ОДБРАНА ОД ПРЕТЊИ У САЈБЕР ПРОСТОРУ

др Дејан Вулетић

Београд, 2011.

Рецензенти
пуковник доц. др Иван Вулић
мајор доц. др Иван Тот

Издавач
Институт за стратегијска истраживања
Незнаног јунака 38, Београд
Тел. 011/2063-852, факс 011/3005-183
www.isi.mod.gov.rs

Језички уредник
Аутор

Дизајн корица
Милан Новичић

Технички уредник
Жељко Хрчек, потпуковник

ISBN 978-86-81121-09-2

САДРЖАЈ

УВОД

Војна организација, стратегија и доктрина, непрекидно се мењају кроз историју под утицајем развоја нових технологија. Чувени кинески војсковођа и војни писац Сун Цу Ву (*Sun Tzu Wu*) давно је рекао "Победити противника без битке", другим речима, остварити сопствене циљеве и интересе без употребе војне силе. Савремене економски и војно јаке силе крајем двадесетог и почетком двадесетпрвог века заступају исту тезу. Разлика између времена Сун Цу Вуа и садашњег времена је велика, када је у питању утицај технологије на остваривање циљева и интереса. Услови прикупљања, обраде и коришћења информација, уз истовремено онемогућавање противника да то исто чини, у савременим условима су далеко сложенији.

Модерно друштво, чији смо савременици, критично је зависно од информације, као стратегијског ресурса и информационо-комуникационе технологије, којом се врши њен пренос, обрада и размена. Савремени сукоб је незамислив без великог броја информација о противнику, сопственим снагама, простору и времену. Међутим, поред предности које пружају, информације су постале и важан циљ за противника. Лишити противника преимућстава које му пружају, уз истовремено обезбеђење потребних информација за сопствене потребе, значи остварити значајну предност у реализацији циља на одређеном простору и за одређено време уз минимално ангажовање снага и минималне губитке. Савремене оружане снаге у великој мери се ослањају на најновија технолошка достигнућа на пољу информационо-комуникационе технологије.

Институционализација дипломатије у новим условима и изградња савременог безбедносног система у свету утицала је на ограничење примене војног фактора у реализацији постављених циљева спољне политике од стране држава као субјеката међународних односа. Такво стање у међународној заједници је утицало да се остварење интереса не врши применом оружане силе, већ да се они остваре другим средствима. Као последица тога, дошло је до другачијег промишљања сукоба, услед чега су и настале теорије попут Сукоба ниског интезитета и Концепција сведимензионалног рата.

Информације постају све важније за националну безбедност уопште, како у миру тако и у оружаном сукобу. Информационо-комуникациона технологија створила је и ново окружење – сајбер (*cyber*) простор који обухвата становнике било ког дела света, свих старосних група и друштвених слојева и који се мора боље спознати. Сагласно овоме, савремени сукоби су наглашено праћени и активностима у сајбер простору. Они који су савладали технике сајбер ратовања су у предности над својим противницима.

Информациона револуција трансформише ратовање, тј. изазива промене у томе како друштва долазе у конфликт и како њихове оружане снаге воде оружани сукоб. Више се не сукобљавају масивне, укопане војске у крвавим и исцрпљујућим борбама. Уместо тога, мале и изузетно мобилне снаге, «наоружане» информацијама у реалном времену, ударају великом брзином на неочекиваним местима. Победник је она страна која може брже да експлоатише информације, односно, она страна која брже анализира, процењује ситуацију и реагује. Велике промене се дешавају у томе како се информација прикупља, чува, обрађује, предаје и приказује, и како су саме организације организоване да искористе повећан обим информација. Информација постаје стратегијски ресурс. Доминација у информационом спектру је, дакле, неопходан услов за успех и победу у сукобу.

Нови начин ангажовања држава у сукобу условио је појаву нових средстава, а са њима и нових начина вођења сукоба. Све учесталија примена информационо-комуникационе технологије у војне сврхе довела је до појаве претњи у сајбер

простору. Захваљујући ефикасности примене оно заузима све значајније место и у савременим сукобима.

Сајбер ратовање, као неоружани облик сукоба, појављује се у миру, али је и редовни пратилац оружаних сукоба у рату. Та чињеница посебно је изражена у савременим оружаним сукобима.

У првом делу публикације разматрају се различите **дефиниције и карактеристике сајбер простора**.

У другом делу обрађен је феномен **претњи у сајбер простору** кроз следеће проблемске целине: **напади на рачунарске системе, сајбер криминал, сајбер тероризам и сајбер ратовање**.

Трећи део посвећен је **одбрани од сајбер напада,** која је презентована кроз препоруке за одбрану од сајбер напада, заштиту критичних информационих инфраструктура и стратегије за обезбеђење сајбер простора.

I

САЈБЕР ПРОСТОР

У модерном друштву, друштву глобалне повезаности, конверзација или милионска новчана трансакција обављају се између људи с једног на други крај света, брзо и јефтино. Све већа употреба персоналних рачунара, лак приступ Интернету, појава савремених уређаја информационо-комуникационе технологије – ИКТ (*Information-Communication Technology – ICT*) као што су нпр. мобилни телефон и рачунарска мрежа, довели су до радикалних промена у животима грађана информационог друштва.

1. Теоријско одређење сајбер простора

Израз ''сајбер простор'' чине две речи с различитим значењем – сајбер и простор. Ради одређења израза ''сајбер простор'' неопходно је одредити значење речи ''сајбер'' и ''простор''.

Префикс ''сајбер'' везује се за термин кибернетика (*cybernetics*) те отуда у свакодневној пракси долази до сукобљавања око термина ''сајбер'' или ''кибер''.[1]

Реч кибернетика потиче од старогрчке речи *kybernao* која у преводу значи управљати, у општем смислу.

[1]"Сајбер" је страна реч, адаптирана у српском језику, која је ушла у општу лексику као препознатљив термин.

Под кибернетиком, амерички математичар Норберт Винер подразумева целу област теорије управљања и комуникација.[2] Винер је указао да научни и технички прогрес имају огромне и сложене друштвене последице. Његов велики допринос науци огледа се у томе што је указао на потребу приближавања метода анализе различитих струка и ширу генерализацију теоријских резултата као и заједничко формирање научних тимова различитих профила ради решавања сложенијих проблема.[3]

Кибернетика је научна дисциплина која проучава живе и неживе системе, њихову структуру (рецепторе, меморију, програме и ефекторе), комуникацијске могућности, принципе деловања, а посебно, механизме контроле, регулације и ауторегулације стања равнотеже путем повратне везе. Кибернетика настоји да развије метод управљања неким системом који ће се користити информацијама о ранијем деловању система за корекцију садашњих операција, као и у планирању будућих.[4]

Мада се корени речи ''сајбер'' могу уочити у Винеровим схватањима, право значење дао је Вилијам Гибсон *William Gibson)* у свом роману *''Neuromancer''*, 1984. године, где се под термином ''сајбер'' подразумева – виртуелно, невидљиво, неограничено, базирано на технологији.

У речнику Матице српске простор се дефинише као неограничена протегнутост, растојање у свим димензијама и правцима.[5] Реч ''простор'' има различито значење у различитим научним дисциплинама те је стога тешко наћи универзалну, општеприхваћену, дефиницију. Простор је један од основних квантитета у науци који не може бити дефинисан преко других квантитета, као што су сила или енергија, које су већ дефинисане преко простора.

