УДК: 355.01:004

НЕУТРАЛНОСТ 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 ратовање се, по својој специфичној природи, знатно разликује од досадашњих облика ратовања. Она је одређена средствима, методама, техникама, војним доктринама и правилима. Могућност прикривања нападача и употреба истих средстава и метода, као и у случају сајбер криминала и обавештајних активности, чини његово међународноправно регулисање веома сложеним. Постојећа правила права оружаних сукоба могу се применити на сајбер ратовање у генералном аспекту, али услед немогућности утврђивања идентитета нападача и државне одговорности за напад тешко их је применити у пракси. Сајбер ратовање узрокује многе опасности по међународни мир, а једна од најважнијих је нарушавање неутралног статуса држава у току сукоба и његово ширење из сајбер на физичко подручје. Сајбер напади током оружаног сукоба између Русије и Грузије 2008. године нису достигли ниво оружаног сукоба, али су пружили могући модел будућих комплексних међудржавних сукоба са компонентом сајбер ратовања и њихов утицај на неутралност у току сукоба. За међународноправно регулисање неутралности држава у току сајбер сукоба неопходно је утврдити праву природу сајбер ратовања, извршити аналогију са постојећим правилима о неутралности и изнаћи нова и оригинална решења која одговарају природи сајбер ратовања.

Кључне речи: *сајбер ратовање, неутралност, сајбер безбедност, сајбер простор, кибернетичко ратовање, право оружаних сукоба.*

Увод

Сајбер ратовање је нови, све заступљенији облик међудржавног сукоба, који се због специфичних карактеристика битно разликује од досадашњих врста ратовања. Стручна и међународна јавност још увек није дефинисала сајбер ратовање. Оно се води истим средствима, методама и техникама као и сајбер криминал, обавештајне активности и тероризам, због чега се ови облици испољавања силе у сајбер простору често мешају. Иако се примењује ради вођења сукоба, сајбер ратовање више зависи од

технологије, природе информационих система, њихових мрежа и недостатака сајбер инфраструктуре, него од војне тактике. Сајбер сукоби остварују директно дејство на информације и информационе системе, а посредно дејство остварује на зависне системе, процесе, сервисе и људе. Посредне последице могу бити идентичне ефектима традиционалних кинетичких напада. Сајбер простор нема физичко одређење, али се његова физичка основа налази у материјалном свету који је подељен политичким границама и у надлежности је различитих државних суверенитета. По међународном праву ратовање представља предузимање оружане агресије између субјеката међународног права. У околностима када не постоји јасно нарушавање физичких граница и територије нападнуте стране, већ су очигледне само последице напада, при чему се најчешће не може доказати одговорност државних органа за напад, лако може настати конфузна ситуација са могућим озбиљним последицама по мир у свету. Природа сајбер простора и начин пакетног саобраћаја дигиталних информација у њему не омогућавају праћење напада у реалном времену. Овакве ситуације у комбинацији са оружаним акцијама у физичком свету лако могу довести до ширења сукоба на неутралне стране. До појаве сајбер ратовања ратни циљеви су постизани нарушавањем суверенитета и територијалног интегритета противничке стране у физичком простору. Његовом применом ратне циљеве је могуће постићи и без претходног физичког нарушавања територије противника. Сајбер простор протеже се целим светом, има физичку инфраструктуру у државном и приватном власништву, у деловима подлеже надлежности државних суверенитета, али се простире и у заједничким светским подручјима, унутар и изван државних граница. У току сајбер напада подаци физички не прелазе државне границе у сајбер простору, јер оне тамо не постоје, али се крећу од, ка и кроз физичке везе и уређаје који се протежу преко физичких граница преко копна, кроз море, свемир[1] или ваздух. Још увек није утврђено да ли се при томе крши суверенитет и неутрални статус транзитних држава.

Досадашњи сукоби у сајбер простору, а посебно сукоб између Русије и Грузије 2008. године, који се одвијао за време конвенционалног сукоба у физичком свету (на копну и у ваздуху), створили су нове дилеме о повреди неутралности у савременим ратовима. Током наведеног сукоба грађани руске националности[2] су на владине и поједине комерцијалне грузијске сервере усмерили масован *DDoS* напад[3] због чега је грузијска влада затражила техничку и стручну помоћ владе САД и дозволу да користи капацитете америчких компанија [1].[4] Без званичног одобрења, али уз незваничну сагласност савезничких држава, Грузија је преместила владине сајтове на сервере у САД, Естонији и Пољској.[5] Иако идентитет нападача и одговорност Русије нису доказани, нити је напад по интензитету и последицама достигао ниво оружаног напада, у јавности су се појавиле дилеме да ли је наведени сајбер напад имао природу агресије и да ли је дошло до повреде неутралности. Слу-

[1] Постоје планови за постављање сателита као Интернет чворишта у свемиру: http://www.space.com/businesstechnology/technology/interplanetary_internet.html, (08.05.2009).

[2] Shaun Waterman, "Georgia Hackers Strike Apart from Russian Military", *The Washington Times*, 19. август 2008, http://www.washingtontimes.com/news/2008/aug/19/georgia-hackers-strike-apart-from-russian-military, (28.05.2010).

[3] *Distributed Denial of Service Attack*

[4] У првом реду то су били *TSHost* и *Google*.

[5] Peter Svensson, "Georgian President's Web Site Moves to Atlanta," *AP News*, 11. август 2008, http://www.usatoday.com/tech/products/2008-08-11-2416394828_x.htm, (28.05.2010).

чај је компликованији, јер се и сукоб у физичком подручју десио без званичне објаве рата, а идентитет сајбер нападача није био познат. У сукобу су учествовале регуларне војне снаге обе државе и дошло је до великих материјалних разарања и људских жртава. У таквим околностима аутоматски се примењује међународно право оружаних сукоба, укључујући и начело неутралности. У случају да су земље које су пружиле помоћ Грузији прекршиле то начело, Русија је имала право да предузме пропорционалне и потребне нападе, чиме би се сукоб проширио.

Иако је сајбер сукоб у Грузији имао ограничен домет, ситуација у којој се десио представља вероватан модел будућег међународног сукоба са компонентом сајбер ратовања, па је стога важно извршити његову анализу. Питање неутралности држава у сајбер сукобима је сложено. Потребно је утврдити какве последице по неутралност суверене државе има сајбер напад који само пролази кроз њену инфраструктуру, а који је покренут из треће државе или истовремено из неколико других држава. Потребно је наћи одговор и на питање да ли је дозвољена војна акција нападнуте државе на информациону инфраструктуру неутралне државе са циљем да се онеспособе капацитети преко којих су преусмерени (рутирани) сајбер напади из земље нападача, а који су изазвали материјална разарања, људске жртве или политичке последице. Постоји дилема да ли постојеће хуманитарно право, у недостатку специфичних прописа, применом одговарајуће аналогије и општих правила може регулисати примену сајбер сукоба, који се могу одвијати током рата, у миру, помешани или маскирани са сајбер криминалом, тероризмом или шпијунажом.[6] Досадашња искуства и процене показују да највећи број сајбер напада вероватно има државно порекло, које је изузетно тешко доказати, а готово немогуће у реалном времену.[7] Ови и слични проблеми изискују јасно одређење природе принципа неутралности током сајбер ратовања. Неутралност представља једно од основних начела међународног права, а историја показује колико је његова природа крхка. Ипак, оно се не може једноставно занемарити и заборавити као принцип прошлости. Његова изворна сврха је спречавање ширења сукоба и за њом постоји потреба и у данашње време. Овај принцип мора се применити и на савремене облике ратовања у изворном или прилагођеном облику.

Појам и историјски развој неутралности

Неутралност је основно начело међународног права оружаних сукоба. Ово право је део међународног јавног права и уређује односе између држава у оружаном сукобу и поводом оружаног сукоба,[8] чиме ограничава ефекте сукоба и настоји да патње и

[6] Cordula Droege, No legal vacuum in cyber space, 16.08.2011, ICRC, http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, (20.08.2011).

[7] По изјави директора компаније McAfee Дејва ДеВелта, из јануара 2010. године, око 20 држава је интензивно развијало сајбер ратовање. У анкети у којој је учествовало преко 600 *IT* руководилаца широм света, 60% њих је сматрало да већина сајбер напада има државно порекло. Greg Austin, „China's Cybersecurity and pre-emptive cyber war", 14 march 2011, EastWest Institute, http://www.ewi.info/china's-cybersecurity-and-pre-emptive-cyber-war, (18.06.2011).

[8] Сукоби могу бити међународни и немеђународни. Први престављају борбу оружаних снага најмање две државе, сукобе са окупацијом дела или целе државе (чак и ако нема оружаног отпора окупацији)

разарања сведе на минималну меру. Право оружаних сукоба настало је спајањем специфичних одредби обичајног права, такозваног Женевског права (које штити оне који не учествују или су престали да учествују у сукобима) и Хашког права (које ограничава средства и методе ратовања). Оно представља нужан компромис између војне потребе и захтева хуманости, а његова примена не спречава војничку победу неке од страна, већ само захтева да се не наноси сувише патње и разарања. Оно се не бави питањем законитости или незаконитости рата и не прави разлику између нападача и браниоца. Уређено је Повељом Уједињених нација и подједнако обавезује све учеснике у оружаном сукобу. У основи, неутралност представља правни статус државе који се везује за политику неангажовања у току рата (сукоба). У најкраћим цртама, оно се може описати следећим суштинским правилима:

– територија неутралних држава мора се поштовати и не сме се користити за војне операције,

– трупе, ваздушна или морска пловила не смеју прелазити преко неутралне државе, нити се стране у сукобу могу снабдевати преко њене територије,

– неутрална држава има дужност да силом брани неутралност,

– неутрална држава не сме да учествује у ратним активностима страна у сукобу, али може дозволити транспорт рањеника, болесника и хуманитарне робе, деловати као сила заштитница и наставити привредне контакте са зарађеним странама, који су започели пре избијања сукоба и који нису у функцији његовог вођења,

– неутрална држава мора се односити једнако према зарађеним странама.

Поред класичне неутралности у сукобу, постоји и трајна неутралност.[9] Принцип неутралности је, попут осталих правила ратовања, настао ради регулисања сукоба током осамнаестог и деветнаестог века. Његова претеча је савез неутралних земаља из 1780. године који је основала руска царица Катарина Друга са циљем да окупи слабије поморске силе ради заштите бродова у току америчког рата за независност.

или ратове за национално ослобођење (у којима не морају учествовати две међународно признате државе). Немеђународни сукоби се воде између редовних оружаних снага и засебних наоружаних група или између наоружаних група које се боре међусобно у току којих размере борбе достижу одређени ниво и интензитет, у току одређеног периода. Код унутрашњих насиља, затегнутости, побуна, изолованих и спорадичних аката насиља и сличних аката којима се озбиљно нарушава унутрашњи поредак, нема примене међународног хуманитарног права, јер нема ни признатог оружаног сукоба.

[9] Трајна неутралност је међународноправно стање државе која се обавезала да у сваком рату буде неутрална, а друге државе су се обавезале према њој да ће поштовати прокламовану неутралност. Она се темељи на међународним уговорима, па није довољна једнострана изјава или најава влада држава да ће водити неутралну политику. Изузетак је трајна неутралност Швајцарске, која је добила статус трајно неутралне земље на Бечком конгресу 1815. године, која је призната и Версајским мировним споразумом из 1919. године, па њена неутралност важи за све државе потписнице. Организација за европску безбедност и сарадњу (ОЕБС) у својим закључцима је потврдила да је право на неутралност део начела суверене једнакости држава. Трајно неутрална држава има обавезу да брани властиту неутралност, па има право да држи стајаћу војску и војне базе. Може бити чланица УН, али и не мора. Нема право да прихвата међународне обавезе које би је могле увући у рат, нити сме склапати војне савезе, помагати трећим државама и преузимати гаранције за њихову неутралност. Пракса показује да трајно неутралне државе ипак улазе у регионалне организације Европе, попут ЕФТА споразума или Савета Европе. Аустрија је чланица Европске уније од 1995. године. Проширење надлежности ових наддржавних организује на спољнополитичка и питања безбедности отвара конфликт принципа неутралности и припадности тим организацијама.

