој специфична и директна упутства или наредбе у вези с чињењем противправних дела. У том тесту општа и генерална упутства државе нису релевантна.[113] И у том случају држава је одговорна, без обзира на могуће прекорачење овлашћења или поступања у супротности са упутствима.[114] То начело је примењено у пракси Међународног кривичног суда за простор бивше Југославије у случају Тадић.[115]

Основна разлика између та два начела је у чињеници да ли нека држава има директну оперативну контролу над активностима недржавних субјеката и контролу над њиховим планирањем или нема. Под начелом потпуне контроле подразумева се да држава има контролу над паравојним снагама или другим недржавним субјектима који учествују у непријатељствима у случају када ти учесници делују у потпуној зависности од те државе. Када је реч о начелу оперативне контроле, сматра да се дела недржавне групе могу приписати држави у случају када држава пружа подршку тој групи (финансијску, логистичку и друге) и има улогу у њеном директном организовању и координацији.[116] Начело стварне контроле је строже јер се захтева утврђивање јачег степена зависности између државе и неке групе, па је, самим тим, теже за доказивање. У својој одлуци у предмету тужбе Босне и Херцеговине против Србије (Примена Конвенције о спречавању и кажњавању злочина геноцида)[117] Међународни суд правде применио је 2007. године одлуке из никарагванског процеса као правног преседана који се често користи у судској пракси. Том приликом је донео одлуку о ослобађајућој пресуди за државу Србију за геноцид у Сребреници. [118] Због непостојања очигледне везе између сајбер нападача и државе порекла и чињенице да је до сада предузето више акција у сајбер простору за које постоји сумња, али не и докази о пореклу напада, примена тих тестова може да буде важан путоказ за евентуални будући систем регулисања сајбер ратовања. Наведе-

[111] Марко Милановић, "State responsibility for genocide", *European Journal of International Law*, Vol 17, No. 3, 2006. године, стр. 553–604.
http://www.ejil.org/pdfs/17/3/204.pdf, (12. 1. 2010).

[112] Пресуда Никарагва против САД, стр. 54, параграф 115.

[113] *Исто*. Пресуда Босна против Србије, стр. 142–143, параграф 396–400.

[114] Нацрт прописа о одговорности држава за међународно противправна дела, стр. 45–47, чл. 7.

[115] Случај Тадић се односи на суђење Душку Тадићу, припаднику снага Републике Српске у току сукоба у Босни, који је осуђен на 20 година у процесу Међународног криминалног суда за бившу Југославију за дела која је учинио у току грађанског рата, http://www.iilj.org/courses/documents/Prosecutorv.Tadic.pdf, (12. 1. 2010).

[116] Међународни суд правде, Случај Тадић , бр. IT-94-1-I-ICTY, од 2. октобра 1995. године.

[117] Пресуда по питању случаја који се односи на примену Конвенције о спречавању и кажњавању злочина геноцида (Босна и Херцеговина против Србије и Црне Горе), од 26. фебруара 2007. године, Општа листа бр. 91. У пресуди је наведено да је Србија прекршила своју обавезу у оквиру примене Конвенције због неспречавања геноцида у Сребреници и по питању својих обавеза према Међународном криминалном трибуналу за бившу Југославију, али да није крива за сам злочин.
http://www.icj-cij.org/docket/files/91/13685.pdf#view=FitH&pagemode=none&search=%22stojanovic%22, (12. 1. 2010)

[118] *Исто*, стр. 140, параграф 391.

на два теста приписивања одговорности државе међусобно су искључива. Уколико се утврди могућност приписивања одговорности по основу једне врсте одговорности, неће се утврђивати одговорност у другом случају. Избор начела које ће се применити на сајбер ратовање зависи од ситуације, али је вероватнија примена начела ефективне контроле, због могућег прикривања порекла сајбер напада.[119] То значи да би се утврдила одговорност државе за сајбер напад довољно је да се утврди да ли постоји њена оперативна одговорност, без доказивања потпуне контроле нападача. Примена тог принципа је погодна у случају масовних *DDoS* напада, попут напада на Естонију и Грузију, али није погодна за софистицираније нападе, попут примене рачунарског црва *Stuxnet*, који представља много озбиљнију претњу.