---

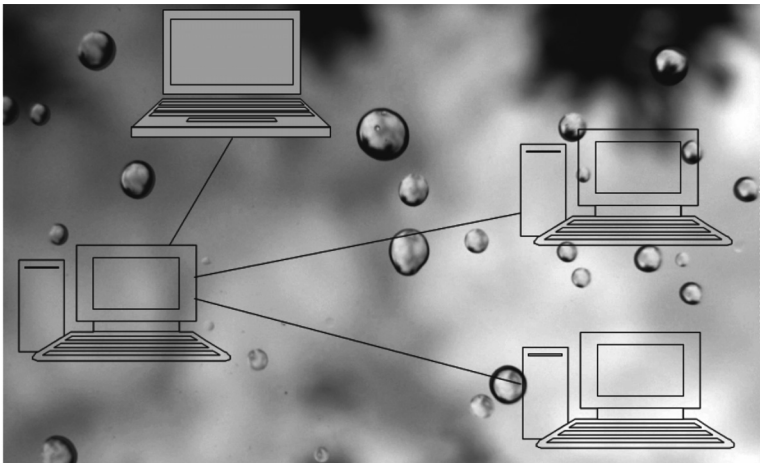
[2]Винер Н., *Кибернетика или управљање и комуникација код живих бића и машина*, Издавачко-информативни центар студената, Београд, 1972, стр. 9.

[3]Винер Н., *Кибернетика и друштво – људска употреба људских бића*, Нолит, Београд, 1973, стр. 10-17.

[4]Требјешанин Ж., *Речник психологије*, Стубови културе, Београд, 2004, стр. 217.

[5]*Речник српскохрватског језика (књига пета)*, Матица српска, Нови Сад, 1973, стр. 226-227.

Синтагму сајбер простор (*cyber space*) Гибсон види као универзум рачунарских мрежа, свет у којем се мултинационалне компаније, друштва и други субјекти боре за освајање података и информација.



Слика 1. Сајбер простор

Под сајбер простором, подразумева се ‘’врста заједнице’’ сачињена од мреже рачунара у којој се елементи класичног друштва[6] налазе у облику битова и бајтова односно, простор који креирају рачунарске мреже.[7]

Префикс ‘’сајбер’’ очито указује на изузетну сложеност, непрекидност интеракција, неограниченост простора и неограничен број различитих услуга, непрестано наилажење на нешто ново и неочекивано, у свету рачунарских мрежа.

Сајбер простор представља термин који означава *online* свет Интернета (рачунарских мрежа) али и дигитални свет уопште.[8]

---

[6]Talkot Parsons definiše društvo kao "tip društvenog sistema sa relativno najvišim stepenom samodovoljnosti". Parsons T., *Društva*, August Cesarec, Zagreb, 1998, str. 12.

[7]Дракулић М., Дракулић Р., *Сајбер криминал*, www.bos.org.yu/cepit/idrustvo/sk/cyberkriminal.pht

[8]Tipton H., Krause M., *Information Security Management Handbook (fifth edition)*, CRC Press, New York, 2004, p. 3171; *Computing Dictionary*, http://computingdictionary.thefreedictionary.com/cyberspace; *Encarta encyclopedia*, http://encyclopedia.msn.com/encyclopedia_761582824/Cyberspace.html

Сајбер простор обухвата све облике умрежавања, дигиталних активности; то укључује садржај и активности вођених кроз дигиталне мреже.[9]

Вера Тасић и Иван Бауер у *Речнику компјутерских термина,* сајбер простор дефинишу као ''окружење виртуелне реалности (као што је Интернет) у коме особе комуницирају помоћу повезаних рачунара.[10]

Стварање сајбер простора омогућавају *Microsoft*, *CISCO* и друге компаније које производе савремене уређаје информационо-комуникационе технологије.

2. Карактеристике сајбер простора

Сајбер простор је вештачка творевина настала као резултат друштвених потреба и технолошких иновација. Пружа огромне могућности и у информационом друштву представља доминантни медиј комуникације. То је простор различитих садржаја, простор који је лак за коришћење.

Појава сајбер простора условила је велики број дигиталних производа и услуга који су заменили многе традиционалне производе и услуге, стварајући и нови начин трговине.[11]

Сајбер простор представља нову форму јавног места, које пружа могућност за изражавање, обезбеђује слободу кретања за разлику од физичког простора који има одређене димензије, границе, збијеност и друге ограничавајуће факторе.[12]

Рачунарске мреже допуштају људима да креирају читав опсег нових друштвених односа у којима се могу састајати и

[9]*Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space*, UK Office of Cyber Security – UK Cyber Security Operations Centre, June 2009, p. 7.

[10]Тасић В., Бауре И., *Речник компјутерских термина*, Микро књига, Београд 2003, стр. 125.

[11]Zekos G., *State cyberspace juristiction and personal cyberspace juristiction, International Journal of Law and Information Technology*, Oxford University Press, London, Vol. 15 No. 1, 2007, p. 3.

[12]Jones S., *Virtual Culture – Identity and Communication in Cybersociety*, SAGE Publications, London, 1997, p. 25, 36.

утицати једни на друге. Могу се формирати хиљаде група да дискутују о различитим темама, играју игрице, забављају једни друге и чак и да раде на сложеним заједничким пројектима. Сајбер простор је ''кућа'' хиљадама група људи који се састају да деле информације, дискутују о заједничким стварима, обављају посао. Неке од тих група су велике и добро развијене, али неки критичари тврде да те групе не могу представљати праве заједнице, док други сматрају да имају могућности да подрже традиционалне (*face-to-face*) заједнице и помажу да се локалне заједнице држе заједно. Критичари описују *online* заједнице као више изоловане него стварне (*real-life)* групе. Пејзаж сајбер простора тешко је схватити. Не постоји јединствено представљање сајбер простора или чак његових главних компоненти.[13]

Одређени аутори изражавају страх да ће велико учешће у виртуелним заједницама удаљити људе од учешћа у стварним заједницама (породице, пријатеља). Сајбер простор успешно подржава друштвене везе између људи који се не могу често виђати. Виртуелне заједнице се разликују од реалних заједница у основама на којима учесници заснивају њихове везе. Људи на мрежи имају већу тенденцију да заснивају осећања блискости на основама заједничких интереса пре него на основу заједничких друштвених карактеристика као што су пол и друштвено-економски статус. Те заједнице су вероватно хомогеније у њиховим интересима и ставовима али су вероватно хетерогеније по питању година, друштвеног статуса или националне припадности.[14]

Томас Ериксен сматра да сајбер простор представља нешто квалитативно ново. Можда је налик на неку врсту бескрајног часописа или неку врсту велике библиотеке, али се разликује од библиотеке по томе што информације на мрежи нису сређене, ни алфабетски ни на било који други начин. Мрежа је, другим речима речено, невероватно демократска и децентрализована, што показује и то да на мрежи све врви од порно-

[13]Kollock P., Smith M., *Communities in cyberspace*, Routledge, New York, 2001, p. 3-17.

[14]Wellman B., Gulia M., ''*Virtual communities as communities – Net surfers don't ride alone*'', Kollock P., Smith M., (ed) *Communities in cyberspace,* Routledge, New York, 2001, p. 181-186.

графије, могу се наћи и политичко шиканирање и пропаганда свакојаке врсте.[15]

Због предоминације енглеског језика, који се успоставља и као језик нове писмености, сајбер простор је упркос својој отворености управо простор у којем западни свет потврђује своју доминацију. Због глобалистичке концепције која му је битна одлика, сајбер простор представља претњу националним културама и националним идентитетима, обликујући готово сваки сегмент живота грађана укључујући забаву, потрошњу, образовање, политички ангажман и друго. То је *Универзум* који пружа илузију анонимности који у ствари зависи од реалне инфраструктуре (одређених институција, комерцијалних интереса, реалних односа моћи).[16]

Маргарет Морс *(Margaret Mors)* сматра да сајбер простор карактерише много разноврсније и брже кретање од кретања које се примећује у материјалном простору и нормалном временском трајању.[17]

Ричард Којн *(Richard Coyne)* посматра сајбер простор троструко:

– Као свет (скуп физичких ентитета нпр. хардвер, комуникациони водови);
– Као простор (објекти могу бити близу или далеко једни од других тако да се удаљеност може мерити) и
– Као место (нпр. *web* страница се може посматрати као место).[18]

Постоји преко милијарду персоналних рачунара од којих је већина повезана на Интернет. Почетком 2008. године, број власника мобилних телефона широм света био је већи од оних који их нису имали (укључена и деца). Сваки мобилни телефон

[15]Eriksen T., *Tiranija trenutka: brzo i sporo vreme u informacionom društvu*, biblioteka XX vek, Beograd, 2003, str. 22-23.

