НЕНАД ПУТНИК *
МИЛИЦА БОШКОВИЋ
Универзитет у Београду
Факултет безбедности
Београд

УДК 316.48:004.49
Монографска студија
Примљен: 26.04.2013
Одобрен: 03.05.2013

САВРЕМЕНИ БЕЗБЕДНОСНИ ИЗАЗОВИ – ХАКТИВИЗАМ КАО НОВИ ОБЛИК ДРУШТВЕНОГ КОНФЛИКТА

Сажетак: Безбедност рачунарских мрежа и, уопште, информационих инфраструктура данас није више само технички проблем него и важно стратешко питање. Услед распрострањености и децентрализованости глобалне рачунарске мреже као и непостојања правне регулативе која би регулисала сајбер ратовање, активност хактивиста - својеврсне сајбер гериле - постала је један од важних проблема сајбер безбедности и додатно нагласила значај заштите информационих система, спровођења међународних истрага, екстрадиције и кажњавања извршилаца. Феномен хактивизма постоји око петанест година, погађао је различите државе на различитим континентима, али до данас није пронађено адекватно и општеприхваћено решење за сузбијање ове непожељне појаве. Овај рад настоји да са аспекта сајбер безбедности опише феномен хактивизма, размотри његове импликације по националну безбедност држава, као и да пружи критички осврт на актуелне проблеме и стратегије који су везани за супротстављање овој појави.

Кључне речи: хактивизам, сајбер безбедност, сајбер ратовање, национална безбедност, међународно право

Увод

Савремено друштво постало је зависно од информационо - комуникационих технологија. Ова зависност изнедрила је и нове безбедносне ризике и претње који се у великој мери разликују од оних који су постојали у прошлости.

* nputnik@fb.bg.ac.rs

Са етиолошког аспекта, нови облици безбедносних претњи информационом друштву евидентирају се од почетка деведесетих година прошлог века, када је интернет постао широко доступан, тј. пуштен у комерцијалну употребу. Нове претње су представљене физичким и софтверским угрожавањем информационе инфраструктуре, али и све чешћом злоупотребом сајбер простора за различите субверзивне активности. Појављивање нових, специфичних безбедносних претњи крајем XX и почетком XXI века омогућено је постојањем „слабих тачака" типичних за информационо комуникационе технологије, са једне стране, а, са друге стране, постојањем субјеката спремних и способних да ове технологије злоупотребе у властиту корист. Сајбер простор, „виртуелни свет", на тај начин је постао не само циљ напада већ и моћно средство у рукама различито мотивисаних корисника информационо - комуникационих технологија.

Безбедносне претње информационом друштву разноврсне су и специфичне по томе што су превасходно усмерене на злонамерно дестабилизовање информационих система. Онемогућавање нормалног функционисања информационих система у друштву које је од њих постало зависно може имати врло озбиљне последице на све сфере друштвеног живота. Последице могу бити чак и фаталне уколико се угрозе поједине инфраструктуре, као што су, на пример, системи за контролу копненог и ваздушног саобраћаја, хидроцентрала, нуклеарних електрана, безбедносних и здравствених служби или, пак, за дистрибуцију електричне енергије.

Нове технологије нису само изнедриле нове претње већ су и отежале способност идентификовања актерâ безбедносних претњи и њиховог разликовања. Актери претњи у новом амбијенту, сајбер простору, могу бити различити – државни, поддржавни и транснационални субјекти. То су најчешће злонамерни појединци, криминалне групе, терористичке организације, привредни субјекти, али и државе и њихове институције (националне армије и обавештајне службе), са различитим мотивима за деструктивно деловање: економским, политичким, идеолошким, религијским или војним.

Сједињене Америчке Државе биле су прва земља која је, у опширнијем преиспитивању националне безбедности након формалног завршетка биполарне поделе света, отворила дискусију о постојању сајбер ризика. Такозвана сајбер претња је, од настанка идеје деведесетих година двадесетог века, сматрана једним од могућих „асиметричних" инструмената противничких земаља, идеолошки мотивисаних група и међународних терористичких организација које нису у стању да се војно

конфронтирају са Сједињеним Америчким Државама.У случају да се остваре, ове претње би могле резултовати погубним прекидима основних функција државе. Безбедносне претње у сајбер простору тиме су стекле статус проблема националне безбедности. Расправа се касније ширила, иако са различитим акцентима, у свим технолошки развијеним земљама, заузевши последњих година значајно место и у међународним безбедносним политикама под називом сајбер безбедност.

Генеза парадигме и појмовно одређење сајбер безбедности

Етимолошки посматрано, корени појма *сајбер безбедност* сежу у шездесете године прошлог века и везују се за простор САД. У том периоду је третирана *комуникациона безбедност* (*Communication Security* - COMSEC). Са појавом компјутера, седамдесетих година прошлог века, настала је *компјутерска безбедност* (Computer Security - COMPUSEC). Већ осамдесетих година XX века, услед инцидената као што су били *Кукавичје јаје* (Cuckoo's egg) и *Морисов црв* (Morris worm), увидело се да мрежа састављена од великог броја рачунара може бити искоришћена за злонамерне циљеве. Тада долази до интеграције комуникационе и компјутерске безбедности, те настаје појам *информациона безбедност* (*Information Security* - INFOSEC). Информациона безбедност је интегрисала раније одвојене дисциплине, као што су безбедност персонала, компјутерска безбедност, комуникациона безбедност и оперативна безбедност. Већ у том тренутку информациона безбедност је постала један од четири камена темељца националне безбедности САД, поред дипломатије, економије и војне компоненте (Синковски, 2005:34).