Поред утврђивања достигнутог нивоа сајбер напада и одговорности државе за напад, у сајбер ратовању постоје и други карактеристични проблеми. Један од њих је проблем укључивања у сукоб статусно неутралних држава, јер сајбер напад може да путује кроз инфраструктуру више суверених држава прелазећи преко њихових националних граница (некада чак и истовремено, због природе *IT* протокола и пакетног слања података). У таквим околностима се повећава вероватноћа ширења сукоба, па питање суверенитета држава у сајбер ратовању има изузетну важност. Доктрина државне одговорности дуго постоји у међународном праву, али је постала готово ирелевантна за одређивање одговорности у случају сајбер напада. Према њој је свака држава обавезна да спречи покретање напада на другу државу са властите територије. Уколико није у могућности да спречи такав напад, или то не жели, онда се држава може сматрати одговорном за тај напад. Међутим, практична процена државне одговорности не може да се узме здраво за готово – зависи од природе напада и околности у одређеној ситуацији. Постоје и ставови да уколико држава има ефективну контролу над учесницима напада, онда она има и способност да усмери и властиту активност према њима ради остварења свог утицаја у датом случају. Уколико држава нема ефективну контролу над актерима напада, питање је да ли остварује општу контролу над њима, тј. да ли, и без обзира на то што не управља поступцима нападача, може да утиче на координацију и планирање њихових активности. Коначно, у већини случајева може се поставити питање да ли је нека држава индиректно одговорна за одређене активности у датом сукобу, односно да ли је изостанак њене реакције основа за тврдњу да је одговорна за сајбер напад. Питање процене одговорности државе за сајбер нападе је веома неодређено. Постоје чак и екстремни ставови да се нека држава може сматрати одговорном за сајбер напад на основу тога да ли је усвојила ефикасне законе помоћу којих би спречила високотехнолошки или сајбер криминал, да ли довољно активно примењује те законе и да ли сарађује са жртвама у току истраге сајбер инцидената, па чак и да ли има историју државе коју сајбер нападачи користе за нападе.[120] Као пример за противтезу таквим ставовима се могу сматрати напади који по природи немају, нити могу имати географско порекло, попут разних врста дистрибуираних напада (*Botnet* мреже, *DDoS* напади, ширење малициозног кода и слично).

[119] То начело је примењено и у случају Тадић у Хашком суду.

[120] Такви ставови нису у потпуности у складу с међународним правом и још увек важећим међународним правним системом, у коме се у потпуности признаје потпуни државни суверенитет. Шта више, такве ставове готово искључиво имају поједини представници америчке државне политике и у свету се углавном сматрају екстремним, тј. да су у функцији правдања санкција према некој земљи.

Тек у случају да се тачно одреде право порекло сајбер напада и природа нападача може се разматрати да ли је тај напад достигао ниво оружаног напада, као и врста и интензитет оправдане противмере према међународном праву оружаних сукоба. Да би се одредила легалност војног одговора потребно је да се анализирају следећа питања: да ли је употреба силе као одговора у складу са принципом војне неопходности, тј. да ли инцидент, осим на војни начин, може да се реши и другачије? Да ли је природа планираног одговора пропорционална нападу? Ако јесте, да ли је ниво силе која се користи претеран у односу на важност војних резултата који се желе постићи? Да ли се приликом планиране употребе силе адекватно разликују војни циљеви и цивилно становништво и добра? Сва постављена питања произилазе из основних принципа права оружаних сукоба. На њих тешко може да се одговори у контексту сукоба у сајбер простору. Очигледно, не постоји консензус око могуће примене постојећег права оружаних сукоба у међународној заједници, а веома је дискутабилно питање да ли и на који начин стварање нових прописа о сајбер ратовању може да помогне све док се не дефинишу основни појмови, у вези са којима постоји много субјективних ставова, заснованих на нејасним чињеницама [6].