И прве јасне формулације доктрине неутралности потичу из овог периода и могу се наћи у два америчка документа: Прокламацији неутралности из 1793. године и Закону о неутралности из 1794. године. Извори савременог правног регулисања неутралности су Париска декларација из 1856. године (регулише односе поморске неутралности током рата), V Хашка конвенција (Права и дужности неутралних држава и лица у случају рата на копну),[10] XIII Хашка конвенција из 1907. године (Права и дужности неутралних држава у поморском рату),[11] Лондонска декларација из 1909. године (Декларација о правилима поморског ратовања, која није била ратификована),[12] четири Женевске конвенције из 1949. године[13] и I Допунски протокол из 1977. године.[14]

Повеља УН и одлуке Савета безбедности могу у одређеним околностима модификовати право о неутралности, дефинисано претходним споразумима. На пример, Повеља УН захтева од држава чланица да пруже УН сваку помоћ у акцијама које предузима,[15] као и да прихвате одлуке Савета безбедности и повинују им се.[16] Мере присиле наведене у Глави VII Повеље УН такође могу имати утицаја на неутралност, јер се њихова правила разликују од правила неутралности која су настала пре Повеље.

Развој правила о неутралности текао је на тежак и сложен начин. На њега су утицале историјско-политичке околности. На пример, правила неутралности су детаљно развијана у области поморских односа у време када је поморски саобраћај био доминантан начин трговине у време супротстављених интереса многих трговачких сила који су доводили до конфликата. Сложеност права и обавеза неутралности зависи од интензитета активности и подручја. На пример, на отвореном мору, ван сопствене територије, држава учесница оружаног сукоба има право да заустави и претражи пловило неутралне државе и да га заузме, уколико нађе доказ да оно непријатељској страни превози недозвољену робу или да крши поморску блокаду. У том случају, једино недозвољена роба може бити заплењена (оружје и ратни материјал намењен држави у сукобу). Међутим, ако се више од пола товара на том пловилу (било по запремини, вредности или тежини) састоји од недозвољене робе пловило може бити заплењено. Таква квалификација и заплена морају се поткрепити пресудом надлежног суда, а уколико се оптужбе не потврде, мора се надокнадити штета власнику за одузету робу и брод. Током времена зарађене стране се често нису слагале око интерпретације ових компликованих правила. На пример, током Првог и Другог светског рата Велика Британија је готово све врсте робе дефинисала недозвољеном и успоставила право да пресреће бродове неутралних држава и да их спроводи у властите луке због претреса у сваком сумњивом случају. Пошто Немачка није била у стању да

[10] http://www.icrc.org/ihl.nsf/FULL/200?OpenDocument, (13.08.2009).

[11] http://www.icrc.org/ihl.nsf/FULL/240?OpenDocument, (13.08.2009).

[12] http://www1.umn.edu/humanrts/instree/1909b.htm , (13.08.2009).

[13] О унапређењу положаја рањеника и оболелих на ратишту (I), рањеника, оболелих и бораца са потопљених бродова на мору (II), третирању ратних заробљеника (III) и о заштити цивила у време рата (III), http://www.icrc.org/ihl.nsf/TOPICS?OpenView, (13.08.2009).

[14] http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079, (13.08.2009); John W. Coogan, *The End of Neutrality: The United States, Britain, and Maritime Rights, 1899-1915*, Cornell University Press, Ithaca, New York, 1981.

[15] Повеља УН, члан 2 (5).

[16] Повеља УН, члан 25.

парира британској морнарици у пресретању бродова, одговорила је подморничким ратовањем, потапајући непријатељска и сумњива неутрална пловила на лицу места. Као неутрална држава током раних фаза оба светска рата, САД су се противиле оваквој пракси и због потапања бродова који су превозили америчке путнике ступиле су у Први светски рат, а под сличним околностима су ушли и у рат са Немачком током Другог светског рата. Наведено показује колико је велики значај имала неутралност у том периоду. Међутим, током два светска рата десио се готово потпун слом неутралности. Овај период карактерисала је економска међузависност држава и промењена природа ратовања. Ратовање је постало механизовано и захтевало је огромне количине средстава, опреме и материјала, а способност масовне производње имала је суштински значај за победу у рату. Привредни ресурси постали су подједнако важне мете као и војне, а готово цео свет је постао ратиште. Трговина са неутралним државама у току рата постала је веома важна. Зараћене стране су одлучно настојале да заштите властите токове снабдевања и истовремено се трудиле да прекину противничке. Овакве околности су значајно повећале вероватноћу повреде неутралности током сукоба. У периоду између два светска рата, алтернативе постојећим прописима о неутралности били су споразум у оквиру Уговора Лиге народа и Келог-Брајандов Пакт из 1928. године.[17] Ове идеје су поново оживљене након Другог светског рат у Повељи УН. Са развојем атомског оружја, неутралност у било каквом облику постаје све мање практично применљива. Ипак, равнотежа нуклеарних претњи и њихови трошкови током хладног рата одвратили су обе суперсиле од њихове употребе и натерали их да нађу минималан заједнички став о потреби ограничавања нуклеарног оружја. Ова равнотежа између блокова довела је до ситуације да је поштована гарантована неутралност појединих држава (Швајцарске, Аустрије, Финске и других).

Права и обавезе држава у области неутралности

Неутралан статус државе доноси посебна права и дужности. Она има право да се издвоји из сукоба, а међународно право јој гарантује неповредивост територије и ваздушног простора од страна у сукобу. Неутралне државе имају обавезу неучествовања и непристрасности током сукоба, забрану формирања борбених јединица за подршку било којој од страна у сукобу и обавезу превенције и санкционисања повреде наведених права.[18] Сложена и често компликована правила о неутралности суштински су заснована на различитим принципима, правима и обавезама.

Међународним актима[19] дефинишу се категорије **неутралног простора** и **неутралних лица**. Неутрални простор обухвата копнену територију неутралне државе, њене територијалне воде и ваздушни простор. Неутрална држава мора предузети мере да обезбеди и оствари заштиту властите неутралности у подручју за који је од-

[17] http://www.yale.edu/lawweb/avalon/imt/kbpact.htm, (18.09.2009).

[18] V Хашка конвенција (Права и дужности неутралних држава и лица у случају рата на копну), чланови 1-5. http://www.icrc.org/ihl.nsf/FULL/200?OpenDocument, (13.08.2009)

[19] Исто, чланови 16. и 17; I Допунски протокол Женевској конвенцији (Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), члан 47.

говорна у односу према зараћеним странама, а нарочито према њиховим оружаним снагама. Државе не морају дати званичну изјаву о неутралности, нити њихов статус морају званично признати друге државе. Такве званичне декларације о неутралности могу имати само ефекат бољег упознавања јавности о неутралном статусу државе.

Неутрална лица су држављани неутралне државе. Они губе свој статус уколико почине акт непријатељства према оружаним снагама зараћене стране или се придруже некој страни у сукобу. Тада они добијају статус бораца у сукобу и могу имати статус ратних заробљеника уколико буду заробљени. Међутим, ако постану плаћеници, немају право на статус бораца или ратних заробљеника.[20] Односи зараћених држава са приватним лицима, грађанима неутралне државе, сложенији су од односа између држава. Неутралне државе не смеју штитити своје грађане од санкција уколико су починили дела која су супротна обавезама о неутралности. Међутим, нису обавезне да спрече своје грађане да продају ратна добра или пружају финансијску помоћ некој зараћеној страни уколико имају законска права на то. Са друге стране, странама у сукобу није забрањено да покушају да спрече такав вид трговине између неутралне државе и својих непријатеља. За све време док њихова држава одржава нормалне дипломатске односе са зараћеном државом у којој живе или је посећују, неутрална лица остају под дипломатском заштитом и морају се третирати на исти начин као и у време мира. Ако такви дипломатски односи не постоје, неутрална лица имају право на третман лица која су заштићена IV Женевском конвенцијом.[21] Њихов статус је исти, без обзира на то да ли су цивили или припадници оружаних снага неутралне државе којој припадају. Неутрална држава, пошто није ни учесник, нити арбитар у сукобу, мора показати непристрасност према свим зараћеним странама, а зараћене стране морају поштовати њен суверенитет. Ипак, у неким случајевима постоје изузеци, јер страна у сукобу има право да сама организује потеру и нападне непријатељске снаге на територији неутралне земље, уколико то она не може или неће да учини, али само у случају уколико претходно дође до повреде неутралности.

Стране у сукобу имају бројне дужности по питању поштовања неутралности држава које не учествују у сукобу. Оне морају издати јасна упутства и наређења властитим оружаним снагама које дејствују у близини неутралног простора да избегавају кршења прописа, као што је пролазак кроз неутрални простор, формирање јединица или регрутовање бораца на неутралној територији, подизање инсталација за телекомуникације у војне сврхе на неутралној територији и коришћење таквих инсталација подигнутих пре оружаног сукоба.[22]

Дужности имају и неутралне државе. Оне морају спроводити политику неутралности и обезбедити поштовање свог неутралног статуса, чак и уз употребу силе, која се у том случају не сматра актом насиља, уколико се поштују општа ограничења ратног права.[23] Уколико то не учине, оне нарушавају начело неутралности, па могу изгубити одређена права или чак неутралност у целости. Неутрална држава мора спречити повреду власти-

[20] Исто.

[21] IV Женевска конвенција (Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949), члан 4, http://www.icrc.org/ihl.nsf/FULL/380?OpenDocument, (16.06.2009).

[22] V Хашка конвенција, чланови 2-4.

[23] V Хашка конвенција, чланови 5. и 10.

те територије од страна у сукобу издавањем јасних упутства и упозорења оружаним снагама које дејствују у близини њеног простора, али и применом силе уколико се оне оглуше о упозорења. Уколико нека страна учини ненамерну грешку, има обавезу да је што пре призна и тиме спречи прерастање инцидента у сукоб. Обавезе неутралности се делимично разликују у односу на околности и подручје примене. На пример, пловилу зараћене стране које није у ратној функцији може се дати дозвола за пролазак кроз територијалне воде, али је обавеза спречавања проласка њених војних снага копном и у ваздушном простору апсолутна. Ова околност је важна за примену у току сајбер ратовања.

Комерцијални односи и неутралност. Комерцијални односи у неутралности су релативни и зависе од више околности. Неутрална држава не сме помагати странама у сукобу, а нарочито их не сме снабдевати ратним средствима и материјалом.[24] Непристрасност неутралне државе према зараћеним странама не значи обавезу идентичног односа у свему, већ само забрањује различито поступање у односу на ратне активности: „Неутрална држава нема обавезу да у име једне или друге стране у сукобу спречи извоз или транспорт оружја, муниције или уопште било чега што би могло бити у користи некој војсци".[25] Она није обавезна да елиминише разлике у комерцијалним односима са обе стране у сукобу у време његовог избијања, али унапређење тих односа са неком од страна по започињању сукоба може бити у супротности са неутралним статусом.

Телекомуникације и неутралност. Односи у области телекомуникација веома су важни у погледу примене на сајбер ратовање. Правила о неутралности не обавезују неутралну државу да спречи употребу властитих телекомуникационих капацитета некој страни у сукобу која их је користила или им је имала приступ пре избијања сукоба. Она може ставити на располагање властите телекомуникационе капацитете странама у сукобу, које могу изнајмљивати фиксне линије за комуникацију гласом и комуникацију података војне природе, или чак сателитске везе. То представља повреду неутралности само уколико стране у сукобу нису имале приступ овим капацитетима пре избијања сукоба, а користе их ради вођења сукоба, у случају подизања нових телекомуникационих инсталација или нове употребе постојећих инсталација ради вођења сукоба.[26] Ово правило не односи се искључиво на војне комуникационе системе, већ и на изградњу нових сервиса који служе вођењу сукоба или допуштање зараћеној страни да их изграде властитим капацитетима.[27] По аналогији, војна употреба неког интернет сервиса, попут сервиса за социјално умрежавање, *VoIP* телефонских сервиса,[28] сервиса за глобално позиционирање или сличних сервиса ради сајбер напада једне стране на другу (без обзира на то да ли та дејства остварују кинетичке или друштвено-политичке последице) предста-

[24] XIII Хашка конвенција (Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War. The Hague, 18 October 1907), члан 6, http://www.icrc.org/ihl.nsf/INTRO/240?OpenDocument, (02.09.2010). Раздвајање државне и приватне индустрије оружја у савременом добу не одражава политичку реалност. Савремено међународно право сматра да држава поступа супротно неутралности ако дозвољава снабдевање било каквим ратним материјалом. Обилна финансијска подршка страни у сукобу, снабдевање нафтом или другим енергентима, такође се сматра понашањем које није неутрално.

[25] V Хашка конвенција, члан 7.

[26] V Хашка конвенција, чланови 2-4.

[27] V Хашка конвенција, чланови 8. и 9.

[28] *Voice Over Internet Protocol*.