У овом тренутку не постоји општеприхваћена дефиниција термина сајбер безбедност, те му се често додељују различита значења. Најраспрострањеније је схватање по којем се сајбер безбедност поистовећује са поменутом информационом безбедношћу, која се односи на заштиту информација и информационих система од улаза, коришћења, ширења, прекида услуга, неауторизованих измена или уништавања, са циљем гаранције њихове поверљивости, интегритета и расположивости. Акценат информационе безбедности стављен је на спречавање неауторизованог приступа информационим системима. Са овог становишта, превасходно се разматра *поверљивост* (енгл. *confidentiality*) информација.

Према другом, новијем, схватању (насталом деведесетих година прошлог века) термин *сајбер безбедност* се поистовећује са термином *информационо обезбеђење* (енгл. Information assurance - IA). Информа-

ционо обезбеђење дефинисано је од стране *Националне агенције за безбедност САД* као скуп мера за заштиту и одбрану информација и информационих система обезбеђивањем њихове расположивости, интегритета, аутентичности, приватности и неопозивости. Оно укључује мере за бекап (енгл. backup) система, његову заштиту, детекцију упада у систем и реакцију на нападе.

У наведеном становишту термин *обезбеђење* представља ниво поверења који је пропорционалан ефикасности додатних мера безбедности. Увођење овог термина на неки начин сведочи о промени „гранитног" концепта безбедности, типичног за традиционалне информационе системе, који нису били повезани у мрежу, ка флексибилнијем концепту безбедности, који, са једне стране, подразумева да се природа сајбер простора супротставља достизању апсолутне сигурности, а који је, са друге стране, одмерен вредношћу информације и уређаја које треба заштитити (Синковски, 2005).

Напредак у рачунарској техници и начинима умрежавања рачунарских система проширио је, дакле, у односу на концепт информационе безбедности, листу својстава информација пред које се постављају безбедносни захтеви. Са становишта информационог обезбеђења значајно је задовољавање следећих својстава информација (или безбедносних сервиса информација и информационих система): *приватност* или *поверљивост* (енгл. *privacy, confidentiality*), *интегритет* (енгл. *integrity*) и *расположивост* (енгл. *availability*). Њима се понекад додају још два: *аутентичност* (енгл. *authentication*) и *неопозивост* (енгл. *non-repudiation*).

Циљ *приватности* је да дозволи приступ информацији искључиво ауторизованим лицима, процесима или програмима. *Поверљивост* информације може бити везана за разлоге националне безбедности (на пример, информације о наоружању), индустријске безбедности (на пример, пројекти неког новог производа) или личне приватности корисника.

Интегритет тежи да осигура да информације и ресурси који њоме управљају (хардвер и софтвер) могу бити модификовани или уништени само уз посебну и претходно дефинисану ауторизацију.

Циљ *расположивости* се састоји у томе да информације и услуге које су са њом повезане буду у сваком тренутку доступне ауторизованим корисницима. Другим речима, систем који даје такве услуге треба да функционише само када се то од њега захтева, и то у ограниченом и унапред одређеном времену. Са оперативнога гледишта, *расположивост* се односи на прихватљиво време одговора система и прикладног

нивоа услуге. Са гледишта безбедности информације, међутим, *расположивост* представља способност заштите од штетног догађаја или могућност бекапа система у случају када се нежељени догађај већ десио. Расположивост савремених информационих система, који су у стању непрекидне активности, неопходна је како за нормално извршавање активности информационог друштва тако и за безбедност људских живота (довољно је поменути, на пример, системе који регулишу авионски саобраћај или аутоматизоване уређаје у операционој сали).

Аутентичност је мера безбедности која тежи да одреди вредност и валидност преноса, поруке или пошиљаоца. Овом мером се, такође, контролише и ауторизација корисника да прими специфичне категорије информација.

Неопозивост је мера безбедности чији је циљ да осигура ток комуникације. Њоме се постиже да пошиљалац информације има доказ о њеној испоруци, али и да прималац информације има податак о идентитету пошиљаоца, тако да ниједан од учесника у преносу касније не може негирати извршену трансакцију.

Степен важности наведених својства информација, са безбедносног становишта, варира у зависности од контекста у којем се размена информација врши. У војним системима, на пример, највећа пажња се посвећује поверљивости информација, док се у банкарским трансакцијама акценат ставља на интегритет.

Иако не постоји општеприхваћена дефиниција сајбер безбедности, можемо закључити да су појмови *информациона безбедност* и *информационо обезбеђење* укључени у шири концепт сајбер безбедности.