Закључак

Основна опасност од сајбер ратовања је у нејасној разлици између стања рата и криминалног дела која лако може да доведе до ескалације сукоба. У складу с међународним правом, не постоји правна основа за напад на неку државу као акт самоодбране од претходног сајбер напада за који се не може доказати да је га је предузела та држава или да је изведен на основу њене подршке. Чак и у случају утврђивања одговорности појединца или групе за тај напад, свака акција против таквих извршилаца на страној територији значила би повреду њеног територијалног интегритета и суверенитета. Једина дозвољена мера је захтев држави порекла напада да предузме акције ради његовог заустављања.[121] Међутим, у случају да се установи да је нападач држава, настаје ситуација која није јасно регулисана. Такве ситуације значајно повећавају могућност ескалације сукоба у међународним оквирима. У пракси се изузетно тешко могу одвојити та два могућа сценарија због тога што се сајбер напади лако могу предузети прикривено, са било које локације у свету. Могућност за регулисање сајбер напада могу да буду класификација таквих напада у категорије, у зависности од ефеката који се нападима остварују, и одређивање одговарајућих противмера. Од тога зависе право на покретање и врста самоодбране.[122] Потребно је да свака национална стратегија буде у складу са одговарају-

[121] То је био случај током НАТО бомбардовања СР Југославије, када су упућени захтеви да се спрече активности хакера (са рачунара Београдског универзитета) и запрећено прекидом интернет саобраћаја уколико изостане таква акција.

[122] Michael N. Schmitt, декан и професор међународног права Колеџа за међународне и безбедносне студије Европског центра за безбедносне студије „Џорџ Маршал“ у Гармишпартенкирхену, у Немачкој, у свом раду „Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework“, објављеном у *The Columbia Journal of Transnational Law*, Vol. 37, 1999. године, на страни 29 понудио је следећи правни оквир за нормирање компјутерских мрежних напада заснован на шеми питања и одговора:

ћим законским, институционалним и процедуралним оквирима како би била легална. Неопходни услови за то су следећи:

– Као прво, потребно је да свака држава усвоји основну доктрину понашања у сајбер ратовању, усклађену са међународним правом, којом је обухваћен став о критеријумима и могућим опцијама деловања при одговору на безбедносне претње у сајбер простору.

– Следећи корак је прецизирање институција и органа који ће имати одређену улогу у процесу одлучивања о евентуалној примени сајбер одбране и ратовања.

– Последњи корак је дефинисање и разрађивање поступака и процедура, попут претходно дефинисаних шема понашања у разним околностима сајбер сукоба, укључујући различите варијанте војног одговора. То би могао да буде универзални правац дефинисања понашања сваке државе у ратном сукобу у сајбер простору.[123]

Сајбер ратовање доноси многе ризике. Због повезаности војних и цивилних информационих система, многи облици сајбер напада се лако могу проширити на цивилне мреже и изазвати глобалне последице. С обзиром на специфичности поштовања неутралности у сајбер простору, неселективном применом сајбер ратовања може се изазвати непотребна ескалација сукоба. Амерички и руски високи војни представници су у више наврата јасно изјавили да информационо и сајбер ратовање против њихових држава ни у ком случају не би било схваћено као невојни облик сукоба, без обзира на то да ли би било војних последица или не, а да војни одговор на такве нападе не би био ограничен на употребу сајбер средстава. Нападачи су у прилици да некажњено покрећу нападе који нису у складу са међународним правом, пошто често технички није могуће доказати порекло напада и идентитет нападача. Ти напади се могу предузимати са туђе територије или могу имати дуготрајно одложено дејство.

Појава нових средстава и врста ратовања није реткост у људској историји, али сајбер ратовање ипак представља велики изазов за међународно право јер се његова средства и методе технолошки развијају много брже од међународног права. Неки

„(1) Да ли је техника примењена у компјутерском мрежном нападу употреба оружане силе? Јесте, уколико је напад намењен за директно проузроковање штете на физичким објектима или за повређивање људи;

(2) Уколико није оружана сила, да ли је компјутерски мрежни напад ипак неки облик употребе силе, како то посматра Повеља УН? Јесте, уколико је природа његових последица истоветна са последицама које карактеришу употребу оружане силе;

(3) Уколико су рачунарски мрежни напади употреба силе (било оружане или не), да ли се могу сматрати применом силе у складу са принципом самоодбране како је она дефинисана у поглављу VII Повеље УН, или важећи скуп правних норми дозвољава њихову употребу у датим околностима?

а) Ако је одговор потврдан, таква употреба сајбер напада ће вероватно бити проглашена легалном.

б) Ако није, а такав напад представља употребу оружане силе, онда он крши члан 2, став 4 Повеље УН и обичајно међународно право по питању забране употребе силе.