[16]Томић З., *"Сајбер простор и проблеми разграничења"*, Култура, бр. 107-108, Завод за проучавање културног развитка, Београд, 2004, стр. 10-13.

[17]Mors M., *"Sajber-predeli, kontrola i transcendencija: estetika virtuelnog"*, Kultura, br. 107-108, Zavod za proučavanje kulturnog razvitka, Beograd, 2004, str. 137-138.

[18]Coyne R., *Designing information technology in the postmodern age: From method to metaphor*, MIT Press, Cambridge, 1995, p. 151-156.

може представљати улаз у сајбер простор. Већина тих корисника или мало зна или води рачуна о безбедности.[19]

О експанзији коришћења Интернета, говоре и следећи подаци који се односе на 2010. годину:

– 1,97 милијарди корисника Интернета (јун 2010. године);
– 14% повећан број корисника Интернета у односу на претходну годину;
– 1,88 милијарди корисника електронске поште;
– 2,9 милијарди отворених налога електронске поште;
– 255 милиона сајтова крајем 2010. године;
– 21,4 милиона нових сајтова у 2010. години.

Сајбер простор није изолован и неприступачан свет. Он је у рукама сваког али захтева поседовање рачунара и одговарајућих алата. У сајбер простору још увек нису сва правила потпуно дефинисана и нови креативни процеси ће се и даље дешавати.[20]

[19]Libicki M.,, *Cyberdeterrence and Cyberwar*, RAND Project Air Force, RAND Corporation, 2009, p. 3-4.

[20]То потврђује и проналазак научника Тим Бернс-Лија (*Tim Berns–Lee*) из женевске лабораторије Европске организације за нуклеарна истраживања (*CERN*) крајем 1990. године. Тим Бернс-Ли је развио групу протокола који омогућују хипертекстуалне везе између докумената (и делова докумената) на мрежи чиме је значајно допринео масовној употреби Интернета.

II

ПРЕТЊЕ У САЈБЕР ПРОСТОРУ

Крајем 19. и почетком 20. века људско друштво карактеришу нагле и драматичне промене у скоро свим областима живота и рада. Убрзани развој науке и технологије, интензивна индустријализација учинили су да свет тога доба почне да поприма сасвим нова обележја као што су растућа стопа криминала, све већа друштвена опасност кривичних дела, професионализација и организованост криминалаца. Период од друге половине 20. века, поред изузетне динамике, карактеришу и извесне контроверзе, које су указивале на тзв. ''тамну страну прогреса''. Напредак науке, а посебно техничких и природних дисциплина доноси, поред позитивних резултата који су његово основно обележје, и огромне потенцијалне опасности.[21]

Убрзани развој информационо-комуникационе технологије и незаустављиви раст примене у свим сферама људског друштва увећава њихову рањивост и изложеност врло озбиљним опасностима. Информационо-комуникациона технологија носи у себи уједно и оно најбоље и оно најгоре. Напредак се састоји у комуникацији скоро без граница, а невоља је у томе што тај ''Титаник'' виртуелне пловидбе наилази на санту леда. После атомске бомбе и успостављања општег нуклеарног одвраћања, модерном друштву је потребна нова врста одвраћања од најновије ''информатичке бомбе''.[22]

---

[21]Алексић Ж., Милошевић З., *Лексиком криминалистике*, Глосаријум, Београд, 1995, стр. 16-20.

[22]Вирилио П., *Информатичка бомба*, Светови, Нови Сад, 2000, стр. 106-133.

Због наглашене комплексности ИКТ и чврсте међузависности, националне инфраструктуре које повезују, покрећу и опслужују рачунари, постале су изузетно осетљиве, и, ако се организовано нападну, могу се проузроковати далекосежне последице на међународном, националном и индивидуалном плану. Друштва су закорачила у све већу глобализацију, и по питању рачунарских мрежа, што је повећало њихову осетљивост и рањивост на потенцијалне нападе. У сајбер простору постоје прилике за сваког: стране шпијуне, незадовољне запослене, политичке активисте, традиционалне криминалце.

Нови миленијум доноси све већу популарност информационо-комуникационих технологија, доступних све већем броју људи, као што је нпр. бежична мрежа (*wireless network*), велика брзина приступа Интернету и сл. Нажалост, те технологије стварају и нове могућности злоупотребе. Проблем са 24/7 технологијама (24 часа, 7 дана у недељи) је тај што нападачи могу лакше остварити неовлашћен приступ имајући више времена да открију и искористе рањивости система.[23]

Паралелно са информационо-комуникационом технологијом, претње у сајбер простору се налазе у фази бурног развоја и динамичких промена. Због тога је, бар у садашњем тренутку, практично немогуће сагледати и предвидети све могуће правце тог развоја, њихов обим, динамику и садржај, као ни временску димензију ових процеса. Као карактеристике претњи у сајбер простору, Петровић наводи:[24]

– Ограничене могућности за непосредно надгледање и контролу и мала вероватноћа откривања тих активности. Починиоци извршавају незаконита дела на начин који је најчешће невидљив за жртву. То је последица, пре свега, примене посебно дизајнираних алата као и због саме форме података који су у дигиталном облику, тако да их је лакше копирати или уништити. Несарадња и несхватање озбиљности проблема угро-

[23]Shinder D., *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland (USA), 2002, p. 95-121.

[24]Петровић С., *Комūјūтерски криминал*, Војноиздавачки завод, Београд, 2004, стр. 54-111.

жених субјеката значајно доприноси малој вероватноћи откривању таквих активности.

– Нове просторне и временске границе. С обзиром на то да у сајбер простору не постоје географска ограничења то потенцијалним починиоцима пружа могућност деловања из било ког дела света. Из ове чињенице и проистиче потреба тешње међусобне сарадње релевантних субјеката на глобалном нивоу у решавању проблема претњи у сајбер простору. Све већа интеграција рачунарских мрежа и *online* приступ пружају потенцијалним починиоцима веће могућности да открију и искористе рањивости система.
– Могућност претходне провере (тестирања) акције. Након откривања рањивости система могуће је извршити тестирање одређеног алата чиме се вероватноћа евентуалног неуспеха смањује на минимум. Примера ради писање одређеног рачунарског вируса прилагођеног рањивостима система може се проверити у интерном систему.
– Драстично повећање моћи починилаца. Употребом средстава ИКТ од стране починиоца са великим техничким знањем могу се постићи знатно већи резултати активности него што би се то могло учинити на други начин. Тиме се криминални потенцијал починилаца знатно увећава. Примера ради, пљачку добро обезбеђене банке много је лакше, и уз мањи ризик, извршити путем рачунарске мреже него извршавањем класичне пљачке користећи ватрено оружје.
– Глорификација починилаца. Услед недовољне едукације јавног мњења, као и због сензационалистичког извештавања појединих средстава јавног информисања о незаконитим делима у сајбер простору, долази до благонаклоног гледања једног дела друштва на тај феномен, не увиђајући његову штетност и негативне импликације.