Потреба за развијањем концепта сајбер безбедности, на међународном плану, била је посебно наглашена у *Декларацији о принципима,* која је донета на *Светском самиту о информационом друштву* 2003. године. У одељку Декларације који је посвећен *Изградњи поверења и безбедности у коришћењу ИКТ* наводи се да је за развој информационог друштва и стварање поверења између корисника ИКТ неопходно јачање међусобног поверења, као и безбедности информација и компјутерских мрежа, аутентичности, приватности и заштите корисникâ. Истиче се потреба за промовисањем, развијањем и имплементацијом глобалне културе сајбер безбедности, кроз сарадњу свих доносилаца одлука и међународних експертских тела. Овај напор би требало да буде подржан кроз повећање међународне сарадње. У оквиру глобалне културе сајбер безбедности важно је повећати безбедност и осигурати заштиту података и приватност корисника, паралелно са повећањем могућности приступа и трговине. Ове активности, према Декларацији, морају

узети у обзир и степен социјалног и економског развоја сваке земље и поштовати развојно оријентисане аспекте информационог друштва (*Declaration of principles building the Information Society: a global challenge in the new millenium*, 2003).

Слична декларација, која је била предложена у резолуцији Уједињених нација из децембра 2002. године, такође је одражавала убеђење да су поверење и безбедност темељ информационог друштва (*Plan of action*, 2003). У резолуцији 57/239, из децембра 2002, Генерална скупштина УН промовисала је елементе за стварање глобалне културе сајбер безбедности, позивајући земље чланице и све међународне организације да узму у обзир те линије водиље у припреми Самита о информационом друштву. У децембру 2003. резолуција 58/199 још једанпут је подвукла неопходност промовисања глобалне културе сајбер безбедности и заштите критичних инфраструктура.

Појам сајбер безбедност данас означава скуп активности, мера и техника осмишљених да заштите од напада, прекида сервиса (услуга) и осталих претњи рачунаре, мреже рачунара и информације које они садрже или размењују, као и софтвер, податке и остале елементе сајбер простора. Према томе, овај појам реферира на обједињене напоре и покушаје, који укључују истраживања и анализе, са циљем да се осмисле нове и побољшају постојеће активности везане за безбедност сајбер простора и ниво његове заштите од претњи и сајбер претњи.

Концепт сајбер безбедности подразумева холистички приступ у истраживању и супротстављању претњама информационим системима - са позиција информатичких и математичких наука и њихових посебних дисциплина (као што су криптографија и криптоанализа), војних, правних, криминалистичких и криминолошких. Под овим појмом, дакле, подразумева се један широк, обухватан приступ проблему заштите информационе инфраструктуре од безбедносних претњи. Историјски посматрано, концепт сајбер безбедности је проистекао из страха од могућег угрожавања националне безбедности путем нарушавања функционалности информационе инфраструктуре једне државе. Овај приступ, данас прихваћен на наднационалном нивоу, захтева синергијску активност свих субјеката у међународној заједници, уз примарну улогу експерата на пољу информатичких наука, у циљу достизања безбедног сајбер простора. Превентивне активности на усвајању хардверских и софтверских стандарда, оснивању националних и наднационалних експертских тела, побољшању међународне сарадње у овој области и усаглашавању националних закона у области сајбер криминала јесу неопходни кораци у

побољшању безбедности сајбер простора (Кешетовић & Путник, 2012, ин принт).

Сајбер безбедност се, према томе, не може одвојити од општег контекста у коме функционише информационо друштво. Она обухвата широки спектар активности и мера, те представља комплексан систем, с обзиром на то да обједињава различите, подједнако важне аспекте. Таква комплексност чини тешким достизање апсолутне сигурности. Није могуће потпуно елиминисати ризик од неадекватног, случајног или намерног, коришћења инструмената информационог доба. Сајбер безбедност је, дакле, изнад свега управљање ризиком, непрестано трагање за компромисом између вредности онога што треба заштитити, нивоа заштите и цене заштите (*Vulnerability Disclosure Framework – Final Report and Recommendations by the Council*, 2004).

Механизми за смањење ризика уобичајено се дефинишу као *противмере* (законске, процедуралне, техничке, физичке итд.). У идеалној ситуацији ризик би се могао потпуно елиминисати усвајањем довољног броја противмера. На жалост, оне имају и економске трошкове и ограничења коришћења заштићених ресурса. Дакле, врло ретко се комплетна елиминација ризика показује као исплатива и практична. Реалистичнији приступ подразумева сманење ризика до прихватљивог нивоа.

Шта се подразумева под прихватљивим ризиком? Одговор варира од особе до особе, од ситуације до ситуације. У оквиру једне организације прихватљиви ризик најчешће одређује руководство, док на нивоу државе ова одговорност лежи на влади.

Однос парадигме сајбер безбедности и националне безбедности

Комплексност сајбер претњи и могуће последице које могу произаћи из угрожавања сајбер простора за безбедност државе и становништва, уврстили су питања сајбер безбедности међу легитимна питања националне безбедности.