вљају повреду неутралности, па угрожена страна има право пропорционалног војног одговора. Наредни услов у том случају је одређивање природе сајбер напада (да ли се може сматрати актом оружане агресије или не). Стране у сукобу немају право да подижу станице бежичне телеграфије или друге објекте на територији неутралне државе ради комуникације са властитим снагама на копну или мору[29] ради вођења сукоба, као ни да их у ту сврху користе уколико су их поставили на територији неутралне државе пре избијања сукоба и уколико нису отворени за јавну употребу (по аналогији, у истим околностима не могу користити ни сервисе у сајбер простору у надлежности неутралне државе). Битно је нагласити да се неутралним државама не намеће дужност да забране зарађеним странама употребу комуникационих система у приватном власништву, али се захтева непристрасност према свим странама у сукобу (неутрална држава не може селективно одобрити или забранити права комуникације зарађеним странама и притом остати неутрална).

Нарушавање суверенитета неутралне државе сајбер ратовањем

Појава сајбер ратовања отвара нова питања у међудржавним односима током сукоба. Док је у традиционалном ратовању потребно нарушити територијални интегритет нападнуте државе за постизање ратног циља, у сајбер ратовању то није неопходно. Оно захтева брижљиво планирање војних операција, али нуди и велику слободу у случају његове злоупотребе. Узрок томе је његова комплексност у погледу надлежности, власништва инфраструктуре, учесника и природе комуникација. Још увек није постигнута сагласност око става да ли то представља повреду суверенитета држава у чијој инфраструктури се то дешава и да ли је само питање релевантно с обзиром на брзину тока информација. Могући приступ овом проблему је стварање аналогије између сајбер ратовања постојећих прописа за специфична подручја ратовања. Пошто нарушавање суверених граница неке државе у ваздушном простору, на копну или мору угрожава њену националну безбедност, територијални интегритет и политичку независност, а с обзиром на то да се физичка инфраструктура сајбер простора налази у овим подручјима, таква аналогија је могућа. Има и супротних ставова, јер многи стручњаци сматрају да се сајбер простор не може у потпуности сматрати елементом националног суверенитета, упркос настојањима држава да остваре и прошире властити суверенитет и у њему.[30] Трећа група стручњака заговара тезу примене принципа „безбедносног суверенитета“ [2, стр. 80],[31] који има за циљ одвраћање од напада, јер омогућава право легитимног превентивног одговора на претњу, што потенцијално може имати опасне последице због злоупотребе.

[29] V Хашка конвенција, чланови 3. i 5.

[30] Michael A. Sinks, *Cyber Warfare and International Law*, Air Command and Staff College, Air University, Maxwell AFB, Alabama, 2008, стр. 18.

[31] Безбедносни принцип суверенитета неке државе дефинише се као „принцип надлежности у коме нације могу узети за право да казне страну државу за одређено понашање ван своје територије, које је усмерено против њихове безбедности, територијалног интегритета и политичке независности”.

Међународно право налаже чланицама УН да се суздрже од претњи и употребе силе против територијалног интегритета и политичке независности било које чланице или на било који начин противречан Повељи и одлукама Уједињених нација. Оно забрањује сваку врсту примене силе, осим у случају самоодбране или ради санкција које су предузете по одлуци Савета безбедности.[32] Али, појам „употреба силе“ се не схвата у свакој прилици на исти начин, а те несугласице нису почеле са сајбер ратовањем. Слична ситуација дешавала се и у случају примене хемијског и биолошког оружја. Њихова примена не представља употребу кинетичке силе и има потенцијал неочекиване примене уз фактор изненађења. Ове недоумице су делимично решене применом критеријума оцене последица напада, а не врсте примењеног средства.[33] Поједини стручњаци сматрају да се и оцена природе сајбер напада може извршити по истом критеријуму [3, стр. 79–81]. Такав став заузима и војна доктрина САД за сајбер операције.[34] У том случају није важно да ли је напад предузет копном, морем, ваздухом, свемиром или у сајбер простору, већ какав је ефекат изазвао. Људске жртве и материјална разарања изазвана сајбер нападом довољан су разлог за самоодбрану. Поједини аутори поричу да је остваривање тог права веома проблематично у погледу избора адекватне врсте одговора (традиционалног или нуклеарног напада) [4 стр. 22], [5]. Међутим, нема свака држава сајбер капацитете за пропорционалан акт самоодбране, исти ниво информационе заштите, нити се примена истог рачунарског вируса може сматрати пропорционалним начином самоодбране.[35] Са друге стране, одсуство ограничења сајбер ратовања може имати далекосежне последице. На пример, поједини руски војни стручњаци сматрају да Русија има право широког спектра војних одговора на сајбер напад, укључујући и нуклеарни противнапад,[36] а САД задржавају право да на напад одговоре свим расположивим средствима.

Повреда неутралности сајбер нападом зависи од његових последица. Изоловани сајбер напад без значајних последица тешко се може сматрати довољним поводом за примену права на самоодбрану.[37] Пример за ову тврдњу су случајеви сајбер напада у Естонији (2007) и Грузији (2008). Чак и да је било могуће утврдити одговорност Русије за покретање поменутих сајбер напада, њихове последице нису биле довољне за позивање на право на самоодбрану и предузимање противнапада оружаном силом.

Хашке конвенције из 1899. године[38] дале су подстицај за даљи развој међународног ратног права. Оне садрже Мартенсове клаузуле,[39] које представљају основу за приме-

[32] Члан 2. Повеље УН; 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, страна 69.

[33] Исто, страна 72.

[34] Siobhan Gorman, Julian E. Barnes, „Cyber Combat: Act of War“, The Wall Street journal, 31 May 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html, (02.06.2011).

[35] Већина напада малициозним кодом може истински бити ефикасна само први пут, док се не његовом употребом не открије и затим исправи грешка чије постојање је искоришћено.

[36] Hildreth, S.A., *Congressional Reasearch Service Report For Congress,* No. RL30735, Cyberwarfare, 2001, http://www.fas.org/irp/crs/RL30735.pdf.

[37] Barkham, стр. 81.

[38] Конвенције I-IV и Декларације I-III, http://avalon.law.yale.edu/subject_menus/lawwar.asp, (18.06.2009).

[39] Преамбуле II Хашке конвенције о праву и обичајима рата на копну из 1899. године, руског делегата, професора Фјодора Фјодоровича Мартенса, http://www.icrc.org/web/eng/siteeng0.nsf/html/57JNHY, (18.01.2009).

ну хуманитарних принципа при употреби нових технологија ратовања и универзално су примењиве у будућности. Међународна заједница их је прихватила и уградила у постојеће право са циљем да спречи будућа непотребна и непропорционална разарања применом нових средстава наоружања која још нису уведена у употребу.[40] Ове одредбе дају став о правном регулисању злочина применом принципа хуманости ценећи њихове последице, а не методе и средства. Овакав систем подразумева поштовање суверенитета држава, али предвиђа њихову одговорност за настале последице у подручју одговорности властитог суверенитета. Валтер Шарп, уредник издања *УН Мировне операције*, тврди да сајбер напади представљају активности које нису у складу са постојећим међународним правом. Он сматра да се сајбер напад или нека друга неконвенционална употреба силе може сматрати оружаним нападом онда када остварује ефекте традиционалног оружаног напада. Такође, тврди да коначне дефиниције појмова „оружани напад", „акт самоодбране" и „агресија" можда никада неће бити прецизиране [6, стр. 138]. Ипак, примена наведеног принципа може пружити само основе за будуће регулисање. Претње сајбер ратовања су сложене, а његова природа се брзо мења. Примена принципа оцене последица напада није једноставна у свим случајевима сајбер операција, попут информационих операција [7]. Део држава окупљених у Шангајску организацију за сарадњу,[41] а пре свих Русија,[42] сматра да и информационе операције у сајбер простору представљају облик агресије. Русија је Уједињеним нацијама предложила забрану употребе информационих операција.[43] Поред тога, приступ оцене последице напада не предвиђа околности у којима постоји јасна намера нападача да сајбер нападом изазове озбиљне последице по нападнуту страну, укључујући материјална уништења или људске жртве, али у којима напад није ефикасан. Са технолошким развојем сајбер ратовања и зависношћу окружења од информационих технологија, могућност изазивања физичког уништења циља је све извеснија. И природа сајбер нападача се мења. Први нападачи су, углавном, били индивидуални хакери, који су предузимали нападе због забаве и личних разлога. Врло брзо су криминалци постали главни извор сајбер напада, који су постали много софистицираније и опасније. У актуелном времену државе су одговорне за све већи проценат сајбер напада којим остварују политичке циљеве. У складу са измењеном природом технологије и врстом нападача последице сајбер напада биће све озбиљније. Пример за то су сајбер напад рачунарским црвом *Stuxnet* на иранско нуклеарно постројење Бушер и информационе операције у сајбер простору којима се иницирају друштвени ломови. Право оружаних сукоба забрањује нападе на „...постројења која у себи садрже опасне силе, попут брана, насипа или електричних централа", која „...не смеју бити циљ напада, чак и када су такви објекти војни циљеви, уколико такав напад може изазвати ослобађање опасних сила и изазвати озбиљне по-

[40] Sinks, стр. 22.

[41] Agreement Between the Governments of the Member States of the Shangai Cooperation Organization on Cooperation in the Field of International Information Security,

http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf, (12.03.2011).

[42] Sergei Korotkov, Legal Aspects of Information, Ministry of Defense, Russian Federation, Information & Communication Technologies and International Security, United Nations Institute for Disarmament esearch, Conference, 24-25 April 2008, Geneva, http://www.unidir.org/audio/2008/Information_Security/08-Korotkov.m3u, (28.02.2010).

[43] Sinks, стр. 19.

следице међу цивилним становништвом".[44] Ова забрана односи се и на војне циљеве у близини наведених објеката уколико напади на њих могу довести до ослобађања опасних сила или изазвати цивилне жртве.[45] Стога сајбер напади у организацији државе представљају ратне злочине. Чак и уколико буду неуспешни, овакве нападе међународна заједница мора да санкционише. Принцип последице није довољан за ваљано регулисање сајбер ратовања, већ се паралелно с њим мора ценити и намера нападача. Средства, методе и технике сајбер напада не могу бити мерило легалности напада, пошто их могу примењивати и недржавни субјекти у намери да почине криминална дела. Она говоре само о природи напада, односно о томе да ли је реч о конвенционалном или сајбер нападу. Мерило за процену природе сајбер напада мора бити обједињена процена природе, последица напада и намере нападача, за све сврхе, укључујући и процену начела неутралности. Имајући у виду начин употребе сајбер капацитета, постоје три основна случаја у којима сајбер напад утиче на неутралност неке државе:

– сајбер напад на неутралну државу или од стране неутралне државе,

– злоупотреба сајбер капацитета неутралне државе за напад стране у сукобу и

– употреба рачунара или комуникационог система неутралне државе као канала за сајбер напад.

Важно је нагласити да се сајбер ратовање не води искључиво над информацијама и информационим системима, нити се у потпуности води у сајбер простору. Оно је активност са веома широким подручјем деловања, усмерено на целокупну сајбер инфраструктуру коју начелно чине људи, процеси и системи који граде сајбер простор [8, стр. 21]. Прецизније, сајбер инфраструктуру сачињава окружење (објекти, средства, физичка инфраструктура, простор на копну, мору, ваздуху и свемиру у коме се налазе та инфраструктура и средства), енергија која омогућава рад информационих система и постројења, хардвер (процесори, рачунари и њихови склопови, оптичке и друге вазе и слично), софтвер (машински, кориснички, слоја везе, електронске базе података и слично), мреже (мрежни уређаји, комуникације, топологије и слично), садржај (информације и датотеке које се чувају и крећу у системима и мрежама, мрежни и аутоматски генерисани статистички подаци и слично), људи (програмери, администратори, оператери, особље за одржавање, корисници) и регулативе (прописи, споразуми, стандарди и друго) [9, стр. 1–4].

Сајбер напад на неутралну државу или од стране неутралне државе

Све стране у сукобу имају обавезу да се уздрже од сајбер напада на неутралну државу, све док она поштује обавезе које проистичу из њеног статуса. И неутрална држава има обавезу да се уздржи од сајбер напада на стране у сукобу. У супротном, губи неутрални статус. Да би га сачувала, поред поштовања, мора и активно да га брани, чак и применом силе.[46]

[44] Допунски протокол I, члан 56 (1). Ова забрана престаје да важи када се ти објекти и објекти у њиховој непосредној околини користе различито од своје нормалне употребе ради редовне, значајне и директне подршке војним операцијама и уколико је војни напад једини начин да се оконча таква подршка.