Претње у сајбер простору карактерише изразита динамичност, велика феноменолошка разноврсност (велики број појавних форми), константно ширење на нове области пара-

лелно са већом употребом рачунара и глобалних рачунарских мрежа, тежина и тешка сагледивост последица, велика тамна бројка починилаца, отежано откривање и доказивање, специфичан профил починилаца, велике могућности за прикривање учињеног кривичног дела итд.[25]

Починиоцима погодује и увођење нових оперативних система што их чини рањивим пре него што корисници научне да их конфигуришу за бољу заштиту. Починиоци такође воле стандардизацију јер када нешто постане стандард, као што је то *Windows* оперативни систем, то постаје омиљена мета за нападаче. Када желе да направе велику штету вирусом циљеви ће бити најпопуларнији и највише примењивани оперативни систем.[26]

Двадесетчетворочасовни приступ рачунарским системима довео је до тога да је време изгубило значај.[27] Број потенцијалних жртава је изузетно велики. Свеприсутна повезаност (од Интернета, до *LAN, WAN, Wireless*) доводи до широкорашрене рањивости.

Претње у сајбер простору представљају све већу друштвену опасност због сталног усавршавања техника, релативно једноставног извршења одређених дела као и велике базе одакле се регрутују починиоци. Тешко је дефинисати претње у сајбер простору као што је и тешко идентификовати извор и мотив нападача.

Симболички значај и важност рачунарских система повећавају њихову вероватноћу да буду мете починилаца. У том смислу су посебно осетљиве виталне информационе инфраструктуре: енергетски систем, водовод, финансијски сектор, систем безбедности. Степен дигитализације организација, и друштва уопште, утиче на вероватноћу напада. Велике компаније имају велике рачунарске мреже и самим тим нуде више мета за напад. Истраживање агенције *Riptech* показује да је

[25]Цетинић М., *Комūјūтерска кривина дела и њихови ūојавни облици*, Правни живот бр.10, Удружење правника Србије, Београд, 1998, стр. 263-267; Алексић Ж., Шкулић М., *Криминалисūика*, Досије, Београд, 2004, стр. 384-396.

[26]Shinder D., *op.cit.*, p. 95-121.

[27]Tipton H., *op.cit.*; part Gabrys E., The International Dimension of Cyber Crime, p. 2942-2958.

већа вероватноћа да ће нападачи извршити циљани напад на веће него мање организације. Послови са великом зависношћу од ИКТ (*online* коцкарнице, банке) такође су, више угрожени. Дакле, степен дигитализације у организацији и друштву повећава његову вероватноћу да буде мета починилаца.[28]

Нације које више користе ИКТ на којој у великој мери базирају своје економије су рањивије од оних које мање користе. Иако мањак ИКТ смањује тренутно рањивост, на економском плану дугорочно гледано доноси штету.

Сваки систем има рањивости. Комплекснији систем подразумева и потенцијално већи број таквих рањивости и пропуста. Осетљивост модерног друштва огледа се у великом броју информационих инфраструктура, сталној реконфигурацији и недостатку особља и ресурса за њихово надгледање.

Архитектуре рачунарских мрежа и система су биле пројектоване за другачије окружење – окружење поверења. Данас, појединци, организације и владе са лошим намерама су наоружани знањем и алатима те могу компромитовати рачунарске мреже. Као последица, заштита рачунарских мрежа и система постало је питање од приоритетног значаја за како за државу тако и за војску.

У модерном друштву је дошло до промене природе рачунарских напада – напади све малициознији, боље координирани, софистицираније. Све већа расположивост и приступачност алата за напад као и релативно ниска цена омогућава скоро сваком да изврши напад. С друге стране цена детектовања, опоравка, одговора је знатно већа.

Опасност или претња је вероватноћа (могућност) дешавања нечега (напад, грешка, дисфункција, природна катастрофа …) што ће повредити, оштетити или уништити ИКТ ресурсе. Претња може имати или не криминално порекло, може бити међународног карактера или не.[29]

---

[28]Kshetri N., *Pattern of global cyber war and crime: A conceptual framework*, Journal of International Management, The Fox School of Business and Management – Temple University, Greensboro (USA), No. 11, 2005, 541–562.

[29]Solange Ghernaouti-Helie, *Cybersecurity Guide for Developing Countries*, International Telecommunication Unione, Geneva, 2009, p.3.

1. Напади на рачунарске системе

Процес извршења сајбер напада састоји се од тражења и прикупљања рањивости циљаних система и њихове експлоатације.[30]

На *слици 2* су приказане различите фазе сајбер напада. Нападач прво прикупља информације и тражи потенцијалне рањивости циљаног система ради добијања максималне количине информација за будућу експлоатацију. Он истражује механизме и нивое заштите који се користе за идентификацију, аутентификацију, контролу приступа, енкрипцију и надзор. Он идентификује техничке, организационе и људске слабости у циљаном систему. Потенцијални нападачи такође траже и експлоатишу безбедносне рањивости које још нису "закрпљене" (*patched*). Користе све расположиве ресурсе (*attack libraries, attack toolkits...*) а током повлачења настоје да прикрију трагове напада како да се не би дошло до њих.

Услови за успешан напад су:

- Познавање циљаног система, укључујући функције, сервисе, конфигурацију, политике и алате заштите и администрирање;
- Ефикасно коришћење програма који ће аутоматски експлоатисати рањивости за проваљивање у рачунар (ти програми су познати под називом "*exploits*");
- Капацитет нападача да прикрије своје трагове да би избегао могућност да буде детектован и праћен;
- Брзина напада чиме се смањује могућност да се за предузетим мерама заштите закасни.

Рањивост сајбер простора представља значајну бригу по безбедност и мора бити разматрана у свим друштвима. Опасност од сајбер напада лежи у способностима нападача да проузрокује, из удаљеног места и са минималним ресурсима, значајне штете. То може бити постигнуто кроз краткотрајно прекидање свакодневних активности, значајну економску штету или кроз проузроковање катастрофа у којима би било људских жртава. Мада досадашњи напади нису узроковали људске жрт-

[30] *Idem*, p. 48-49.

Слика 2. Фазе сајбер напада

ве та могућност не може бити искључена у нападима на критичне информационе инфраструктуре. Употреба сајбер простора од стране терористичких организација, организованих криминалних група и актера спонзорисаних од стране државе, представља озбиљну претњу по безбедност.

Претње у сајбер простору могу бити класификоване на више начина. Једна од најопштијих класификација на основу мотивационих фактора: сајбер криминал, сајбер тероризам и сајбер ратовање.[31]

2. Сајбер криминал

Сајбер криминал представља такав облик криминалног понашања, једног или више лица у сајбер простору, у којем се рачунарске мреже појављују као средство, циљ, доказ или окружење извршеног кривичног дела.

[31] *Cyber Security Strategy*, Ministry of Defence Estonia, Tallinn, 2008, p. 10.

Постоје различити облици сајбер криминала:

– *Сајбер шпијунажа* (прикупљање обавештајних података употребом информационо-комуникационе технологије, нпр. систем за надзор комуникација ''*Eshelon*'' који контролишу пет држава енглеског говорног подручја – САД, Велика Британија, Аустралија, Канада и Нови Зеланд);
– ''*Хакинг*'' (неовлашћен приступ рачунарским ресурсима, нпр. неовлашћен упад у рачунски систем владиних организација ради остварења одређених политичких циљева);
– *Сајбер саботажа* (оштећење, уништење и на друге начине чињење неупотребљивим података, програма, рачунара или рачунарских мрежа);
– *Сајбер превара* (подразумева прикривање и лажно приказивање података с циљем се себи или другоме прибави противправна имовинска корист и тиме другом лицу нанесе штета, нпр. наруџба неког производа путем Интернета дајући при томе личне податке друге особе);
– Криминал везан за садржаје подразумева производњу и дистрибуцију недозвољених и штетних садржаја на Интернету, нпр. ширење дечијег порнографског материјала, расистичких, нацистичких и сличних идеја и ставова.
– Криминал везан за производе и супстанце (рачунарска мрежа се користи за манипулацију забрањеним производима, супстанцама и робама, нпр. трговина дрогом, људским органима или оружјем помоћу Интернета).
– Повреде приватности (подразумева долазак до података о личности нпр. коришћењем одређених алата на мреже врши се надгледање електронске поште или прислушкивање).