Са аспекта националне безбедности, пак, од суштинског значаја су одговори на следећа питања: Може ли се проблем решити уколико не познајемо његове суштинске узроке? Ко су актери безбедносних претњи, какви су њихови циљеви и који их мотиви покрећу? Јесу ли то појединци, организације или државне структуре? Да ли је угрожавање безбедности сајбер простора последица само супротстављених и противречних интереса актера у сајбер простору или је оно последица и њихо-

вих различитих вредносних перцепција? Није ли сајбер простор постао универзално доступно бојно поље, поприште сукоба, које предочава сву комплексност односа проистеклих из процеса глобализације и њених последица?

Приступ овом сложеном проблему са позиција националне безбедности захтевао би идентификацију, класификацију и исцрпну анализу не само претњи уперених ка сајбер простору, већ и свих субјеката претњи, тј. њихових актера. На садашњем степену тематизације овог проблема, и у оквирима овог рада, то није могуће учинити. Управо из тог разлога, уважавајући основна епистемолошка начела, у раду смо се усредсредили на исцрпну дескрипцију једног веома значајног појавног облика угрожавања националне безбедности - хактивизма, у циљу формирања полазне грађе за будућа истраживања.

Појмовно одређење и генеза хактивизма

Хактивизам је специфичан вид хакерског деловања, који се, због прокламованих циљева и изабраних објеката напада, може сврстати под облик герилске борбе. Реч је о новом облику герилске борбе која се води на електронском пољу или, другачије речено, о идеолошки мотивисаним групама чије је деловање усмерено против електронских контролних и информационих система и технологија непријатељских земаља. Хактивисти у сајбер простору виде инструмент којим недржавни актери могу да учествују у конфликтима ван националних граница. Према њиховим етичким начелима не могу само државе бити овлашћене за започињање ратова или агресије. За разлику од државе, „хактивисти се не сматрају ограниченима законом о оружаном конфликту или Повељом Уједињених нација“ (Denning, 2001).

Хактивисти користе исте методе и технике као и хакери, с тим што је њихов примарни циљ да сајбер нападом привуку пажњу јавности на одређени друштвени или политички проблем. Пример најпростије форме хактивизма би представљао напад на сајт чији садржај нападач перципира као противан личним политичким убеђењима, мењањем почетне странице сајта (defacement) – истицањем видљиве поруке која је отворено у контрасту са вредностима које заступа дотични сајт. У многим случајевима нападач и блокира сајт, најчешће нападом типа DoC. Хактивизам пружа многе предности, првенствено визибилност по ниској цени, без географских ограничења и без потребе за излажењем на улицу и јавним демонстрирањем. Данас је овај облик „електронске ге-

риле“ у широкој употреби од стране великог броја друштвених група и индивидуалних политичких активиста на свим континентима. У зачетку, њихова активност евидентирана је у Великој Британији, Аустралији, Индији и Кини (Wray, 1998).

Хактивизам постаје запажени вид грађанске непослушности средином 1990-их година прошлог века. У пролеће 1998. године британски хакер под псеудонимом „JF“ неовлашћено је изменио почетне странице на скоро 300 Интернет сајтова. Оригиналне садржаје он је заменио сликом облака у облику печурке и текстом: „Ово масовно изобличавање (defacement) посвећено је свим оним људима који желе да виде мир у свету“. Међу нападнутим сајтовима били су сервери индијског Центра за атомска истраживања и Саудијске краљевске породице (Главе, 1998). У том тренутку, то је био највећи напад ове врсте. Од тада, евидентирани су бројни случајеви неовлашћеног приступа сајтовима чији се садржај замењује другим, политичким, садржајем.

Временом хактивисти почињу да користе различите алате и технике за извршење напада на информационе ресурсе противничких држава. О томе сведоче резултати истраживања о њиховој активности у Србији, 1999. године, током конфликта између НАТО-а и Србије и Црне Горе. Најагилније су биле две хактивистичке групе, *Црна рука* и *Српски анђели*, чији су чланови нападали електронске базе података америчких, британских и албанских обавештајних, војних и државних служби, те присвајали, мењали и брисали одговарајуће информације. Поменимо и занимљиву чињеницу – без претензија да се бавимо дубљом анализом његових политичких и социјалних узрока – да је овај вид деловања врло брзо попримио озбиљније размере, претећи да прерасте у први електронски рат: српске групе су добиле подршку руских хакера, а након бомбардовања кинеске амбасаде у Београду, придружиле су им се и кинеске хакерске групе. Удружено деловање хакерских организација онеспособило је на неколико недеља важне америчке војне информационе системе, што је довело до развоја догађаја са неочекиваним последицама: америчка служба ФБИ покренула је велику „контраофанзиву“ у циљу подизања нивоа заштите рачунарских система, при чему су ухапшене десетине америчких хакера. То су америчке хакерске групе схватиле као објаву рата, па су и саме почеле да учествују у акцијама против служби властите државе (Путник, 2009:124). Да се по наведеним, апстрахованим диференцијалним карактеристикама – начину настанка, организацији, циљевима и борбеној тактици – хактивистичка и војна герила практично не разликују (Милашиновић, Путник, 2007) сведоче објаве и прогласи хактивиста: „*Црна Рука је устала у ‘електронску од-*

брану' интереса ове земље и не одустаје од напада на сајтове који пласирају лажи о ситуацији у овој земљи", и даље, припадници *Црне руке* тврде да се залажу за „*мир, љубав и благостање на целој планети*", а као доказ прилажу чињеницу да „*никада нису непотребно обрисали податке, иако су били у прилици*" (Дингарац, Станчевић,1998). „Нова герила" се, према томе, ограђује од хакера чији је циљ искључиво малициозно и деструктивно деловање усмерено према „обичним" корисницима Интернета, већ заступа поменуту идеологију националног ослобођења, промовишући при том пацифистичку идеју општег мира и поштујући етичко начело ненаношења штете неутралним корисницима електронских ресурса.