[45] Допунски протокол I, члан 56 (1). Овај протокол није ратификовало само неколико држава у свету: Иран, Мароко, Пакистан, Филипини и САД.

[46] V Хашка конвенција, члан 10.

Злоупотреба сајбер инфраструктуре неутралне државе

Иако сајбер простор „не припада“ територији државе, оне остварују јурисдикцију у његовим деловима и задржавају право и дужност да регулишу употребу информационих капацитета на властитој територији, као и активности у сајбер простору под својом контролом. Постоје разне могућности злоупотребе ових капацитета од стране друге државе за вођење сајбер ратовања против треће стране. Угрожена страна има право на самоодбрану и предузимање противнапада, јер сваки извор напада постаје легитимна мета за страну која се брани, под условом да неутрална држава није у стању или нема намеру да заустави акте агресије. У таквим ситуацијама неутралност је вишеструко угрожена. Оваква злоупотреба капацитета неутралне државе представља ратну перфидност која је ратни злочин. Процена да ли је повређена неутралност зависи од утврђивања идентитета нападача (што је изузетно сложено и често немогуће), тежине и последица напада. Поштовање процедуре прописане правилима о неутралности старим један век није практично у условима сајбер ратовања, у којем се напади готово тренутно дешавају, па је једини начин спречавања оваквих ситуација њихова превенција међународним прописима.

Употреба капацитета неутралне државе као канала за сајбер напад

Средства сајбер напада су рачунари, рачунарски системи и инфраструктура, програми и дигиталне информације које се налазе у тим системима или се крећу сајбер простором. Хардвер, физичке везе и дигиталне апликације и информације нису сами по себи оружје, јер имају и мирнодопску примену, али у складу са намером нападача могу бити средство напада и, у том случају, постају легитимне мете противнапада. Када злонамерни програм којим се врши сајбер напад путује ка циљу кроз информационе мреже које су у надлежности суверенитета неутралне државе, строга и буквална примена принципа неутралности подразумевала би да је нарушена њена неутралност. Међутим, технологија функционисања сајбер простора није погодна за такве тврдње. Буквална примена прописа о неутралности може бити опасна због правних и техничких разлога. Неутрална држава не мора бити ни свесна да је кроз њену инфраструктуру усмерен сајбер напад, а посебно не у реалном времену, па стога њени системи не смеју постати легитимни циљеви напада нападнуте државе. Правни разлози односне се првенствено на квалификацију природе сајбер напада и утврђивање да ли се он може изједначити са оружаном агресијом у складу са њеном дефиницијом, резолуцијом Генералне скупштине УН 3314,[47] Резолуцијом Генералне скупштине УН број 2625[48] и другим одговарајућим

[47] Ради појашњења нејасноћа у вези схватања појма „агресија” Генерална скупштина УН га је 1974. године дефинисала као „употребу оружане силе од стране државе против суверенитета, територијалног интегритета или политичке независности друге државе или на начин супротан са Повељом Уједињених нација”. Резолуција генералне скупштине УН број 3314, члан 1, 14. децембар 1974, Definition of Aggression, United Nations General Assembly Resolution 3314, (XXIX),

актима, попут Бечке конвенције о праву међународних уговора,[49] која је поставила императивне смернице међународним телима приликом интерпретације споразума у складу са међународним правом. Друга група правних проблема односи се на сукоб надлежности националних и међународних правних прописа и, уопште, на надлежност државног суверенитета у сајбер простору. Делови физичке информационе инфраструктуре (оптичких каблови, рутери, сателити и друго) који су у приватном или државном власништву налазе се у подручјима заједничке баштине човечанства (морско дно или свемир). Поједине државе усвојиле су прописе и процедуре за заштиту националне сајбер инфраструктуре у случају опасности (одлука Конгреса САД да председник САД има право да „искључи" целокупан интернет у националној надлежности у случају опасности[50]) или су то већ учиниле у тренуцима унутрашњих немира (поступак Египта током револуционарних протеста 2011. године[51]). Државе могу манипулисати радом рутера националних провајдера, посебно са функцијом *Border Gateway Protocol*-а.[52] Сајбер простор представља умреженост свих мрежа, па се поремећаји рада у једном делу лако преносу на цео систем.

Технички проблеми утврђивања порекла напада односе се на начин функционисања информационих мрежа. Пут информације кроз сајбер простор није могуће прецизно предвидети. Када један сервер постане преоптерећен, саобраћај се аутоматски преусмерава на суседни, који је слободан. Подаци су подељени на појединачне пакете који могу путовати различитим, аутоматски генерисаним путањама до одредишта на којем се поново састављају у првобитну целину. Те путање не могу сигурно знати у потпуности ни пошиљаоци, ни транзитне државе, ни државе одред-

---

http://untreaty.un.org/cod/avl/ha/da/da.html, (20.05.2010)

Члан 3. ове резолуције наводи седам чинова који се сматрају агресијом. Члан 4. каже да агресија није ограничена само тиме.

[48] Дефинише ратну агресију као злочин против мира и опомиње државе чланице 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". 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. године,

http://www.yudikorsou.com/download/UN%20GENERAL%20ASSEMBLY%20RESOLUTION%202625.doc, (20.05.2010)

[49] „Уговор се мора добронамерно тумачити према уобичајеном смислу који се мора дати изразима у уговору у њиховом контексту и у светлу његовог предмета и циља". Члан 31, став 1, Vienna Convention on the Law of Treaties, 1969. године (ступила на снагу 1980. године). Конвенција нема обавезујући карактер. http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf, (20.05.2010).

[50] The Protecting Cyberspace as a National Asset Act,

http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=42926cbe-76fd-4eeb-a08b-d7838a4aae8f, (15.06.2010).

[51] Iijitsch van Bejinum, „Haw Egypt did (and your government could) shut down the Internet", Ars Technica, http://arstechnica.com/tech-policy/news/2011/01/how-egypt-or-how-your-government-could-shut-down-the-internet.ars, (17.06.2011).

[52] Кина је оптужена да је преко властитих рутера на крађи период преусмерила комплетан интернет саобраћај америчког Сената, канцеларије секретара одбране, агенције НАСА, министарства трговине САД и неколико америчких берзи. 2010 Report to Congress of the U.S.-China Econimic And Security Review Commision, November 2010,

http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf, (26.11.2010).

нице. Једини поуздан начин прекида, али и превенције напада који може предузети неутрална држава јесте пресецање комплетног тока комуникација. Наметање овакве обавезе неутралним државама било би неразумно, јер би такав захтев у потпуности зауставио функционисање интернета (или другог облика електронских комуникација). Иако је форензички могуће утврдити *Internet Protocol (IP)* адресу порекла напада, нападе због преусмеравања није могуће пратити до извора у реалном времену. Уколико се и утврди локација (*IP* адреса уређаја са кога је упућен напад) или чак уређај са кога је напад потекао (његова MAC адреса), то не значи да је доказана и одговорност лица, а посебно не државе за покренути напад. Некада су за форензичко утврђивање нападача потребни месеци истраживачког рада, потпуна сарадња између држава, укључујући и оних које су можда одговорне за напад. Закаснеле информације о нападачу могу бити ирелевантне, уколико је напад већ окончан, а сукоб неповратно ескалирао.

Упркос наведеним проблемима, прописи о неутралности у сајбер ратовању морају имати моћ да заштите суштину овог принципа, да обавежу све стране да га поштују и да буду усклађени са суштином сајбер простора. Технички предуслов за то је поуздана идентификација лица и садржаја у сајбер простору, попут дубинске инспекције појединачних пакета података, поступака утврђивања генетског отиска сваког садржаја и једнозначне идентификације лица без обзира на уређај и платформу приступа сајбер простору.[53] Савремени трендови корпоративног света крећу се ка обавезној идентификацији корисника.[54] Ипак, и даље постоје начини да се злоупотреби туђи идентитет или да се заобиђе обавеза идентификације. У судској пракси САД постоје одлуке да се *Internet Protocol* (IP) адреса неког уређаја не може поистоветити са њеним регистрованим корисником.[55] Због техничке немогућности утврђивања одговорности на нивоу појединца, једино могуће начело заштите неутралности у сајбер ратовању представља захтевање обавезе његовог очувања, било прописивањем државне одговорности за сваки напад из подручја њеног суверенитета и (или) потпуне забране сајбер ратовања. Злоупотреба капацитета неутралне државе морала би представљати противзаконито дело. Рачунарски системи и информационе комуникације неутралних држава не би смели бити циљеви напада (без обзира на то да ли се ради о традиционалном или сајбер нападу), чак и у случају да се користе као средства преноса напада, осим у случају да неутрална држава изгуби свој неутрални статус. Утврђена повреда неутралности неке државе требало би да представља довољан разлог за прекид интернет комуникације са државом нападачем, без обавезе да се исто учини са осталим странама у сукобу.

[53] John Keller, „Cyber Genome program launched to bolster DOD infomation intelligence and cyber defense capabilities", 31.01.2010. године,

http://www.militaryaerospace.com/index/display/article-display/372766/articles/military-aerospace-electronics/executive-watch-2/2010/01/cyber-genome-program-launched-to-bolster-dod-information-intelligence-and-cyber-defense-capabilities.html, (31.01.2010).

[54] Alex Hudson, „Why does Google insist on having your real name?", BBC News, 28. July 2011, http://www.bbc.co.uk/news/magazine-14312047, (07.08.2011).

[55] United states District Court, Central District of Illinois, 2:11-cv-02068-HAB –DGB #15, 29 April, 2011, http://www.scribd.com/doc/54508329/ip-baker#open_download, (17.07.2011).

Примена прописа о неутралности на сајбер ратовање

Постојеће међународно право оружаних сукоба настало је из потребе регулисања оружаних сукоба који се односе на традиционалне сукобе, а не на сајбер ратовање. Технологија сајбер ратовања развија се много брже од међународног права.[56] Сајбер ратовање води се средствима која истовремено имају и војну и мирнодопску примену. Сајбер ратовање се може водити дистрибуирано и временски одложено. Због технолошког раскорака између права и природе ратовања постојећи међународни споразуми нису довољни за практичну примену на сајбер ратовање, што се не односи на основне принципе,[57] већ на праксу примене. То је узрок захтева да се регулисање сајбер ратовања мора спровести полазећи од општих ка посебним нормама. Његова анализа треба да започне од обичајног права и општих принципа међународног права,[58] а полазна смерница за то може се наћи у Повељи УН.[59] Наредни корак требало би да буде примена општеприхваћених обавезујућих норми,[60] у мери у којој су практично примењиви на сајбер ратовање. Последњи ниво анализе представља примена постојећих мултилатералних и билатералних споразума, специфичних принципа обичајног права и свега што се може применити у посебним ситуацијама праксе државне неутралности [10] .

Технолошки развој и међународно право

Развој националног и међународног права касни у односу на технолошки развој, што је првенствено последица неопходног консензуса свих релевантних субјеката у условима постојања супротстављених интереса. То је био чест случај током историје, попут регулисања примене ратне авијације, бојних и биолошких отрова[61] или нуклеарног наоружања.

[56] У првом наступу пред америчким Конгресом, начелник Здружене сајбер команде америчке војске (уједно и директор највеће обавештајне агенције у САД, *NSA*), генерал Кит Александер је истакао да су политичке директиве и правне норме које регулишу сајбер ратовање застареле и да нису у стању да прате брз развој техничких војних капацитета у области сајбер ратовања. Thom Shanker, "Cyberwar Nominee Sees Gap in Law", *The New York Times*, 14. априла 2010.

http://www.nytimes.com/2010/04/15/world/15military.html, (28.05.2010).

[57] Cordula Droege, No legal vacuum in cyber space, 16-08-2011 Interview, International Committee of the Red Cross , http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, (17.08.2011).

[58] Члан 38. Статута Међународног суда правде наводи опште принципе права као примарне изворе које треба цитирати у случајевима пред судом.

[59] Повеља УН, чланови 25, 48, 51 и 103.

[60] *Ius cogens* норме (обавезујуће право) представљају основни принцип међународног права за који се сматра да је свеприхваћен у међународној заједници. За разлику од обичајног права које захтева претходни пристанак и дозвољава измене кроз конвенције, ниједна држава нема право да прекрши *ius cogens* норме. У начелу, чине га забране агресорског рата, злочина против човечности, ратних злочина, пиратерије, геноцида, ропства, мучења и слично.