Начин извршења дела говори о техничкој способности починилаца. Ако је напад строго технички нпр. *IP spoofing*[32]

[32]Скраћеница за *Internet Protocol (IP) Address Spoofing* а представља процес фалсификовања IP адресе у оквиру IP пакета.

реч је о починиоцу са великим техничким знањем. Ако је у питању *социјални инжењеринг*[33] претпоставка је да је реч о учиниоцу са мањим техничким знањем што не мора увек да буде тачно. Могуће је да починилац почиње са лакшим начином за добијање приступа, а ако то не успе приступа тежим. Уколико нема доказа о спољњем упаду, напад је извршен од стране неког из система те је потребно погледати и мере физичког обезбеђења.[34]

Напади се углавном дешавају ноћу (између осталог и због одсуства администратора система) мада није увек правило. Уколико се напад деси у радно време вероватно је нападач из друге временске зоне (8-12 сати разлике). Уколико се напад дешава ноћу претпоставља се да је нападач свестан физичке локације мете, зна када администратор система није присутан бирајући најбоље време за продирање у систем. То аутоматски наводи на сумњу да починилац има везе са неким из система или је починилац неко од корисника или неко ко има приступ упутствима компаније.[35]

Напад је могуће починити из било ког дела света. Економисти су израчунали да починиоци пре него што изврше криминалне активности, анализирају одређене параметре.[36]

Сајбер криминал се дешава ако је Mb + Pb > Ocp + OcmPaPc, где је

Mb (*monetary benefits*) представља новчану корист извршеног дела.

Pb (*psychological benefits*) представља психолошкуе добит извршеног дела (унутрашње задовољство). Уколико је нападач идеолошки мотивисан, унутрашње задовољство је свакако много веће него у случају када починилац почини одређено дело ради забаве.

---

[33]Техника компромитовања заштите рачунарског система, убеђивањем и обмањивањем, пре него употребом информационо-комуникационе технологије.

[34]Marcella A., Greenfield R., *CYBER FORENSICS: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes*, CRC Press, New York, 2002, p. 98.

[35]Marcella A., *op.cit.*, p. 97.

[36]*The Simple Economics of Cybercrimes*, IEEE Security & Privacy, january/february 2006, p. 36, www.computer.org/security

Ocp (*psychological costs of committing the crime*) представља психолошку цену извршеног криминала. Као и психолошка добит овај елемент је неопипљив, али је везан за психолошку и менталну енергију потребну за извршење криминала. Она је резултат страха од хапшења и осуде. Овај елеменат зависи и од одређених друштвених норми, односно разликује се од друштва до друштва. Наиме, велики број хакера сматра да су сајбер преваре погрешна активност, али оправдана ако су жртве богаташи.

Ocm (*monetary opportunity costs of conviction*) представља цену осуде. Потенцијални починилац прави трошкове колико може легално зарадити за нпр. три године на колико може бити осуђен за одређено дело. На наведени елеменат велики утицај има одговарајућа законска регулатива која се тиче сајбер криминала. Уколико су предвиђене строжије санкције за дела која представљају сајбер криминал, то ће у одређеним случајевима деловати одвраћајуће на потенцијалног починиоца.

Pa (*probability of arrest*) представља вероватноћу хапшења. Ова вероватноћа је веома мала нарочито ако је починилац с другог континента због, још увек, недовољне сарадње на глобалном нивоу.

Pc (*probability of conviction*) представља вероватноћу осуде. Као и вероватноћа хапшења, вероватноћа осуде је веома мала. Статистике показују да вероватноћа да починиоцу буду ухапшени и осуђени износи мање од 1%.[37]

Производ OcmPaPc се назива још и ''очекиване казнене последице'' (*expected penalty effect*).

Мотиви починилаца су веома комплексни и могу бити политички (нпр. сајбер тероризам), финансијски (нпр. лична корист, наношење штете компанији), образовни (тестирање знања, истраживање сајбер простора), психолошки (различити поремећаји, узбуђење услед моћи и контроле над другим људима), социјални (жеља да се исправи неправда у свету и равномерније расподели богатство). Прикупљени докази на месту извршења кривичног дела значајни су и због тога што показују мотив нападача. Уколико је у питању систем који садржи

[37]Stephenson P., *Investigating Computer-Related Crime: A Handbook for Corporate Investigators*, CRC Press, New York, 2000, p. 18.

финансијске податке чијим компромитовањем би компанија била знатно оштећена или би конкуренту обезбедио значајну предност опасност највише прети од незадовољних запослених или корпорацијских шпијуна. Уколико је, дакле, упад добро организован и фокусиран на одређене податке очито је директно нападнута организација и са одређеним циљем. Уколико је насумичан напад, починилац је слабо организован, вероватно без искуства и мало зна о унутрашњој структури система.

3. Сајбер тероризам

Означавање напада на рачунаре и рачунарске мреже као сајбер тероризам је проблематично зато што је тешко одредити намеру, идентитет или политичку мотивацију нападача.

Синтагма "сајбер тероризам" користи се све чешће у модерном друштву. Сајбер тероризам је коришћен да опише различите акције као што су крађа података или хакинг, планирање терористичких напада, проузроковање насиља,[38] или напад на информационе системе (рачунарске мреже).[39]

Званична дефиниција сајбер тероризма коју дају експерти из Центра за заштиту националне инфраструктуре (*National Infrastructure Protection Center – NIPC*) Сједињених Америчких Држава, дефинише сајбер тероризам као "криминални акт извршен кроз рачунаре резултујући у насиљу, смрти и/или деструкцији, стварајући терор ради убеђивања владе да промени своју политику".[40]

Марк Полит (*Marc Pollitt*) наводи да сајбер тероризам представља унапред смишљен, политички мотивисан, напад против информација, рачунарских система програма и података који изазивају насиље и страх код цивилних мета.[41]

[38]Pollitt Marc, *"Cyberterrorism – fact or fancy?"*, www.cs.georgetown.edu/~denning/infosec/pollitt.html

[39]*Statement of Dorothy Denning*, www.house.gov/hasc/testimony/106thcongress/00-05-23denning.htm

[40]*National Infrastructure Protection Center*, www.nipc.gov

[41]Pollitt Marc, *op.cit.*

Познати експерт за сајбер тероризам, Дороти Денинг (*Dorothy Denning*), дефинише га као "недозвољени напад или претњу нападом против рачунара, рачунарских мрежа или сачуваних података с циљем да се заплаши влада или њени грађани у циљу остварења политичких или других циљева".[42]

Слично њој, Џејмс Луис (*James Lewis)* из Центра за стратегијске и међународне студије (*Center for Strategic and International Studies*) и стручњак за сајбер тероризам Маркус Хендршот *(Marcus Hendershot)* дефинишу сајбер тероризам као "коришћење рачунарских мрежа и алата ради прекида рада критичних националних инфраструктура или да примора или застраши владу или њене грађане.[43]

Одређени стучњаци за информациону безбедност сматрају да напади на рачунаре и рачунарске мреже могу бити дефинисани као сајбер тероризам ако су ефекти довољно деструктивни или реметилачки да производе страх упоредив са физичким актом тероризма.[44]

Више аутора сајбер тероризам види као облик сајбер криминала. Неки од њих, класификујући сајбер криминал у зависности од типа почињених дела на; а) политички, б) економски, в) производња и дистрибуција недозвољених и штетних садржаја, г) манипулација забрањеним супстанцама, производима и робама и д) нарушавање сајбер приватности, сајбер тероризам сврставају у категорију политичког сајбер криминала.[45]

Дебра Шиндер класификујући сајбер криминал у две широке категорија а) насилна или потенцијално насилна дела и б) ненасилна дела, сајбер тероризам сврстава у прву категорију. Под сајбер тероризмом подразумева тероризам који је извршен, планиран или координисан помоћу рачунарских мре-

[42]Denning D., *Is Cyber Terror Next?*, New York, U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm

[43]Lewis J., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington, 2002, p. 1.; Hendershot M., *"CyberCrime 2003 – Terrorists' Activity in Cyberspace"*, http://www.isedj.org/3/44/Jain.v1.txt

[44]Denning Dorothy, *Is Cyber War Next?*, op.cit.