Хактивистички напад на Естонију 2007. године је представљао својеврсну прекретницу у перцепцији претње хактивизма и подстакао је интензивне расправе о безбедности сајбер простора на међународном нивоу. Да подсетимо, напад који је почео 27. априла 2007. године, био је усмерен на опструкцију званичних интернет-сајтова Естоније, једне од најинформатизованијих земаља на свету. Током неколико недеља, колико је трајао напад, Естонија се носила са по обиму најширим нападом ове врсте до тада. Сајтови естонске владе (министарства иностраних послова и министарства правде), медија и банака били су блокирани услед напада за који су окривљени руски хакери. У изјави коју је том приликом дао медијима естонски министар одбране захтевао је примену члана 5 НАТО-а, који предвиђа колективну одбрану нападнуте земље (*BBC NEWS*, 2. 5. 2007; *The Economist*, 10. 5. 2007; *Telegraph*, 19. 5. 2007). Ово је, дакле, био први случај директног угрожавања суверенитета државе рачунарским нападом, који је био спроведен од стране недодирљивог непријатеља.

Само годину дана након што је оптужена за ове нападе, Русија је у августу 2008. године поново оптужена за извођење сајбер напада на Грузију. У новембру 1989. Јужна Осетија је прогласила аутономију од Совјетске Социјалистичке Републике Грузије. Од тада, новонастала држава има напет однос са Грузијом који се коначно претворио у оружани сукоб. Да би поново успоставила контролу, Грузија је 8. августа 2008. године покренула војну офанзиву против отцепљене Јужне Осетије. Будући да већина грађана Јужне Осетије има руски пасош, Русија је на потез Грузије одговорила слањем тенкова да би одбранила оне које сматра својим грађанима. Док су се осетијске, грузијске и руске трупе борile на земљи, сукоби су се разбуктали и на WEB-у. Резултати сајбер-форензичке анализе, спроведене након конфликта, показали су да су за поменути сајбер конфликт одговорни хактивисти − руски и грузијски

националисти, појединци и групе који су личним ангажманом желели да пруже подршку својој земљи (Ifrah, 2008:2.; Tikk et al., 2008).

Проблем супротстављања хактивизму

Наведени догађаји су показали да су сајбер напади постали веома популарно средство асиметричног ратовања у савременим околностима. Земље са нижим нивоом зависности од нових технологија не само да су мање рањиве, већ могу да искористе рањивост развијенијих земаља за достизање својих стратешких циљева. Исти принцип важи и за појединце и за колективне субјекте у сајбер простору. Могућност извршавања деструктивних акција је, са економске тачке гледишта, све доступнија. Развијање офанзивних стратегија у сајбер простору не захтева високе инвестиције, попут оних неопходних за конвенционално ратовање и, изнад свега, ове стратегије доступне су великом броју актера. За разлику од технолошки софистицираног оружја, сајбер оружје могу развијати појединци или групе за шта су им једино потребни знање и мотивација. То омогућава државама или актерима којима до сада није придаван значај у стратешком контексту, да теже другачијој позицији у сајбер простору, где знање одређује равнотежу моћи пре него количина војног арсенала.

Осим тога, у сајбер простору је мање изражена веза између безбедности и територије. Геополитичка позиција која је одувек била централни, средишњи, елемент безбедносне политике државе постепено губи свој значај. Данас није више неопходно физички ући у неку територију, нити је напасти кинетичким оружјем. Дакле, комплетна контрола физичких ентитета као што су ваздушни или копнени простор није довољна да гарантује безбедност једној држави. Војна надмоћ не значи сигурност у сајбер простору где је неопходно развити нове стратегије одбране сајбер инфраструктуре, што је посебно тешко због типичног амбигвитета сајбер напада. Уколико је сајбер напад извршен професионално, врло је тешко одредити порекло извршиоца и мотивације из више разлога:

- сачувати анонимност у сајбер простору је технички врло лако;
- напад се може извршити из било ког дела света или, ако је неопходно, и са више тачака у исто време;
- последице напада се могу манифестовати након дужег временског периода, спречавајући тако откривање средстава и актера;

- време између откривања нове рањивости и стварања офанзивних информатичких инструмената који се могу применити за извршење напада све је краће, захваљујући усавршавању моћи рачунара;
- технологија која се користи за нападе релативно је једноставна за коришћење и врло је економична;
- инструменти и технике за извршавање напада могу се лако наћи у сајбер простору;
- учинковитост напада је све већа захваљујући аутоматизацији и софистицираности метода напада – само један напад може изазвати тешке последице.