[61] Након прве употребе бојних отрова за време Првог светског рата, 1925. године у Женеви је усвојен први споразум који је регулисао употребу хемијских отрова и биолошких агенса ради вођења сукоба, Протокол за забрану употребе у рату омамљујућих, отровних и других гасова и бактериолошких метода ратовања.

Ова усаглашавања морају бити правовремена и адекватна. 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.[62] Било је потребно педесет година да се формулише потпуна забрана биолошког оружја[63] и додатних двадесет година да се доврши регулисање употребе хемијског оружја.[64] Са друге стране, нека правила ратовања претходила су свом времену, попут Конвенције о забрани војне или било које непријатељске употребе метода модификације животне околине из 1976. године,[65] Протокола о забрани оружја чији се делови не могу открити рендгенским зрацима из 1980. године[66] и Протокола о употреби ласерског оружја из 1995. године[67]. Ипак, теоретски или практично, ови *jus in bello*[68] прописи су на крају прилагодили постојеће ратно право употреби нових врста оружја.[69] Основни принципи права оружаних сукоба нису створени искључиво за поједине ситуације и окружења, већ регулишу општу употребу силе у свим ситуацијама. Проблем сајбер ратовања јесте што се његове активности не могу географски одредити, већ само последице,[70] што није могуће јасно разликовање војних и цивилних циљева, нити бораца и цивила, идентитет нападача се не може утврдити у реалном времену, а сајбер оружје не постоји у физичком облику. Стога је неопходно усвајање нових, специфичних стандарда за његово регулисање.[71]

---

[62] Draft Rules of Aerial Warfare, februar 1923. године, http://www.dannen.com/decision/int-law.html#C, (16.07.2009).

[63] 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. April 1972, http://www.icrc.org/ihl.nsf/FULL/450?OpenDocument, (16.97.2009).

[64] Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction, Paris, 13 January 1993, http://www.icrc.org/ihl.nsf/FULL/553?OpenDocument (16.07.2009).

[65] Convention on the prohibition of military or any hostile use of environmental modification techniques, 10. December 1976, http://www.icrc.org/ihl.nsf/FULL/460?OpenDocument, (16.07.2009).

[66] Protocol on Non-Detectable Fragments (Protocol I), Geneva, 10 October 1980, http://www.icrc.org/ihl.nsf/FULL/505?OpenDocument, (16.07.2009).

[67] Protocol on Blinding Laser Weapons (Protocol IV to the 1980 Convention), 13. October 1995, http://www.icrc.org/ihl.nsf/FULL/570?OpenDocument, (16.07.2009).

[68] *Jus in bello* су правила ратовања која регулишу понашање у рату која се примењују када државе прибегну оружаном сукобу и ограничавају прихватљиве активности у току сукоба. Принципи који се односе на заштиту цивила у време рата или потребе за пропорционалношћу употребе оружане силе углавном се сврставају у овај скуп правила. Најпознатији пример оваквих прописа је Женевска конвенција.

Jus ad bellum (легалност употребе силе) представљају међународно прихваћен скуп правила који потенцијално сукобљене стране морају испоштовати пре започињања сукоба ради процене да ли је улазак у њега легалан. Међународни споразуми користе ова правила да ограниче државама могуће оправдане разлоге за започињање рата. У двадесетом веку најчешће помињани билатерални споразуми који су укључивали оваква правила били су Кејлог-Брајандов пакт, Лондонска (Нинбершка) повеља и Повеља Уједињених нација. Граница између принципа *jus ad bellum* и *jus in bello* је генерална и није прецизна, већ се њихово разликовање своди, углавном, на област легалности пре отпочињања рата и у току вођења рата.

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

[70] 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.

[71] 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" u Computer Network Attack and In-

Разликовање бораца и небораца у сајбер рату

Право оружаних сукоба ставља посебан нагласак на заштиту лица током оружаних сукоба и дели их на борце и неборце. Борци су сви припадници оружаних снага страна учесница у сукобу, сем медицинског и верског особља.[72] Они имају права да учествују у непријатељствима[73] и представљају „скуп организованих оружаних снага, група или јединица који се налазе под командном одговорношћу институција и лица дате државе која су одговорна за руковођење својим подређенима".[74] Борци имају обавезу да се „разликују од цивилне популације док су укључени у борбена дејства или се налазе у стању припрема за напад".[75] У категорију бораца спадају и „чланови милиција и добровољачких група, укључујући и припаднике организованих покрета отпора, који се боре на страни државе учеснице у сукобу", под условом да испуњавају посебне услове.[76] Неборци су цивили и непријатељско особље ван борбе (ратни заробљеници, рањени и болесни, медицинско и верско особље). Цивили су особе које нису чланови оружаних снага учесница у сукобу и који не узимају директно учешће у непријатељствима.[77] Опште је правило да цивили, било као део популације, било као појединци, не смеју бити циљеви напада.[78] Забрањени су и акти претње насиљем, чија је основна функција да шире страх међу цивилном популацијом. Цивили уживају заштиту од напада „сем уколико, и само за време док узимају директно учешће у непријатељствима".[79] Оваква регулација није практична за примену у сајбер ратовању. Сајбер ратовање могу водити сви (припадници војске, терористи, припадници организованих група мимо званичних војних снага неке државе, цивили које ангажује држава или који делују самостално и било ко други). Средства сајбер ратовања имају истовремено и ратну и мирнодопску примену и не захтевају ангажовање војног особља. То не значи да се у свету не развијају војни капацитети, јединице, команде и институције за сајбер ратовање.[80] Карактер сајбер напада се мења. Савремене сајбер нападе све чешће покрећу државе.[81] Свакој

---

ternational 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.

[72] Допунски протокол I, Члан 43 (2).

[73] Допунски протокол I, Члан 43.

[74] Исто, члан 43 (1).

[75] Исто, члан 44 (3).

[76] Конвенција о поступању са ратним заробљеницима (III), члан 4(A)(2), од 12. августа 1949. године (у даљем тексту Трећа Женевска конвенција). Ови услови су да „њима командује особа која је одговорна за своје подређене", носе „фиксни карактеристични знак који је препознатљив са даљине", „отворено носе оружје" и спроводе своје операције „у складу са законима и обичајима рата".

http://www.icrc.org/ihl.nsf/FULL/375?OpenDocument, (19.01.2010).

[77] Допунски протокол I, члан 50 (1).

[78] Исто, члан 51 (2).

[79] Исто, члан 51 (3).

[80] Hui Min Neo, „China, US, Russia in cyber arms race: net security chief", AFP. 28 January 2010, http://www.google.com/hostednews/afp/article/ALeqM5gBI-UmsuwvR6i-mxl5TDGvDuGtrw, (24.02.2010).

[81] Greg Austin, „China's Cybersecurity and Pre/emptive Cyber War", New Euope, 14 March 2011, http://www.neurope.eu/articles/Chinas-Cybersecurity-and-Preemptive-Cyber-War/105270.php, (19.03.2011).

држави је једноставније да унајми рачунарске стручњаке за припрему и покретање сајбер операција него да изгради војне капацитете. Научноистраживачке агенције војске САД, DARPA[82] и специјализована одељења NSA[83] већ дуги низ година јавно објављују конкурсе за разне пројекте у области сајбер одбране, шпијунаже или напада. Пример за то је обиман одбрамбени програм *Cyber Fast Track*.[84] Овакав начин вођења сајбер ратовања је у складу са растућим трендом ангажовања приватних армија и најамника у свету.[85] Развој софтвера и техника за сајбер ратовање може бити поверен чак и компанијама у страним државама. Таква ситуација се не може лако регулисати постојећим правом оружаних сукоба које обавезује борце да се јасно идентификују као припадници војних јединица [11]. У сајбер ратовању није неопходно да сајбер борци буду прикључени војним јединицама. Иако међународно право препознаје реалност ратних ситуација у којима борци из објективних разлога нису у могућности да се разликују од небораца,[86] у случају сајбер ратовања ради се о нерелевантности овакве одредбе. У теорији, једини облик идентификације је могућ остављањем „ауторског потписа" у злонамерни програм употребљен за напад или јавним признавањем напада, што није реално да се деси, јер је супротно суштини сајбер ратовања које остварује предност баш у прикривености нападача. Међутим, она је противна праву оружаних сукоба.[87] Непоштовање правила ратовања представља ратни злочин, који је тежи што су теже последице сајбер напада. Цивили који учествују у сајбер нападу су легитимне мете противнапада, али само за време док остварују директно учешће у операцијама, а то је, такође, веома тешко утврдити у реалном времену.[88] Насупрот томе, борци могу бити нападнути без обзира на њихове тренутне борбене активности. Ангажовање цивила у борбама је преступ,[89] а учешће војног особља у сајбер нападима је легално. Припадници војних јединица који предузимају сајбер нападе имају право да предузимају ратне акције и не могу бити оптужени за ратна дела, укључујући и убиства противничких бораца, уколико су она изведена у складу са правом оружаних сукоба.[90] Ангажовање цивила да воде борбе може бити индивидуални ратни злочин, уколико не постоји одговорност државе за њихово ангажовање или колективни, ако их ангажује држава. Овај принцип је применила влада САД када је по одредби Акта о војним судовима из 2006. године[91] осудила ра-

[82] Defense Advanced Research Projects Agency

[83] National Security Agency

[84] DARPA-RA-11-52: Cyber fast Track (CFT), Defense Advanced Research Projects Agency, 3 August 2011, https://www.fbo.gov/?s=opportunity&mode=form&id=406db188e0e1935a806c143a5603eb48&tab=core&_cview=0, (03.08.2011).

[85] Desire Athow, „Former NSA/CIA Director Suggests Employing Mercenaries For Cyberwarfare", IT Pro Portal, 01 August 2011, http://www.itproportal.com/2011/08/01/former-nsa-cia-director-suggests-employing-mercenaries-cyberwarfare/, (03.08.2011).

[86] Тада се идентификују отвореним ношењем наоружања. Исто, члан 44, став 3.

[87] Допунски протокол I, члан 37.

[88] Допунски протокол I, члан 51 (3).

[89] Цивили нису категорија којој је дозвољено учешће у борбама. Допунски протокол I, члан 43.

[90] „Борци имају право да директно учествују у борбама", Допунски протокол I, члан 43 (2).

[91] Military Commissions Act of 2006, HR-6166 је акт америчког Конгреса са циљем да регулише суђења војних комисија ратним заробљеницима за повреде ратног права, као и за друге сврхе. http://www.loc.gov/rr/frd/Military_Law/pdf/PL-109-366.pdf , (29.06.2010).

њеног малолетног Канађанина муслиманског порекла, ухваћеног у Авганистану, под оптужбом да је учествовао у борбама на противзаконит начин.[92]

Поред цивила и бораца, постоје и друге категорије лица која могу узети активно учешће у борбама.[93] То су:

– припадници цивилних милиција, добровољачких одреда и покрета отпора који припадају некој од страна у сукобу,

– оружане снаге страна у сукобу које непријатељ не признаје и

– грађани који спонтано одговарају на инвазију, такозвани *levee en masse.*[94]

За сајбер ратовање је посебно карактеристична последња категорија. Широка група спонтано организованих руских цивила била је директно укључена у нападе на Естонију, Грузију и Киргистан током периода 2007–2009. године, али не у акту самоодбране, већ у функцији сајбер агресије на политички супротстављене државе у време мира. Статус бораца може се дати и нерегуларним снагама.[95] Корени ове идеје датирају из Бриселске декларације из 1874. године,[96] која је описивала неконвенционалне групе бораца, на које се примењују сви закони, права и дужности ратног права, а не само статус ратних заробљеника. Ова идеја се у прилагођеном облику може применити и на сајбер ратовање. Националистичке групе могу лако бити употребљене у току сајбер сукоба као патриотска подршка ратним активностима својих влада [12]. Такав случај се десио и током бомбардовања СР Југославије 1999. године, када су групе и појединци из Србије, Русије, Кине и других држава предузимали пропагандне активности на разним форумима у иностранству, измене *web* страница и спорадичне *DDoS* нападе на сервере *NATO*-а као покушај супротстављања његовим војним дејствима.[97] Статус ових нападача је изузетно проблематичан. Уколико се њихово ангажовање оцени као агресија, не може им се признати статус бораца, па стога немају ни њихова права. Њима се може судити на основу чињенице да су борбено ангажовани у сукобима и могу бити мете напада. Њихово војно ангажовање у сукобу није легално и представља кршење права оружаних сукоба, а напад на њих у облику војног одговора је оправдан.