[45]Кукрика М., Управљање сигурношћу информација, INFOhome Press, Београд, 2002, стр. 70-71; Дракулић М., Дракулић Р., *op.cit.*

жа.[46] Експерт за сајбер криминал, Хинган такође види сајбер тероризам као један од његових облика.[47]

Велики број дефиниција сајбер тероризма говори о комплексности тог феномена. На основу извршене анализе литературе у којима се говори о сајбер тероризму, тај појам се може дефинисати на следећи начин: **Сајбер тероризам представља криминални акт у сајбер простору који има за циљ да се заплаши влада или њени грађани у циљу остварења политичких циљева**.

Мојра Конвеј (*Maura Conway*) предлаже скалу која активност терористе на Интернету карактерише као употребу, злоупотребу, офанзивну употребу и сајбер тероризам.[48] Од стране стручњака углавном прихваћена класификација наводи четири могућа начина напада од стране сајбер терористе: одбијање, обмана, уништавање и експлоатација. То у суштини значи упад у информациони систем (рачунарску мрежу) да би зауставио рад, убацивање лажних података или ''злоћудних'' софтвера, уништавање система, или ''качење'' на систем да би се дошло до одређених тајних података.[49]

Кларк Стејт (*Clark State*), извршни директор Института за истраживања и хитан одговор *(Emergency Response & Research Institute)* у Чикагу упозоравао је да чланови неких радикалних исламистичких организација покушавају да развију мрежу хакера и могу бити ангажовани у сајбер нападима у будућности.[50]

Према приручнику ''Војни водич за тероризам у двадесетпрвом веку'' сајбер тероризам представља један сегмент сајбер операције док други сегмент представља сајбер подршка (планирање, регрутовање, пропаганда). Код сајбер тероризма рачунарска мрежа може бити оружје, медијум или циљ. Пре-

[46]Shinder D., *op.cit*, p. 51-67.

[47]Xingan Li, *Cybercrime: An Introduction*, www.studycrime.com/crime/cybercrime.php

[48]Conway M., *Reality Bytes: Terrorist Use of Internet*, http://www.firstmonday.dk/ issue7_11/conway

[49]Berkowitz B., Hahn R., *Cyber security: Who's watching the store?*, Issues in Science and Technology, www.issues.org/19.3/berkowitz.htm

[50]Denning D., *''Reflections on Cyberweapons Controls''*, www.cs.georgetown.edu/~denning/infosec/cyberweapons-controls.doc

ма истом извору, деструктивни напади на рачунарске мреже вероватно могу бити извршени да повећају ефекат физичких напада.[51]

4. Сајбер ратовање

Поједини експерти, као што је нпр. Атина Карацојани, сматрају да је сукоб 1999. године био први већи конфликт који је праћен сајбер ратовањем.[52] НАТО *web* сајтови и сервери били изложени бројним нападим од стране југословенских и кинеских хакера у току агресије 1999. године.[53]

Године 2003.-ће, рачунарски црв *Slammer* (велики, успешан *malware*) убачен је и успорио је контролу енергетског система у Сједињеним Америчким Државама. Резултат је био да је осам држава, две канадске провинције и око 50 милиона људи остало без електричне енергије.[54]

Јуна 2005. године, британски држављанин *Gary McKinnon* је ухапшен због наводног извршавања ''највећег војног компјутерског неовлашћеног приступа икада учињеног'', упадајући у рачунарске системе Министарства одбране Сједињених Америчких Држава и НАСА-е. Према проценама званичника САД цена праћења починиоца и решавања проблема које је он изазвао коштала је око милион америчких долара.[55]

У периоду 9-10. августа 2006. године, један од четири мејл сервера НАТО, био је изложен серији ДоС напада од стране *botnet* а детектован је од стране уређаја за надгледање

[51]*Cyber Operations and Cyber Terrorism*, DCSINT Handbook No. 1.02, 15 August 2005.

[52]Karatzogianni A., *The Politics of Cyberconflict*, Routledge, London, 2006.

[53]*Centre of Excellence Defence Against Terrorism*, Responses to Cyber Terrorism, IOS Press, Ankara (Turkey), 2007, p. 121; Patrick A., *Information Operations Planning*, Artech House, Boston-London, 2007, p.8.

[54]Clarke R., Knake R., *Cyber War – The next treat to National Security and What to do about it*, HarperCollins e-books, 2010, p. 87.

[55]Blyth A., Kovacich G., *Information Assurance*, Springer, London, 2006, p. 51.

(*monitoring*). Напад је блокиран и извршена реконфигурација сервера.[56]

У Естонији DDOS, 2007. године, био је највећи напад икада виђен. Више различитих ботнетова, сваки са десетинама хиљада заражених рачунара.[57] Неки називају случај Естоније ''првим ратом на мрежи (*Web War One – WWI*). Ене Ергма, портпарол Естонског Парламента, која има докторат из области нуклеарне физике, изјавила је: ''Када посматрам нуклеарну експлозију и експлозију која се догодила у Естонији маја 2007. године, видим исте ствари''.[58]

Годину дана касније, 2008. године, DDOS нападима били су погођени и Грузијски владини сајтови и хакован *web* сервер на којем је био хостован сајт председника Грузије. Грузија је повезана на Интернет преко Русије и Турске. Већина рутера у Русији и Турској су били преплављени нападима тако да се саобраћај није могао обављати. Потпуно је преузет национални домен ''*.ge*'', а корисници нису могли слати електронску пошту ван земље, нису се могли конектовати на спољне информационе ресурсе.[59]

Министарство одбране Сједињених Америчких Држава претрпело је, 2008. године, значајно компромитовање својих поверљивих рачунарских мрежа. Малициозни програм убачен је помоћу флеша у војни лаптоп у бази *Middle East* од иностране обавештајне агенције. Програм се брзо непримећено раширио у оквиру поверљивих и неповерљивих система, преносећи податке на сервер који је био под страном контролом.[60]

Године 2009. просечно је на сваких 2.2 секунде долазило до појаве малициозног програма у сајбер простору. Три или четири компаније које се баве антивирусним софтверима имале су софистициране мреже да надгледају нове малициозне програме, али су оне нашле и решиле један од десет малициозних

[56]Centre of Excellence Defence Against Terrorism, *op.cit.*, p. 124.

[57]Clarke R., Knake R., *op.cit*, p. 21.

[58]Shackelford S., *Estonia three years later: A progress report on combating cyber attacks*, Journal of Internet Law, February 2010, p. 23.

[59]Clarke R., Knake R., *op.cit*, p. 24-25.