ц) Уколико није, а такав чин представља употребу силе, али не оружане, биће прекршен само члан 2, став 4 Повеље УН;

(4) уколико компјутерски мрежни напад није досегао степен употребе силе, да ли постоји нека друга забрана у међународном праву која би забранила његову употребу? Највероватнији пропис, ако не и једини, би била забрана мешања у послове друге државе."

[123] Видети Процену о међународноправним питањима информационих операција Министарства одбране Војске САД, "An Assessment of International Legal issues in Information Operations", 1999. године, стр. 24, http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf, (23. 2. 2010).

од споразума тог права, попут Хашких конвенција, толико су већ дуго у међународној употреби да се данас скоро универзално сматрају обичајним правом. Ипак, сајбер простор је специфичан и приликом ратовања у њему постоје ситуације које су нове и за које се не може једногласно утврдити аналогија с постојећим правом. Стога је за ту врсту ратовања, поред постојећих, неопходна израда и потпуно нових међународних прописа. Такође, неопходно је да се дограде постојеће право усвајањем посебног правног система за регулисање сајбер ратовања. Њиме се мора обезбедити заштита цивила и цивилне инфраструктуре – људских права, и треба забранити неселективне, терористичке и нехумане врсте напада, нападе на критичну друштвену инфраструктуру и нападе којима се крши суверенитет држава у периоду када не постоји званична објава рата. Државе морају преузети одговорност за све нападе предузете у надлежности њиховог суверенитета и, у складу с тим, мора им се омогућити надлежност у сајбер простору у области националне безбедности.

Да би се то постигло, потребно је на међународном нивоу да се дефинишу заједничка терминологија и надлежности држава, њихових органа и појединаца, и да се одреде заједничке институције и стручна тела за усвајање стандарда у области сајбер ратовања. При томе, кључна питања су утврђивање државне одговорности и дефинисање нивоа на којем сајбер напад достиже ниво оружаног напада. Од тога зависе право нападнуте државе на самоодбрану и начин војног одговора. Досадашњи сукоби у сајбер простору су показали да су основни критеријуми за то оцена последица напада, природа напада и намера нападача. Пошто се намера тешко може доказати а сајбер напади се могу покретати прикривено, неопходно је да се усвоје нови принципи одговорности држава за активности у сајбер простору. По свему судећи, међународно право се мења у складу са праксом, а не добрим намерама и логиком, па је неопходно да се развију и властити одбрамбени, офанзивни и обавештајни капацитети ради одвраћања потенцијалних нападача. У складу са Амстердамским препорукама ОЕБС-а о слободи медија и интернету, то мора да се оствари ради спречавања недозвољених активности, а не због угрожавања људских права корисника сајбер простора. С обзиром на велики значај сајбер простора за човечанство, неопходни су иницијатива и учешће у међународној сарадњи у кризним ситуацијама које настају као последица сајбер ратовања, као и активно учешће у међународној изградњи правног система за сајбер ратовање ради забране употребе напада са одложеним деловањем и напади на критичну инфраструктуру и инсистирање на прихватању принципа одрицања права на први напад.

У наведеним околностима, стратегија Републике Србије би требало да се креће у два условно одвојена правца. Као активни члан међународне заједнице, потребно је да правовремено узмемо учешћа у међународној акцији регулисања сајбер ратовања. То би требало учинити са аспекта поштовања универзалних вредности, али и ради заштите властитих националних интереса. Из тог разлога, а у складу са својом позицијом у светском информационом простору у сајбер подручју, неопходно је да се активно настави са подржавањем става да је информационо ратовање усмерено против нација облик сајбер ратовања који треба забранити. Други специфични приступ том проблему огледа се у неопходној потреби да се што пре отпочне са изградњом властитих капацитета за сајбер ратовање. Они се морају развијати паралелно у свим правцима и не смеју да се ограниче на пасивну одбрану, јер

такав правац води у подређен положај у области сајбер сукоба. С обзиром на степен зависности српског друштва од активности у сајбер простору, приоритетне области развоја би требало да буду активна одбрана сувереног сајбер простора, развој обавештајних сајбер активности и капацитета за офанзивна сајбер дејства и информационо ратовање у сајбер простору. Једина ограничења у томе морала би да буду обавезе поштовања постојећих регулатива међународног права оружаних сукоба, људских права и националних интереса.