---

[92] Канадски држављанин Омар Кадр је, наводно, у Авганистану ручном бомбом напао америчке снаге. Након рањавања је ухапшен и пребачен у војни затвор Гуантанамо на Куби, где га је војни суд осудио на казну затвора. У тренутку хапшења имао је 15 година. Кадр није користио незаконито оружје, ограничио је ефекте свог напада на непријатељске снаге и није се представљао као заштићени цивил док се припремао за напад. Стога је једино дело за које је могао бити оптужен по ратном праву било само незаконито учешће у борби. The Omar Khadr Case, University os Toronto, Faculty of Law,

http://www.law.utoronto.ca/faculty_content.asp?itemPath=1/3/4/0/0&contentId=1617, (18.05.2011).

[93] Допунски протокол I, члан 50.

[94] Ова категорија била је директно укључена у руска сајбер дејства у Естонији, Грузији и Киргистану од руске стране током периода 2007– 2009. године, али не у функцији одбране, већ напада.

[95] Друга Хашка конвенција из 1899. године, члан 1. http://www.icrc.org/ihl.nsf/FULL/150?OpenDocument, (13.02.2009). Трећа женевска конвенција из 1949. године.

[96] Иако ова декларација никада није ступила на снагу као правоснажан међународни законски инструмент, каснији споразуми су репродуковали њене значајне делове.

[97] Лазар Николић, „Размена информација и/или емоција", Нова српска политичка мисао, Специјално издање 1, 1999. године, Србија и НАТО; Слободан Наумовић, „Netwars: Интернет и агресија на Југославију", Нова српска политичка мисао, Специјално издање 1, 1999. године, Србија и НАТО; Душан Дингарац, „На мрежи, на положају" Свет компјутера, мај 1999. године, www.sk.rs/1999/05/skak01.html, (11.05.2010).

Поред национално настројених цивилних група учешће у сајбер сукобима могу узети и други облици група. Најпознатији пример су организоване групе младих, информатички оспособљених појединаца, попут хакерске групе *Anonymous*, њене фракције *AnonOps* и *LulzSec* или старије групе *Peoples Liberation Front*, чије порекло датира од средине осамдесетих година двадесетог века. Оне представљају међународне, дистрибуиране, хијерархијски хоризонтално организоване и политички мотивисане групе хакера–активиста (*hacktivists*). Њихове активности су усмерене на веома широк круг мета, од појединаца, преко организација, институција и држава (владе Ирана, Туниса, Бахреина, Египта, Зимбабвеа, Аустралије, Турске, Израела и других), на разне финансијске корпорације (попут *Sony Corporation*, *Visa*, Сајентолошке цркве, Вестборо баптистичке цркве, безбедносних фирми и организација попут *HBGary Federal*, па чак и владиних агенција попут CIA–е). У њиховом деловању нема образаца, јер остварују широки спектар активности, па је тешко утврдити њихову позадину, порекло и намере. Облик њихове организације и функционисања на најбољи начин представља могућности примене сајбер простора за политички мотивисане активности. Иако њихово деловање представља облик сајбер криминала, који у неким случајевима може бити окарактерисан као сајбер тероризам, не постоји ниједан разлог због којег се у будућности не би десио сличан облик сајбер ратовања усмерен на неку државу или групу држава, који би предузеле слично организоване групе које не би спајала националност, већ идеолошка и политичка оријентација. Такви напади могу се предузети у време оружаног сукоба или мира. Они не би имали статус најамника, јер не воде дејства због накнаде, већ због идеологије, па такав облик организовања веома подсећа на начин окупљања и војног ангажовања интернационалних бригада шпанског грађанског рата, у којем борци покрећу нападе од куће. С друге стране, велике силе све чешће прате тренд роботизације армија и ангажовања плаћеника.[98] То ставља међународно право на искушење, пошто је оно ограничено на сукобе међународних ентитета, а не на дистрибуиране и комплексне сукобе и свакако ће утицати да се у будућности усвоје нови облици норми међународног права.[99]

Схватање сајбер оружја

Сајбер ратовање представља примену сајбер оружја од стране државних актера усмерену против сајбер инфраструктуре противника применом војних активности. Практично, оно се састоји од одбрамбених и офанзивних активности,[100] које имају све већу моћ да остварују кинетичке ефекте употребе силе. Иако постојеће право нема много додирних тачака са технологијом сајбер ратовања, оно се ди-

[98] Nathan Hodge, „Drone Pilots Could Be Tried for 'War Crimes' Law Prof Seys", Wired, 31 March 2010, http://www.wired.com/dangerroom/2010/03/the-drone-war-legal-smackdown/, (18.07.2011).

[99] Rauscher, K., Korotkov, A., *Working Towards Rules for Governing Cyber Conflict*, *Russia-U.S. Bilateral on Critical Infrastructure Protection*, EastWest Institute, January 2011, http://www.ewi.info/working-towards-rules-governing-cyber-conflict, [citirano: 28. januar 2011], str. 36.

[100] Обавештајне активности се у већини националних правних система не сматрају врстом ратних дејстава.

ректно односи на ефекте разарања и угрожавања људи, као последице примене било које врсте оружја. Појам „сајбер оружје“ има широко значење. У начелу, оно представља сваки програм, технику или уређај којим се употребом информација и информационих средстава приступа противничким системима ради војног дејства на њих. Ратно право се односи на све врсте непријатељстава које предузимају оружане снаге неке државе.[101] Да би право могло да регулише сајбер ратовање, потребно је да се претходно дефинише појам сајбер оружја. Америчко Министарство одбране дефинише појам „оружје“ као: „средство намењено да убије, повреди или онеспособи људе или да оштети или уништи материјална средства“.[102] Да би се разумела природа сајбер оружја може се направити аналогија са ватреним оружјем. Након опаљења из ватреног оружја метак пролази кроз ваздух и погађа мету, разарајући је. Оружје, само по себи, не ствара штету, већ му је намена да допреми средство уништења (метак) до мете. Средство уништења не може да начини штету, све док се не испали из ватреног оружја. На крају, ни оружје, ни метак нису опасни све док их борац не узме у своје руке, напуни оружје мецима и опали их. У сајбер рату, малициозни код, рачунарска инструкција или податак су средство уништења и имају улогу метка. Рачунарски хардвер је средство којим се тај „метак“ ствара и допрема до циља напада. Оператер који користи информационе системе, односно програмер који пише програме којима се предузима сајбер напад је борац. Према томе, три елемента су основ сајбер напада: **софтвер, хардвер и нападач**. Сваки од њих је битан ратном праву за регулисање ратних сукоба. Они се морају употребљавати у складу са принципима права оружаних сукоба, а чињеница да се користе за борбена дејства чини их легитимним циљевима напада.[103] Међутим, прихватање чињенице да информације, програми, рачунарски системи и целокупна сајбер инфраструктура могу бити оружје не значи да они јесу оружје у свакој ситуацији. Они су статусно неутрални, јер служе за пренос свих информација, мирнодопских или нападачких.[104] Није иста употреба информатичких средстава за директан сајбер напад и у случају обезбеђења пратећих функција ратовања, попут комуникација, логистике, у обавештајне сврхе или за пасивну одбрану. У првом случају они су оружје, а у другом средства вођења рата. Као средства која омогућују ратна дејства

[101] На пример, САД имају став да: „…ратно право обухвата све међународне прописе за вођење непријатељстава усмерених ка САД или њене грађане, укључујући и међународне споразуме, чији су потписници САД и међународно јавно право примењиво на њих”. Директива Министарства одбране САД 5100.77,1998, http://www.dtic.mil/whs/directives/corres/pdf/d510077_120998/d510077p.pdf 12.12.2006).

[102] http://www.epublishing.af.mil/pubªles/af/51/aª51-402/aª51-402.pdf (01.02. 2006).

[103] Стране у сукобу морају правити разлику између цивила и бораца и смеју нападати само борце. Цивили губе право на заштиту у току сукоба за време док узимају директно учешће у непријатељским дејствима. Насупрот томе, статус борца даје право противнику да их нападне, без обзира на њихове борбене активности у току сукоба. Ангажовање цивила у борбама је преступ, а учешће војног особља у сајбер нападима је легално. Цивили нису категорија којој је дозвољено учешће у борбама. Допунски протокол Женевској конвенцији од 12. августа 1949. који се односи на заштиту жртви у међународним оружаним конфликтима (Допунски протокол I), члан 43, 8. јун 1977,

http://www.icrc.org/ihl.nsf/full/470?opendocument, (16.05.2010).

[104] Америчка морнарица не третира сателите употребљене за прослеђење информатичког напада оружјем. Видети David DiCenso, „IW CyberLaw: The Legal Issues of Information Warfare“, *Airpower Journal* 1999.

ства, информациони системи и инфраструктура доприносе способности вођења рата и њихово онеспособљавање или уништење у појединим ситуацијама може довести до значајне војне предности. У том светлу, напад на непријатељске информационе системе није у супротности са ратним правом.[105] У новијој историји НАТО савез је у неколико наврата употребио овакво објашњење, попут бомбардовања Радио телевизије Србије 1999. године или Либијске државне телевизије 2011. године. Међутим, сајбер ратовање омогућава асиметричност дејстава, па се овакво тумачење може подједнако применити у случају напада на информационе ресурсе малих држава и великих сила.

Надлежност држава и повреда неутралности у току сајбер ратовања

Проблем државне надлежности у сајбер простору је сложен. Дигитални подаци у раздвојеним пакетима информација прелазе неприметно преко државних граница. Сајбер нападачи могу бити државни органи, али и не морају. Зато је процена природе сајбер напада веома сложена. При процени повреде неутралности у току сајбер напада неопходно је да се докаже да је за њега одговорна држава.

Резолуција УН предвиђа да Савет безбедности одређује да ли је неки напад акт агресије, која је дефинисана као „употреба оружане силе од стране неке државе против суверенитета, територијалног интегритета или политичке независности друге државе“.[106] Она набраја облике агресије у које укључује „инвазију или напад оружаним снагама, војну окупацију, анексију путем употребе силе“ предузету против стране државе, „употребу било каквог оружја“ против стране државе, као и напад на оружане снаге друге државе. Оваква формулација агресије не омогућава одговор на питање да ли је сајбер напад акт агресије. Ова процена може ићи од крајности да је сваки сајбер напад акт агресије,[107] до става да то није ниједан, јер њихово дејство није кинетичко, па не представљају примену физичке силе,[108] и да стога не повређују неутралност нападнуте државе [13].[109] Трећа група аутора сматра да квалификацију природе сајбер оружја треба извести на основу последица, а не врсте напада [14], јер употреба биолошког и хемијског оружја показује да примена кине-

[105] У складу са I Додатним протоколом (из 1977. године) на Женевску конвенцију из 1949. године, (односи се на заштиту жртава међународног ратног сукоба), члан 52,

http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 (01.04.2009.)

[106] Резолуција УН број 3314 (1974. година) http://www.un.org/documents/ga/res/29/ares29.htm, (12.2.2010).

[107] „Било који рачунарски напад који у међународним оквирима узрокује било какав облик деструкције унутар суверене територије друге државе представља незакониту употребу силе јер може да изазове ефекте као и у случају оружаног напада у чијем случају је оправдано право на самоодбрану и потпада под надлежност Повеље УН, члан 2(4).”; Sharp, Cyberspace and the Use of Force, стр. 133.

[108] По члану 2, став 4 и Члану 51 Повеље УН о дефиницији агресије.

[109] Овај став је временом застарео, с обзиром на развој нових врста сајбер напада који могу онеспособити рад нападнутих система и изазвати физичку штету у зависности од врсте циља.

тичке силе не мора да буде критеријум за процену природе напада и последице дејства. У складу с тим, сајбер напад са смртним последицама или уништењем физичких објеката треба да се сматра актом употребе силе [15, стр. 207], [3, стр. 16]. Четврта група аутора као основ за разматрање узима искључиво државни статус нападача.[110]

Утицај сајбер ратовања на повреду неутралности нарушавањем суверенитета државе зависи и од облика његове манифестације – територијалног и националног суверенитета.[111] Свака држава има надлежност на властитој територији, али постоје и изузеци, на пример, у случају када се примењује на дипломате страних држава. Надлежност над тим лицима по националном принципу имају њихове матичне државе, чак и када се они физички не налазе на њиховој територији. У пракси постоји и трећи, безбедносни принцип суверености, који се схвата као „принцип надлежности у коме нације могу узети за право да казне страну државу за одређено понашање ван своје територије, које је усмерено против њене безбедности, територијалног интегритета и политичке независности".[112] Иако овај принцип није усвојила међународна заједница, а постоји реална опасност да га поједине државе злоупотребе по „праву јачег", по својој форми је погодан за примену у ситуацијама сајбер ратовања, нарочито у ситуацијама када се сајбер напад покрене из неутралне државе. За разлику од традиционалног ратовања, принцип територијалне надлежности није практичан за оцену повреде неутралности у току сајбер ратовања, јер сајбер напад не повређује државну безбедност, територијални интегритет и политичку независност буквалним проласком кроз информационе комуникације до циља.