[60]Lynn W., *Defending a New Domain*, www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

програма. Решење подразумева део софтвера направљен да блокира малициозни програм. Некада су потребни дани па и недеље да би се проблем решио. До проналаска решења, компаније, владини органи и обични корисници су потпуно рањиви на нове малициозне програме.[61]

У априлу 2009. године, непознати нападач (нападачи) је упао у један од рачунарских система у САД-у и преузео велику количину података везаних за развој авиона Ф-35 (дизајн, подаци о електронским системима …). Шта је тачно украдено није се могло открити пошто су нападачи криптовали украдене податке пре него што су их преузели.[62]

Почетком 2010. године, 75.000 рачунарских система у око 2.500 компанија широм света је било хаковано у комплексном нападу на *online* финансијске системе, сајтове за друштвено умрежавање и *e-mail* налоге. То је био један од највећих откривених напада, иако је слабо пропраћен кроз медије.[63]

Америчке агенције за националну безбедност су забринуте због логичких бомби од када су пронађене у више енергетских постројења.[64]

Прошле, 2010. године, велику пажњу јавности привукао је *Stuxnet* – специјално направљен малициозни програм који је заразио Сименсове SCADA уређаје који контролишу нафтоводе, електрична, нуклеарна и друга индустријска постројења у Ирану, инфицирајући најмање 30.000 рачунара широм земље. Према проценама стручњака, *Stuxnet* је најсофистициранији малициозни програм икад направљен тј. представља комбинацију која експлоатише четири различите рањивости у *Windows* оперативним системима.[65]

Многи експерти сматрају да сајбер напад може имати велики утицај на борбену способност нарочито у току конфликта. Напади на други информационе инфраструктуре као што

[61]Clarke R., Knake R., *op.cit*, p. 79.

[62]*Idem*, p. 185.

[63]O'Rourke M., *The Real Enemy*, Risk and Insurance Management Society (RIMS), New York, 2010, p. 80.

[64]Clarke R., Knake R., *op.cit*, p. 81.

[65]*EU Agency analysis of Stuxnet malware: a paradigm shift in threats and Critical Information Infrastructure Protection*, European Network and Information Security Agency, http://www.enisa.europa.eu

је систем телекомуникација или напајања електричном енергијом може имати велики утицај на борбену способност. Досадашњи напада нису имали превелики ефекат.

Данас су сајбер напади јефтин и лак начин да једна нација нападне другу. Прошле, 2010. године, генерални секретар Уједињених нација (УН), Бан Ки-Мун, изјавио је да сајбер оружје треба да буде додато на листу наоружања које потпада под Саветодавни одбор УН за разоружање (*UN's Advisory Board on Disarmament Matters*). Бан је навео да прекидање критичних система представља претњу по међународну безбедност, откад јавни и приватни сектор критично зависе од дигиталних информација.[66]

Рањивости Интернета, лежи, између осталог, у следећим чињеницама:[67]

- *DNS* (нпр. случај Естоније и Грузије када су нападнути сервери ботнетовима са хиљадама захтева по секунди). На тај начин оборена су два сервера од којих је један обављао саобраћај за Министарство одбране.
- Друга рањивост је рутирање пакета између провајдера, систем познат као *Border Gateway Protocol*.[68]
- Пренос углавном некриптованих садржаја.
- Могућност ширења малициозног саобраћаја ради напада на друге рачунаре.
- Чињеница да је то огромна мрежа са децентрализованим дизајном. Дизајнери Интернета нису желели да буде контролисан од стране влада, појединачне или колективне

Војно присуство у сајбер простору је несумњиво. Наведени, а и други бројни, примери показују озбиљност претњи у сајбер простору и последице које могу наступити по систем

[66]Marks P., *Fighting wars in cyber space*, New Scientist, 14.03.2009, Vol. 201, Issue 2699; Database: Computers & Applied Sciences Complete

[67]Clarke R., Knake R., *op.cit*, p. 69-73.

[68]Софтвер помоћу којег провајдер интернет услуга информише друге провајдере ко су његови клијенти тако да поруке намењене клијентима могу бити упућене према одређеном провајдеру услуга. Понекад провајдер може имати друге провајдере као клијенте.

одбране земље. То је условило и обуку нове категорије официра и специјалиста за различите области сајбер ратовања.

Процењује се да Северна Кореја има између 600 и 1.000 лица за сајбер ратовање који делују у ћелијама, под заједничком командом. Северна Кореја селектује елитне студенте у основној школи за будуће сајбер ратнике. Такви студенти пролазе кроз средње и високо образовање, после чега аутоматски уписују *Command Automation University* у Пјонгјангу (*Pyongyang*), где је фокус у образовању стављен на то како да хакују рачунарске системе противника. Они реализују редовне вежбе сајбер ратовања, једни против других, али и настоје да се и инфилтрирају у Јапан да науче најактуелније рачунарске вештине.[69]

4.1 Теоријско одређење сајбер ратовања

Сајбер ратовање је врста непријатељске активности предузета против рачунарских мрежа, рачунарских система и база података са циљем деградирања или уништавања циљаних система. На тај начин циљани системи могу бити неупотребљиви, деградираних перформанси што може утицати на команданта да донесе лошу одлуку услед недостатка информација.[70]

Сајбер ратовање се дефинише и као неовлашћено упадање од стране (за или уз подршку) владе у рачунаре или мреже друге нације, или предузимање других активности које утичу на рачунарски систем са циљем додавања, измене или фалсификовања података или проузроковање прекида или оштећења рачунара, мрежних уређаја или објеката контроле рачунарских система.[71]

Либицки сматра да је сајбер напад намерно онеспособљавање или ремећење рачунарских система једног субјекта (ентитета) од стране другог субјекта (ентитета). Угрожени субјект представља циљани систем (*target system*).[72]

[69]Clarke R., Knake R., *op.cit.*, p. 31-33.

[70]Stytz M., *Cyberwarfare Distributed Training*, Military Technology (MILTECH), 11/2006, p. 95-96.

[71]Clarke R., Knake R., *op.cit.*, p. 181.

[72]Libicki C. Martin, *op.cit.*, p. 23.

Сајбер напад изведен од стране неког ентитета против државе и њеног друштва, примарно али не искључиво са циљем утицања на понашање циљане стране, представља сајбер ратовање. Ентитет који спроводи напад може бити државни или недржавни актер.[73]

Сајбер ратовање, дакле, представља облик информационог ратовања који се састоји од низа акција којима се прекидају или уништавају информациони и комуникациони системи противника (нпр. убацивање рачунарских вируса у војне системе противника).

Стратегијско сајбер ратовање (*Strategic Cyberwar*), Либицки види као војну акцију у којој један ентитет изводи сајбер нападе на други. Може бити и једностран. Оперативно сајбер ратовање (*Operational Cyberwar*) обухвата употребу сајбер напада као допуне у оквиру класичног, физичког рата односно представља подршку класичним војним операцијама. Иако не представља основну снагу у сукобу, може бити одлучујући умножавач моћи ако се пажљиво и прецизно планира. Сајбер одбрана (*Cyberdefense*) укључује све што је неопходно да нападач не би имао користи и успеха у својим покушајима.[74]

Државе се могу наћи у сајбер рату на два начина. Кроз намерну провокацију или кроз ескалацију. Може се јавити намерно, када једна страна сматра да може постићи предност над другом прекидањем или ометањем њених информационих инфраструктура. Може се водити и као последица ескалације кризе. Сврха (циљ) може бити да се натера противник да се покори нечијој вољи, да се избегне ескалација у насиље и сл.[75]

Сиромашне земље имају довољно паметних људи да озбиљно угрозе државу која је богатија и зависнија од информационо-комуникационих технологија. Надмоћ у сајбер простору (*cybersupremacy*) је немогуће постићи. Обе стране, у исто време, желе држати једни друге ван својих мрежа.[76]

Сајбер ратовање може играти три кључне улоге:[77]

[73] *Idem*, p. 117.
[74] *Idem*, p. 8, 118..
[75] *Idem*, p. 118.
[76] *Idem*, p. 122, 141.
[77] *Idem*, p. 142.

– Може брзо умањити способности непријатеља, ако је постигнут ефекат изненађења;
– Може бити коришћен као ''тас на ваги'' у неизвесној ситуацији и на тај начин допринети привременој али потенцијално одлучујућој војној предности и
– Може утицати на непријатеља када је у питању поверљивост његових система.