Претња сајбер напада није лако уочљива нити се актери претње могу лако категоризовати. Првенствено, не постоји јасна идентификација актера – сваки члан „електронске друштвене заједнице“ је потенцијални противник. Непријатељске државе, војни савези, терористи, незадовољни радници, обесни појединци, комерцијална или индустријска предузећа, политички активисти и криминалне организације само су примери могућих актера. Сваки од ових актера мотивисан је различитим циљевима, ограничен различитим нивоима ресурса, сопственим могућностима и могућностима система да се брани. Тешко је пронаћи евидентне доказе у вези са непријатељским намерама могућих нападача и проценити њихове реалне способности да изведу напад на тако широком нивоу да угрозе безбедност државе.

Хипотетички гледано, у случају да довољно велика група хактивиста синхронизовано покрене електронски напад који би циљао војну критичну инфирмациону инфраструктуру једне државе, величина штете била би огромна. У таквој ситуацији би било тешко идентификовати правог актера напада, тј. разликовати хактивистички напад од почетне фазе напада у оквиру војне кампање сајбер ратовања.

Ако се у обзир узму катастрофалне последице које сајбер напади могу изазвати, од виталног је значаја да државе буду оспособљене да ефикасно одбране своју критичну инфраструктуру. Једна од стратегија за ефикасно супротстављање сајбер нападу је употреба слојевитог система одбране, састављеног од мера пасивне и активне одбране (спровођење електронског контранапада) (Склеров, 2009). У пракси, међутим, државе намерно бирају искључиво мере пасивне одбране, најчешће из страха да би коришћењем мера активне одбране прекршиле међународно ратно право. Метју Склеров, капетан Морнарице САД, сматра да према међународном праву државе имају право да:

- тумаче сајбер нападе као чинове рата, а не само као кривична питања, те да у складу са тим и одговоре на њих;

- користе мере активне, а не само пасивне одбране против рачунарских система других држава, без обзира на то да ли су те државе иницирале напад или су само занемариле своју обавезу да спрече сајбер нападе који долазе са њихове територије (Склеров, 2009:2).

Склеров сматра да је страх од употребе мера активне одбране спутавајући и штетан по државе из два разлога. Прво, будући да се мере активне одбране сматрају видом примене електронске силе, одбрана рачунарских система државе бива препуштена само мерама пасивне одбране, што доводи до слабљења дефанзивне позиције државе. Друго, оно приморава државе да се ослањају на домаће кривичне законе како би се одбраниле од сајбер напада, што је неефикасно јер је неколико великих држава (међу којима су Кина и Русија) невољно да спроведе екстрадицију или кривично гоњење нападача. Прихватањем оваквог, преовлађујућег тумачења међународног ратног права, државе се могу наћи у „одбрамбеној кризи“ током сајбер напада јер су принуђене да одлуче између ефикасних, али правно спорних мера активне одбране и мање ефикасних, али легалних мера пасивне одбране и кривичних закона.

Одбрамбену кризу, више од било чега другог, компликује атрибуциони захтев (одговорност за напад) јер је у пракси немогуће било коме приписати одговорност за сајбер напад током његовог трајања. Иако нападнута држава може лоцирати сервере у другој држави са којих су упућени сајбер напади, утврђивање идентитета нападача захтева интензивну и дуготрајну истрагу током које је неопходна сарадња државе из које је напад иницран. Будући да међународно ратно право забрањује употребу силе све док се не докаже да напад може бити приписан некој држави или њеним актерима (тим пре што пракса показује да је велики број сајбер напада изведен од стране хактивиста) не изненађује чињеница да су државе невољне да третирају сајбер нападе као чинове рата и ризикују кршење међународног ратног права.

Стратегија капетана Склерова је веома оригинална и фундирана на прагматичким принципима, али и заснована на једном смелом и прилично слободном тумачењу међународног права. Међународно ратно право је састављено од добро познатих и прихваћених принципа, али примена тих принципа на сајбер нападе представља тежак задатак. Потешкоће настају из чињенице да се међународно ратно право развило, већим делом, као одговор на „класичне“ међудржавне ратове. Из парадигме традиционалних оружаних сукоба релативно је једноставно проценити обим напада и открити идентитет нападача. Међутим, током

сајбер напада, нападнутој држави је тешко да процени обим напада, као и да закључи ко је за њега одговоран.

У претходним одељцима рада смо поменули да се активност хактивиста може посматрати као нови облик герилског ратовања. Данас је, након дугог периода спорења, герилска борба призната са становишта међународног ратног права. Допунским Протоколом I из 1977. године озакоњен је статус борца и припадницима ослободилачких покрета за самоопредељење, чиме је и ова категорија учесника у оружаним сукобима стављена под ингеренције међународног ратног (хуманитарног) права. Истим Протоколом признат је карактер оружаног сукоба „борби за самоопредељење народа против колонијалне доминације и стране окупације, као и против расистичких режима". Према оцени највећег броја делегација, учесника на Дипломатској конференцији у Женеви, усвајање оваквих решења представљало је њено највеће достигнуће и историјску прекретницу у развоју хуманитарног права. И поред тога, питање сајбер гериле и правног статуса бораца у сајбер конфликтима до сада није било предмет разматрања међународног ратног права.