Аналогија принципа неутралности у сајбер ратовању и класичним облицима ратовања

Свако географско подручје у којем се може ратовати има своја правила о неутралности. Иако су им општи принципи и циљ заједнички, ова правила се међусобно разликују због различите природе подручја. У погледу неутралности, основни принцип је да стране у сукобу не смеју повредити неутралност неутралне државе, а она је у обавези да одбрани властиту неутралност у складу са расположивим могућностима. Из географске перспективе одређена подручја су, по својој природи и ограничењима, слична сајбер простору. Ваздух, море и космос су флуидне средине чије границе морају бити замишљене у простору и нису јасно видљиве попут копнених. Отворено море није у власништву ниједне државе. У неким деловима, као што је територијално море, државни суверенитет је потпун, али са одређеним околностима и друге државе у току рата имају одређена права у њему.

[110] Ira Flatow, „Cyberattacks May Be 'Acts of War'" 3 June 2011, NPR, Science Friday, http://www.npr.org/2011/06/03/136925541/cyber-attacks-may-be-acts-of-war, (14.07.2011).

[111] Sinks, *Cyber Warfare and International Law*, стр. 14.

[112] Boczek, B., *International Law: A Dictionary,* стр. 80.

Аналогија неутралности у копненом и сајбер ратовању

Неутралност у току копненог ратовања регулише V Хашка конвенција из 1907. године.[113] Међународне границе „су имагинарне линије које раздвајају територијалне суверенитете“[114] и усаглашене су вишестраним међународним уговорима. Повреда државних граница од стране недржавних субјеката представља кршење закона те државе. Насилно нарушавање тих граница од стране друге државе представља акт агресије и спада у надлежност међународног права. Ово право не сматра све повреде државних граница актом агресије. У појединим случајевима надлежна тела међународне заједнице доносила су одлуке да повреда територије неке државе не представља насилни акт, већ право државе на колективну самоодбрану.[115]

Последице напада нису једино мерило повреде међународног права. У сајбер ратовању могући су напади са потенцијално смртоносним и разарајућим последицама који нису били успешни, или су били прикривени, па жртва није ни свесна чињенице да се ради о нападу. Аналогно томе, безуспешно артиљеријско бомбардовање циља на страној територији је акт агресије и без уништења мете. И у тим ситуацијама угрожена држава има право на самоодбрану или заштиту неутралности.

Неутрална земља има обавезу да спречи употребу своје територије као базе или уточишта за стране у сукобу.[116] Уколико изостане таква активност, држава угрожена нападом има право да предузме одговарајућу акцију против нападача. Оваква ситуација током сајбер ратовања може имати далекосежне последице по ширење могућег конфликта. По аналогији са правилима која важе у току копненог ратовања, неутрална држава има обавезу да онемогући војну употребу властите информационе инфраструктуре и сајбер простора од стране држава у сукобу или постављање војних инсталација које имају функцију вођења сукоба. Ова обавеза неутралне државе не постоји у случају спречавања активности појединаца. То је значајно за сајбер ратовање, јер за покретање сајбер напада није неопходно ангажовање војних јединица. Правила о копненој неутралности у току оружаних сукоба стога се не могу дословно применити на већину ситуација у сајбер ратовању.[117]

---

[113] http://www.icrc.org/ihl.nsf/FULL/200?OpenDocument, (28.05.2010).

[114] Boczek, B., *International Law: A Dictionary*, str 208.

[115] Пресуда Међународног суда правде у случају Војне и паравојне активности унутар и против Никарагве (Никарагва против САД), по питању упада снага Никарагве на територију Ел Салвадора 1986. године. International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),
http://www.icj-cij.org/docket/index.php?sum=367&code=nus&p1=3&p2=3&case=70&k=66&p3=5 (02.06.2009); Sinks, стр. 12.

[116] V i XIII Haška konvencija.

[117] Правила којим се ратним заробљеницима забрањује слање писама, телефонирање или емитовање информација које су у функцији вођења рата се не могу по аналогији дословно употребити за забрану ратним заробљеницима на неутралној територији да приступају рачунарима и Интернету, нарочито када се узме у обзир да је у појединим државама приступ Интернету проглашен основним људским правом (Финска, Естонија, Француска, Грчка, Шпанија) и досадашње ставове УН. Report of the Special Repporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Human Rights Council, General Assembly, 16 May 2011,
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, (12.06.2011)

Аналогија неутралности у поморском и сајбер ратовању

Принципи ратовања на мору дефинисани су у више различитих међународних конвенција.[118] Море је подељено на подручја у којима се разликује државни суверенитет: отворено море, територијално море и поморске економске зоне. Територијално море представља појас мора до државне обале који обухвата ваздушни простор изнад и морско дно испод њега у којем државе остварују пун суверенитет.[119] Сајбер напади предузети у овом подручју се по надлежностима и последицама не разликују од напада на копну.[120] Међународне воде нису предмет суверенитета било које државе и све имају права да их користе слободно у мирољубиве сврхе, док било који облик агресије у међународним водама, укључујући и сајбер нападе, представља кршење међународног права. Сви општи принципи ратног права примењиви су и на поморско ратовање. Корисници мора и океана морају поштовати права и слободе неутралних корисника отвореног мора и правила поморског ратовања у току сукоба.[121] Ова правила су специфична и прилично компликована у неким случајевима. Странама у сукобу дозвољен је пролаз кроз неутралне воде, али није употреба вода и лука неутралних страна за постављање система за комуникацију војних снага и војне операције.[122] У правилима поморског ратовања може се приметити битна разлика у односу на копнено ратовање. Обавеза да се спречи повреда неутралности на копну је апсолутна, док у поморском ратовању она зависи од могућности неутралне земље да то учини. Неутрална држава је „овлашћена," не и обавезна, да задржи ратни брод зарађене стране када се тај брод налази у њеним водама, а требало је да их напусти.[123] Ова правила су последица околности у време настанка правила о поморској неутралности, 1907. године, када многе државе нису имале властиту морнарицу и капацитете да одврате стране ратне бродове, а све су поседовале некакву могућност спречавања проласка копнених снага. Овакво поређење може се применити и данас у случају сајбер ратовања. Дужност неутралне земље да спречи злоупотребу властитих сајбер капацитета за сајбер нападе не може бити, већ је условљена техничким могућностима. У таквим ситуацијама нападнута страна има право на самоодбрану и предузимање пропорционалних мера одбране. Неутралне државе имају обавезу да остваре контролу емитовања ра-

[118] Хашка конвенција V и XIII; Конвенција о поморској неутралности; Статут Међународног суда правде и Бечка конвенција.

[119] UNCLOS, Part 2, Territorial Sea and Contiguous Waters, http://www.un.org/Depts/los/convention_agreements/texts/unclos/closindx.htm, (13.05.2009).

[120] Уређује га XIII Хашка конвенција, 1907, http://www.icrc.org/ihl.nsf/INTRO/240?OpenDocument, (13.05.2009).

[121] Конвенција о поморској неутралности, UNCLOS (United Nations Convention on the Law of the Sea), Бечка конвенција (члан 61); УН конвенција о морском праву; Walker, G.,*Information Warfare and Neutrality",* стр 38.

[122] V Хашка конвенција, члан 3; XIII Хашка конвенција, члан 5; Конвенција о поморској неутралности, члан 4б и Хелсиншки принципи 1.4.

[123] XIII Хашка конвенција, чланови 21-24; Конвенција о поморској неутралности, члан 17; Нордијска правила о неутралности, члан 4 (1); Хелсиншки принципи, 2.2; UNCLOS, 1982 год, http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm, (19.05.2009).

дио-сигнала у властитим територијалним водама,[124] што у савременим условима треба да важи и за комуникацију у сајбер простору. Без обзира на могућу аналогију, питање је да ли постоји могућност њене примене у пракси. Одговор на то питање није коначан и зависи од технолошког развоја. Нужан услов за потпуно остваривање неутралности у сајбер ратовању стога зависи од технолошке могућности за дубинску контролу интернет саобраћаја у реалном времену на пакетном нивоу [5] и програма за откривање активности на интернету.[125] Влада САД је далеко напредовала у том погледу, применом и унапређивањем аутоматизованих система за контролу интернет саобраћаја, пре свих система *Einstein*[126] (наследника ранијег система *Carnivore*) и широке мреже праћења свих врста комуникација мреже *Eshelon*.

Поред Хашких конвенција, на регулисање поморског ратовања и неутралност могу се применити и други, билатерални и мултилатерални прописи попут *Notice to Mariners – NOTMAR*[127] споразума (служе за јавно емитовање битних хидрографских, навигационих, комуникационих и других информација за поморце, попут одржавања поморских војних маневара војних снага неке државе),[128] INCSEA[129] и *ADIZ (Air Defence Identification Zone*)[130] споразуми и други који практично регулишу ситуације за превазилажење могућности избијања инцидената на отвореном мору и изнад њега.[131] Ипак, с обзиром на то да су више оријентисани на практична питања, ови споразуми немају већи потенцијал за аналогију примене у сајбер ратовања.

Аналогија неутралности у ваздушном и сајбер ратовању

Ваздушни простор неке државе део је атмосфере изнад копнене територије и територијалних вода и у надлежности је њеног суверенитета.[132] Све летелице које улазе у нечији ваздушни простор морају се идентификовати и обавестити домаће органе о детаљима лета. У складу са Чикашком конвенцијом о међународној цивилној авијацији из 1944. године,[133] државе могу склапати међусобне уговоре ради планирања међународних цивилних авио-услуга. Ови споразуми односе се на цивилне летове, док су процедуре знатно рестриктније за војне летелице. Државе

[124] V Хашка конвенција, члан 3. и XIII Хашка конвенција члан 5; Конвенција о поморској неутралности, члан 4 (б) и Нордијска правила о неутралности, чланови 12. и 13.

[125] Fact Sheet: U.S. Department of Homeland Security Five-Year Anniversary progress and Priorities, Homeland Security, 6 March 2008, http://www.dhs.gov/xnews/releases/pr_1204819171793.shtm, (13.05.2011).

[126] Систем *Einstein* служи за надзор интернет саобраћаја у реалном времену у Националном интегрисаном центру за сајбер безбедност и комуникације Министарства за унутрашњу безбедност САД (*National Cybersecurity and Communications Integration Center of The Department of Homeland Security*).

[127] http://www.notmar.gc.ca/privacy.php

[128] http://msi.nga.mil/NGAPortal/MSI.portal

[129] „Agreement on Prevention of Incidents on and Over the High Seas", споразум је сачињен 1972. године између САД и СССР, касније су дограђивани у више наврата.

[130] http://en.wikipedia.org/wiki/Air_Defense_Identification_Zone , (19.05.2009).

[131] У току бомбардовања 1999. године интернет саобраћај СР Југославије био је краткотрајно прекинут.

[132] Boczek, стр. 202.

[133] http://www.icao.int/icaonet/dcs/7300.html, (12.04.2009).

драстично бране властити ваздушни простор и интересе. О томе сведоче разни инциденти у ваздушном простору, попут обарања америчког војног шпијунског авиона У-2 над СССР-ом 1960. године, путничког јужнокорејског авиона 1983. године и иранског путничког авиона у Персијском заливу 1988. године. Хашким правилима за ратовање у ваздушном простору дефинисано је да акције неутралних држава ради заштите своје неутралности које оне предузимају да би одбраниле своја права, која им припадају неутралним статусом, не смеју се тумачити као непријатељски акти.[134] Општи принципи ратног права дефинисани у Повељи УН могу се применити и у случају ратовања у ваздушном простору. Међутим, једноставно пресликавање међународних правила ратовања у ваздушном простору[135] на сајбер простор није могуће, због разлике у специфичној природи окружења сукоба. На пример, у ваздушном саобраћају постоји правило да се обавезно захтева дозвола за прелет преко територије стране државе, што би било тешко остварив, чак и у случају аутоматске комуникације. Такав захтев није могућ ни због етичког принципа да ни једна држава на свету нема право да контролише светске дигиталне информације које се преносе путем интернета и селективно их блокира.[136] И у овом случају не постоји апсолутна обавеза неутралне државе да спречи повреду властите неутралности, већ то зависи од технолошких могућности.