Литература

1. Faillere, N., O'Murchy, L., Chien, E.: W32.Stuxnet Dossier, Symantec Corporation, February 2011, www.symantec.
com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, (цитирано: 28. марта 2011).

2. US Senate. Witnesses - NOMINATIONS OF VADM JAMES A. WINNEFELD, JR., USN, TO BE ADMIRAL AND COMMANDER, U. S. NORTHERN COMMAND/COMMANDER, NORTH AMERICAN AEROSPACE DEFENSE COMMAND; AND LTG KEITH B. ALEXANDER, USA, TO BE GENERAL AND DIRECTOR, NATIONAL SECURITY AGENCY, United States Senate Armed Services Committee, 15 April 2010, http://armed-services. senate. gov/Transcripts/2010/04%20April/10–32%20-%204–15–10.pdf, (цитирано: 13. маја 2010).

3. International Strategy For Cyberspace, The White House, www.whitehouse. gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace. pdf, May 2011, (цитирано: 20. маја 2011).

4. Sommer, P., Brown, I.: Recuding Systemic Cybersecurity Risk, *OECD/IFP Project on „Fututre Global Shocks",* 4 January 2011,
www.oecd. org/dataoecd/57/44/46889922.pdf, (цитирано: 5. јануара 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, www.ewi. info/working-towards-rules-governing-cyber-conflict, (цитирано: 28. јануара 2011).

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

7. Wright, T.: America has double standards in fighting cyberwar, Financial Times, 26. June 2011, www.ft. com/intl/cms/s/0/c8002f6a-a01b-11e0-a115–00144feabdc0.html#axzz1QhkVEyll, (цитирано: 27. јуна 2011).

8. General Assembly, Developments in the Fileld of Information and telecommunications in the Context of International Security, report of the Secretary-Genaral, Addendum, A/56/164/Add. 1. 3 October 2001,

www.un. org/documents/ga/docs/56/a56164a1.pdf, [цитирано: 19. марта 2011].

9. Streltsov, A.: International information security: description and legal aspects, 2007, www.unidir. org/pdf/articles/pdf-art2642, (цитирано: 13. маја 2011).

10. Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949, www.icrc. org/ihl. nsf/FULL/380?OpenDocument, (цитирано: 12. децембра 2010).

11. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, www.icrc. org/ihl. nsf/FULL/470?OpenDocument, [цитирано: 12. децембра 2010].

12. Warden, J.: The Enemy as a System, *Airpower Journal,* Spring, 1995, T. VIV, No. 1, стр. 40–55.

13. Morozov, E.: *The Net Delusion: The Dark Side of Internet Freedom,* New York : PublicAffairs, 2011, ISBN 9871586488741.

14. Korotkov, S.: Ministry of Defence, Russian Federation, Legal Aspects of Informational Operations, Information & Communication Technologies and International Security, United Nations Institute for Disarmament esearch, Conference, 24–25 April 2008, Geneva, 24–25 April 2008, www.unidir. org/audio/2008/Information_Security/en. htm, (цитирано: 1. марта 2011).

15. Clinton, H.: Remarks on Internet Freedom, *U. S. Departmenet of State,* 21 January 2010, www.state. gov/secretary/rm/2010/01/135519.htm, [цитирано: 2. фебруар 2011].

16. 1389.IH, 112th Congress (2011–2012), H. R.1389 - Global Online Freedom Act of 2011, *The Library of Congress, Thomas,* 6 April 2011, http://thomas. loc. gov/cgi-bin/query/z? c112:H. R.1389, (цитирано: 12. априла 2011).

17. Kellz, S., Cook, S.: Freedom on the Net 2011, A global Assessment of Internet and digital media, Freedom House, 18 April 2011, www.freedomhouse. org/images/File/FotN/FOTN2011.pdf, (цитирано: 20. априла 2011).

18. Joyner, C., Lotrionte, C.: Information Warfare s International Coercion: Elements of Legal Framework, *European Journal of International Law, Volume 12, Number 5, 1 December 2001,* стр. 825–865.

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

20. 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.

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

22. Gady, F., S., Austin, G.: Russia, The United States, And Cyber Diplomacy, The EastWest Institute, 14 September 2010, www.ewi. info/russia-united-states-and-cyber-diplomacy-opening-doors, (цитирано: 16. јануара 2011).