У међународном ратном праву још увек није пронађена адекватна дефиниција за активности које се конвенционално називају сајбер ратовањем, иако се оне спроводе већ дуги низ година. У овом тренутку, дакле, не постоји свеобухватни међународни споразум који би регулисао сајбер нападе, нити пружио неку правну дефиницију чина сајбер агресије. Повеља Уједињених нација одређује када суверена држава може да употреби силу у циљу самоодбране од чина агресије, али се то у потпуности односи на традиционално схваћени оружани сукоб. Ни други споразуми које познаје међународно право, попут *Споразума о нешириењу нуклеарног наоружања*, *Међународног космичког права*, *Система антарктичке повеље*, *Конвенције УН о праву мора* и *Уговора о узајамној правној помоћи (MALT)* не представљају адекватне моделе који би се могли употребити за регулисање проблема сајбер напада (Shackleford, 2009). Заправо је целокупно поље сајбер права још увек недовољно развијено.

Закључна разматрања

Парадигма сајбер безбедности реферира на обједињене напоре и покушаје, који укључују истраживања и анализе, са циљем да се осмисле и побољшају активности везане за безбедност сајбер простора и ниво његове заштите од разноврсних претњи. У том смислу, стратегија капе-

тана Склерова представља један оригиналан приступ у елаборацији проблема супротстављања сајбер ратовању и несумњив научни допринос тероији сајбер безбедности.

Идеја да се обухват међународног права прошири на сајбер свет, да се утврде одговорности државе за сајбер нападе и њене дужности да спречи сајбер нападе који потичу са њене територије би свакако допринела супротстављању хактивизму, уколико би се постигао међународни консензус у таквом тумачењу међународног права. Међутим, у пракси таквог консензуса нема, нити ће га бити у скоријој будућности. Основни разлог непостојања консензуса јесте у томе што велике суперсиле (Русија, САД и Кина) заговарају различите приступе у начину решавања проблема сајбер ратовања.

Москва се, у складу са властитим интересима, залаже за склапање билатералних или мултилатералних споразума о некоришћењу рачунара у сврхе ратовања (слично споразуму о нешириењу нуклеарног, хемијског и биолошког наоружања) и за развој међународног права. САД се, са друге стране, залажу за то да Русија и Кина потпишу Конвенцију и сајбер криминалу и да, на основу ње, процесуирају хактивисте који делују са њихових територија.

Можемо закључити да је појава хактивизма, као феномена који представља проширење делокруга сајбер ратовања изван војних активности, у техничком смислу омогућена дифузном и децентрализованом структуром глобалне рачунарске мреже – Интернета. Сваки корисник рачунара је слободан да се у сајбер простору понаша у складу са властитим политичким уверењима и да учествује у псеудо-војним акцијама ван било каквог формалног ланца команде. Суштински, феномен сукобљавања у сајбер простору помоћу оружја које нуди сам сајбер простор, и његово преливање у сфере „цивилног“ света узроковано је противречном природом процеса глобализације и идеолошким, политичким, културним и социјалним диспаритетима које овај процес носи.

Из наведених разлога државе, које су се определиле за пут информатизације својих виталних процеса, морају предузети мере за обезбеђивање властитог „сегмента“ сајбер простора као засебне државне границе. Случајеви Естоније и Грузије су несумњиво показали да суверенитет државе може бити угрожен и из „виртуелног света“.

Повећање проблема који се могу легитимно сматрати питањем националне безбедности, ширење изворâ претњи и починилаца који су у стању да утичу на безбедност држава представљају нове, посебно значајне изазове за аналитичаре и доносиоце политичких одлука. Они морају бити способни да уоче разлику између претњи националној без-

бедности и мање важних проблема. Доносиоци одлука битних за безбедност државе, у присуству реалних претњи, морају бити у стању да идентификују извор, циљ претње и могуће последице, као и да омогуће пружање најефикаснијих одговора, а све то у стратешком контексту, који сваког дана постаје све комплекснији.

Са аспекта националне, али и регионалне и глобалне безбедности, разумљива је теза по којој се безбедан сајбер простор сматра императивом информационог доба. Не треба, међутим, сметнути с ума да се природа сајбер простора противи стању апсолутне безбедности. Брзина којом се претње увећавају захтева усвајање поузданих, брзих и ефикасних безбедносних мера које треба да буду дискриминишуће према творцима претње.

Досадашња искуства у супротстављању безбедносним претњама у сајбер простору указују на потребу стварања кохерентног делатног оквира који подразумева примену како превентивних, тако и репресивних мера у стварању безбедног сајбер амбијента. Превентивне активности, на првоме месту, подразумевају осмишљавање различитих мера и стратегија заштите информационих система и њихову имплементацију, унапређивање законске регулативе, како на националном тако и на међународном нивоу, као и њихово усклађивање са обавештајним активностима у покушају супротстављања сајбер претњама.