Аналогија неутралности при ратовању у свемиру и сајбер ратовању

Свемир је простор изнад атмосфере који окружује Земљу. Међународно право не дефинише границу између ваздушног простора и свемира, али наглашава да су „државе сагласне да се државни суверенитет не простире у висину без икаквих ограничења".[137] Предлози за могућу границу између свемира и ваздушног простора заснивају се на различитим стручним и техничким критеријумима (на пример, гравитационој сили или густини атмосфере која омогућава кретање савремених летелица, итд.), а постоје и предлози да није ни потребно дефинисати ову границу, да се не би ометао развој космичке технологије. Иако граница свемира није одређена, он се физички разликује од ваздушног простора и постоји потреба да се активности у њима различито дефинишу. На пример, слободан лет авиона преко туђе територије није неограничен, а прелети сателита јесу, јер ниједна држава по Споразуму о

[134] Уколико војни ваздухоплови повреде простор неутралне земље, може им се наредити да се приземе и могу се запленити, а уколико то одбију, могу бити присилно приземљени или оборени. У случају да је у невољи, авион стране у сукобу може слетети на територију неутралне државе, али претходно мора сигнализирати да је у таквој ситуацији (чак и у таквој ситуацији посада мора бити интернирана, а ваздухоплов заплењен).

[135] Хашка правила за ратовање у ваздушном простору из 1922. године, http://lawofwar.org/hague_rules_of_air_warfare.htm, (12.04.2009).

[136] Grant Gross, „Obama 'Internet kill switch' plan approved by US Senate panel", techworld.com, 25. јун 2010, http://news.techworld.com/security/3228198/obama-internet-kill-switch-plan-approved-by-us-senate/?olo=rss, (25.06.2010).

[137] Boczek, стр. 238.

свемиру из 1967. године не полаже право својине над свемирским простором и космичким телима. То је изузетно значајан принцип који може послужити и у случају сајбер простора. Сајбер простор се стално повећава, а његово ширење зависи од количине података и активности корисника. С друге стране, државни суверенитет у сајбер простору све више јача и границе његовог протезања су релативно познате. Стога је дефинисање заједничког дела сајбер простора једино могуће инверзним дефинисањем подручја у којима владају национални суверенитети.

У свемиру државе смеју да предузимају искључиво мирољубиве активности. Оружје за масовно уништење је забрањено. Ипак, употреба свемира у неке војне сврхе је дозвољена, као што су обавештајне и извиђачке активности.[138] Многобројни војни сателити користе се за снимања земљине површине, преношење војних телекомуниационих и управљачких сигнала за авионе, пројектиле и беспилотне летелице. Овакав принцип ограничавања војних активности погодан је и за сајбер простор у којем би се могла забранити употреба сајбер напада на циљеве чије би уништење могло изазвати велике жртве и разарања, док би обавештајне, извиђачке и управљачке активности биле дозвољене. Пошто се сајбер простор може простирати и у свемиру, постојећи прописи за свемир морају се применити и на сајбер ратовање у свемиру. Сајбер напад упућен кроз свемир не регулише ниједан споразум, а мало постојећих међународних прописа може се применити на њега по аналогији.[139] Ратно право могуће је применити на ситуације у свемиру на општи начин као и у свим осталим подручјима.

Закључак

Сајбер простор представља једно од највећих цивилизацијских достигнућа. Њиме се изједначавају права и знање свих људи и омогућава остваривање најзначајнијих идеала човечанства. С друге стране, баш та масовност му умањује ниво безбедности на индивидуалном, националном и међународном нивоу. У њему се манифестују међусобно супротстављени појединачни интереси криминалаца, терориста, али и нација. Без општеприхваћене регулације његова деструктивна примена може поништити све предности и наде које пружа човечанству.

Човечанство ратује од свог постанка и мало је вероватно да ће у скорој будућности престати. Штавише, ова активност се налази на врху лествице државних приоритета. Имајући то у виду, разумљиво је настојање већине држава да сајбер простор и његову инфраструктуру, сервисе и информације употребе у функцији вођења сукоба. Многе националне одбрамбене стратегије већ дефинишу сајбер простор као ново подручје вођења војних операција.[140] Ова околност не мора имати искључиво нега-

[138] Boczek, стр 239.

[139] Споразум о забрани тестирања нуклеарног оружја у атмосфери, свемиру и под водом (1963. год), Споразум о принципима о руковођењу активностима у истраживању и употреби свемира, укључујући Месец и друга космичка тела (1967. год), Конвенција о међународној одговорности за штету узроковану свемирским објектима (1972. год), Конвенција о регистрацији објеката лансираним у свемир (1975. год) и други.

[140] Keith B. Alexander, "Warfighting in Cyberspace", *Joint Forces Quarterly*, 31. јул 2007, http://www.military.com/forums/0,15240,143898,00.html, *(19.04.2010)*.

тивно значење. Међународно уређено сајбер ратовање може имати предност у односу на ратовање кинетичким оружјем, јер нуди исти резултат уз мање штете. Примена сајбер ратовања неће укинути вођење рата физичком силом, али ће значајно променити природу сукоба који се воде у стању мира, без званичне објаве рата.

Сајбер ратовање доноси и многе ризике. Због повезаности војних и цивилних информационих система многи сајбер напади могу се проширити на цивилне мреже и утицати на неконтролисано ширење сукоба у физичком свету. У том погледу је очување неутралности држава које не учествују у сукобу од изузетног значаја. Нападачи су у прилици да покрећу нападе који нису у складу са међународним правом, пошто технички није могуће доказати идентитет нападача. Иако појава нових средстава и врста ратовања није нова у људској историји, сајбер ратовање ставља велики изазов за међународно право, јер се његова средства и методе технолошки развијају много брже од међународног права. Ипак, сајбер ратовање је специфично и садржи много посебних ситуација за које није могуће наћи одговарајућу аналогију.

Регулисање сајбер ратовања захтева да се на међународном нивоу морају дефинисати надлежности држава, њихових органа и појединаца и одредити заједничке институције и стручна тела за усвајање стандарда у области сајбер ратовања. Поред утврђивања државне одговорности, неопходно је међународноправно дефинисати када сајбер напад достиже ниво оружаног напада. Значење суверенитета у сајбер простору је измењено у односу на традиционално значење у физичком свету. Он у сајбер простору има и активну компоненту, јер захтева и способност државе да ту сувереност ефикасно и оствари.

У погледу очувања неутралности током сајбер сукоба неопходно је обезбедити следеће принципе:

– дефинисати ниво на којем сајбер напад достиже природу оружаног напада,

– успоставити одговорност државе за сајбер напад који су предузели недржавни субјекту у њеној надлежности,

– дефинисати стандарде и обавезе за међународну сарадњу у кризним ситуацијама и ради откривања нападача,

– забрану сајбер напада на цивилну инфраструктуру уз успостављање принципа одрицања држава на право „првог сајбер напада“,

– забрану активности у току мира које се односе на припрему бојног поља постављањем прикривеног софтвера и хардвера на цивилној инфраструктури потенцијалних противника и употребе сајбер оружја у цивилној инфраструктури са одложеним дејством,

– забрану измене података или оштећење мрежа хуманитарних, медицинских, финансијских и других цивилних институција у време мира или рата,

– успостављање стручних међународних тела за усвајање стандарда, размену информација, иницијативу за развој сајбер простора, пружање помоћи државама у кризним ситуацијама, техничко-стручну арбитражу у међународним инцидентима и решавање спорова и доношење међународно надлежних судских одлука у овој области,

– забрану сваке злоупотребе капацитета неутралних држава за вођење сајбер ратовања,

– успостављање међународног система присиле на нивоу УН у случају кршења споразума.

Чињеница да поједине војне активности, попут сајбер ратовања, нису посебно регулисане, не подразумева да оне могу бити употребљене без одређених ограничења. Једно од основних правила ратног права гласи да право зарађене стране у сукобу да изабере средство или метод вођења рата није неограничено. Ако се сајбер ратовање употреби против непријатеља ради изазивања штете, тешко се може порећи да оно није облик ратовања.[141]

Анализа случаја сајбер ратовања у контексту постојећих прописа о неутралности који се примењују на копнено, поморско и ваздушно ратовање, показује заједничке чиниоце и разлике. Обавеза неутралне земље да спречи злоупотребу властите неутралности варира у односу на технолошке могућности. Општи принципи права оружаних сукоба важе у свим ситуацијама, па и у случају сајбер ратовања. Међутим, његова специфична природа не омогућава њихову примену у пракси. Узевши у обзир нејасно дефинисање сајбер простора, брз развој технологије и недостатак праксе у ситуацијама сајбер ратовања, било какав детаљан међународни споразум за његово регулисање вероватно би постао застарео у односу на праксу пре него што би постао потпуно употребљив.[142] Још већи ризик представља недостатак икакве регулативе. Многе државе примењују сајбер ратовање и регулишу га националним доктринама на начин како то њима одговара. Државни суверенитет је суштински већ нарушен самом чињеницом да информације слободно пролазе њихове границе без икаквих препрека. Наведено показује значај потребе да се што пре усвоје међународни споразуми који ограничавају и делом забрањују сајбер ратовање у околностима које опасно угрожавају међународну безбедност, међу којима је један од најважнијих нарушавање неутралног статуса држава које не учествују у сукобу. Они морају бити специфични, али и довољно општи како би задржали способност примене у дужем периоду, имајући у виду брзе технолошке промене информационих технологија. Фокус анализе природе сајбер напада мора се ставити на последице напада и намеру нападача, а не на методе и средства којима су они остварени.

Литература

1 Korns S., Kastenberg, J.: „Georgia's Cyber Left Hook", *Parameters*, U. S. Army War College's quarterly publication *,* Winter 2008–2009, Volume 38, No. 4, страна 60–76.

2 Boczek, B.: *International Law: A Dictionary*, Scarecrow Press, Lanham, Maryland, 2005.

3 Barkham, J.: „Information Warfare and International Law on the Use of Force", *International Law and Politics,* Issue 34, New York University School of Law, 2002, страна 57–113.

4 Sinks, M. A.: *Cyber Warfare and International Law*, unpublished research paper, Air University, Air Command and Staff College, Maxwell AFB, Alabama, 2008.

5 Joyner, C., Lotrionte, C.: „Information Warfare as International Coercion: Elements of a Legal Framework", *European Journal of International Law* 12, No. 5, 2001, страна 825–865.

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

[142] Пример за овакву тврдњу могла би бити међународна Декларација о забрани испуштања пројектила и експлозива из балона, из 1907. Та декларација је још увек важећа за 28 држава првобитних потписника (вероватно и више ако се узму у обзир њихови правни наследници).

6 Sharp, W. G., „Cyberspace and the Use of Force“, Aegis Research Corp., Falls Church, Virginia, 1999.

7 Komov, S., Korotkov, S., Dylevski, I., Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law, *ICTs and International Security*, www.unidir. org, 2007. www.unidir. org/pdf/articles/pdf-art2645.pdf, [цитирано: 16. новембар 2010].

8 Rausher, K., Yaschenko, V., *Russia-U. S. Bilateral on Cybersecurity: Critical Terminology Foundations*, EastWest Institute, Институт проблем информационной безопасности, 26 April 2011, http://www.ewi. info/russia-us-bilateral-cybersecurity-critical-terminology-foundations, [цитирано: 28. април 2011].

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

10 Walker, G., „Information Warfare and Neutrality”, *Vanderbilt Journal of Transnational Law,* Vanderbilt University, Vol. 33, No. 5, 1 November 2000, страна 1079.

11 Queguiner, J. F., Commentary on the Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem (Protocol III). *International Review of the Red Cross.* March, 2007, Vol. 89, Issue 865, страна 175–208.

12 Klimburg, A., Mobilising Cyber Power, Survival, February-March, 2011, 53:1, страна 41–60.

13 Greenberg L., Goodman, S., Soo Hoo, K., *Information Warfare And International Law*, National Defense University, Institute for National Stategic Studies, 1997, поглавље 2, страна 7–12 и поглавље 3, страна 21–33.

14 Schmitt, M., Dinnis, H., Wingfield, T., „Computers And War: The Legal Battlespace“, Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge, June 25–27, 2004, Program on Humanitarian Policy and Conflict Research at Harvard University,

http://www.ihlresearch. org/ihl/pdfs/schmittetal. pdf, [цитирано: 21. јул 2011].

15 Jensen, T.„„Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self. Defense“, Stanford Journal of International Law, Vol. 38, 2002, страна 207.