Ефикасан одговор сајбер претњама није могуће пружити само правним мерама. Задовољавајући степен заштите сајбер простора није могуће постићи ни усвајањем и спровођењем техничких мера, већ, изнад свега, формулисањем стратегија заштите и синергијским спровођењем серије противмера од стране међународних организација, државних институција, експертских удружења и индивидуалних корисника информационих система.

Заштитне активности, према томе, морају подразумевати константан напор свих оних који су одговорни за функционисање информационе инфраструктуре. На индивидуалном нивоу, однос корисника према информационим системима може да обезвреди и најсавременије и најскупље хардверске и софтверске безбедносне системе. Сваки корисник, дакле, има важну улогу у унапређивању безбедности сајбер простора. Било који рачунар, уколико није адекватно заштићен, може постати објект и/или средство напада против других рачунарских система. Према томе, промовисање безбедносне културе и развијање компјутерске етике би можда требало сврстати у ред приоритетних активности на пољу превенције не само хактивизма већ безбедносних претњи уопште.

Литература:

1. *Declaration of principles building the Information Society: a global challenge in the new millennium* (2003): World Summit on the Information Society, doc. WSIS-03/GENEVA/DOC/4-E, B5, 35, 2003, http://www.itu.int
2. *Plan of action* (2003): World Summit on the Information Society, doc. WSIS-03/GENEVA/DOC/5-E, 2003, http://www.itu.int
3. Pleskonjić, Dragan., Maček, Nemanja, Đorđević, Borislav, Carić, Marko (2007): *Sigurnost računarskih sistema i mreža*, Mikro knjiga, Beograd
4. *Vulnerability Disclosure Framework – Final Report and Recommendations by the Council* (2004): National Infrastructure Advisory Council, http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf
5. Denning, Dorothy (2001): *Cyberwarriors, Activists and Terrorists Turn to Cyberspace*, Harvard International Review, Vol. XXIII, No. 2, pp. 70–75.
6. Wray, Stephan (1998): *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics*, A paper for The world Wide Web and Contemporary Cultural Theory Conference, Drake University
7. Glave, James, (1998): *Anti-Nuke Cracker Strikes Again*, Wired
8. Putnik, Nenad (2009): *Sajber prostor i bezbednosni izazovi*, Univerzitet u Beogradu - Fakultet bezbednosti, Beograd
9. Kešetović, Želimir, Putnik, Nenad, (2012, in print): *Encyclopedia of Crisis Management*, Entry: Cyber security, Editor: Golson, J. Geoffrey, Penuel, K. Bradley, Statler, Matt, Hagen, Ryan, SAGE Publications, London.
10. Milašinović, Radomir, Putnik, Nenad (2007): *The essence of guerilla as a social conflict, in Guerilla in the Balkans:Freedom Fighters, Rebels or Bandits - Researchingthe Guerrilla and Paramilitary Forces in the Balkans*, Tokyo: University Meiji, Institute for Disarmament and Peace Studies, Beograd: Institut za savremenu istoriju, Fakultet bezbednosti, pp. 327–339.
11. Dingarac, Dušan, Stančević, Tihomir (1998): *Srpski hakeri Crna ruka,* Svet kompjutera
12. *BBC NEWS*, 2. 5. 2007, http://news.bbc.co.uk/go/pr/fr//2/hi/europe/6614273.stm
13. *The Economist*, 10. 5. 2007, http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598
14. *Telegraph*, 19. 5. 2007, http://www.telegraph.co.uk
15. Ifrah, Laurence, (2008): *The Georgia-Russia conflict: Internet, the other battlefield*, Défense nationale et sécurité collective, Committee for National Defence Studies, Paris
16. Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul (2008): *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia,http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf
17. Vučinić, Zoran (2001): *Međunarodno ratno i humanitarno pravo*, Vojnoizdavački zavod, Beograd

18. Shackleford, Scott (2009): *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law, Vol 27, No 1
19. Sinkovski, Stevan (2005): *Informaciona bezbednost – komponenta nacionalne bezbednosti,* Vojno delo, br. 2
20. Sklerov, Matthew (2009): *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, Military Law Review, No. 201

Contemporary security challenges – hactivism as a new form of social conflict

Summary: Nowadays, computer networks and information infrastructures security in general is not just a technical problem, but also an important strategic question. Due to the fact that global computer network is widespread and decentralized, together with the absence of legal framework which would regulate cyber warfare, activities of hacktivists – a sui generis cyber guerilla– has become an important problem of cyber security and additionally emphasized the importance of protection of information systems, conducting international investigations, extradition and punishment of perpetrators. The phenomenon of hacktivism has been present for about fifteen years, and it has affected various states on different continents, but even to this day no adequate and widely accepted solution for preventing this undesirable occurrence has been found. This paper attempts to describe the phenomenon of hactivism, discuss its implications for national security, as well as to offer a critical review of the current problems and strategies related to counteracting this occurrence.

Key words: hacktivism, cyber security, cyber warfare, national security, international law