Сајбер напади против држава су све бројнији и озбиљнији. Сајбер оружје је скоро идеално оружје које нико не сме игнорисати. За комплексне, координиране нападе, потребно је неколико година припреме. Означити сајбер напад као сајбер криминал, тероризам или некако другачије је дискутабилно јер је тешко одредити идентитет, намеру или политичку мотивацију нападача.

4.2 Разматрање сајбер безбедности у одређеним међународним организацијама (НАТО, ЕУ) и развијеним државама (САД, Кина, Велика Британија)

Бројне земље и међународне организације посвећују значајну пажњу безбедности у сајбер простору. Тако је још на НАТО самиту у Прагу, 21.11.2002. године, констатовано да "НАТО мора појачати своје способности у одбрани од сајбер напада". Члан 5 Вашингтонског споразума до сада није примењен као последица сајбер напада.

Политика сајбер одбране (*Cyber Defence Policy*) НАТО-а, усвојена 2008. године, између осталог истиче следеће:

– НАТО мора имати способности да помогне и заштити савезнике од сајбер напада;
– Савезници имају примарну одговорност за заштиту својих мрежа на националном нивоу;
– Неопходно је предузети нове мере заштите од сајбер напада као што су: постојање једног ауторитета који ће координирати националне и механизме за одговор савезника; успостављање механизама за консултације; подршка националним тимовима за одговор у случају сајбер напада...

Као приоритети НАТО-а по питању сајбер одбране наглашавају се:

– Заштита властитих мрежа;

– Помоћ земљама чланицама НАТО и

– Изградња партнерства.

НАТО је акредитовао Стручни центар за сајбер одбрану (*Cyber Defense Center of Excellence*) у Естонији 2008. године, с циљем управљања сајбер одбраном[78] у свим земљама чланицама НАТО и пружања појединачне помоћи земљама чланицама у случају њиховог захтева.

Почетком августа 2010. године почело је са радом и Одељење за нове изазове по безбедност (*Emerging Security Challenges Division – ESCD*) које ће се бавити проблемима који ће све више утицати на безбедност НАТО-а као што су: тероризам, сајбер напади, претње енергетском систему и пролиферација оружја за масовно уништавање.

На НАТО самиту у Лисабону, новембра 2010. године, усвојен је нови Стратегијски концепт (*New NATO Strategic Concept*) до 2020. године, којим су обухваћене нове претње као што су сајбер напади. На самиту је констатовано да се претње брзо увећавају и еволуирају у софистикацији. Констатовано је да управо због тога НАТО настоји да убрза развој способности за одговор на инцидент (*NATO Computer Incident Response Capability – NCIRC*) у пуну оперативну способност (*Full Operational Capability – FOC*) до краја 2012. године као и да до тада сви елементи НАТО буду под централизованом сајбер заштитом. На самиту је и дат рок да се до јуна 2011. године уради нова Политика сајбер одбране (*Cyber Defence Policy*) и припрема Акциони план за њену имплементацију.[79]

Од 16–18. новембра 2010. године је реализована вежба *''Cyber Coalition 2010''* којом је тестиран одговор на инциденте у сајбер простору, сарадња између релевантних субјеката и про-

[78]Сајбер одбрана (*Cyber Defence*) се у НАТО-у посматра као део информационог обезбеђења (*Information Assurance – IA*)

[79]Anil S., *NATO's New Cyber Defence Concept and Roadmap (Power Point Pesentation)*, Cyber Terrorism Course, Center of Excellence Defence Against Terrorism, Ankara, 15.03.2011, p. 14.

цес доношења стратегијских одлука у оквиру НАТО као организације и у земљама чланицама.

За Републику Србију је, као учесницу програма Партнерство за мир, значајно да је на састанку Политичко-војног надзорног комитета Партнерства за мир (*Political-Military Streering Committee on Partnership for Peace*), 23.3.2009. године, утврђен оквир за сарадњу о сајбер одбрани између НАТО и земаља чланица Партнерства за мир. Између осталог, констатовано да НАТО може пружити помоћ у креирању Националних тимова за одговор на инцидент (*Computer Emergency Response Team – CERT*) и других потреба из домена сајбер безбедности, у складу са индивидуалним потребама партнера. Оквир регулише циљеве, принципе и потенцијалне области сарадње, механизме и процедуре имплементације сарадње између НАТО и замаља учесница програма Партнерство за мир.[80]

Према анализама и препорукама групе експерата о новом стратегијском концепту НАТО наводи се да ће у текућој декади највероватније претње по Алијансу бити неконвенционалне, пре свих: напад балистичким пројектилима (са или без нуклеарних бојевих глава), напади од стране међународних терористичких група и сајбер напади различитих нивоа озбиљности. У анализама и препорукама се наводи да ће НАТО морати да убрза напоре у проналажењу одговора на сајбер нападе, заштити властитих комуникационих система, помоћи савезницима да унапреде способност спречавања и опоравка у случају напада као и развоју способности за ефикасну детекцију и одвраћање од сајбер напада.[81]

[80]Један од облика сарадње Републике Србије и НАТО-а јесу и вежбе "Удружени напор (*Combined Endeavor*)". Тако је и 2010. године одржана вежба на две локације *Grafenver* (Немачка) і *Konstanca* (Румунија). Циљеви вежбе били су: Достићи интероперабилност телекомуникационо-информатичких система (С4 система) између учесника-нација, идентификовање проблема и примена научених лекција при пројектовању националних система; Истаћи значај интероперабилности људства (*human interoperability*) у мултинационалном окружењу и успоставити личне контакте и пријатељске односе између учесника вежбе; Пронаћи "везе" са сличним вежбама у циљу повећања техничке интероперабилности ради смањења укупних трошкова; Промовисати нове технологије и уређаје у области телекомуникација и информатике кроз демонстрације и дискусије.

[81]*NATO 2020: Assured security – dynamic engagement*, Analysis and recommendations of the group of experts on a new strategic concept for NATO, 17 May 2010, p. 11, 17; www.nato.int/strategic-concept/expertsreport.pdf

Способност и успех НАТО-а у великој мери зависи од способности да користе општа добра (мора и океани, ваздух, свемир, сајбер простор). Управо зато, у мају 2010. године, генерал Стефан Ејбриел *(Stephane Abrial)*, командант Савезничке команде за транформацију, наредио је да се уради судија "Сигуран приступ општим добрима" како би се идентификовали изазови и рањивости које утичу на сигуран приступ и употребу општих добара од стране НАТО. Та четири подручја су од критичне важности за међународну безбедност и просперитет. Ремећење или немогућност приступа сајбер простору може имати непосредан утицај на способности НАТО да извршава своје мисије. [82]

Према изјавама Џејми Шиа (*Jamie Shea*), директора НАТО за политику и планирање, око 120 земаља тренутно има или развија офанзивне способности за сајбер напад. НАТО је научио да су сајбер напади веома ефикасни у првих 36 сати док им је након тог периода ефекат значајно смањен због предузетих мера. НАТО претрпи око 100 напада дневно што што има и својих добрих страна с обзиром да је НАТО под сталним изазовима и учи како да се одговори на претњу.[83]

Још за време Бушове администрације уочена је озбиљност проблема угрожености сајбер простора у Сједињеним Америчким Државама. Именован је Специјални саветник председника за сајбер безбедност (*Special Advisor to the President for Cybersecurity*). Касније је донета Стратегија за обезбеђење сајбер простора (фебруара 2003. године), формирано Министарство унутрашње безбедности (*Department of Homeland Security – DHS*) …[84]

Председник Обама је изјавио да су рачунарске мреже стратегијски ресурс који треба бити заштићен. То ће бити реализовано и новом владином стратегијом за спречавање сајбер напада, вођеном од стране координатора за сајбер безбедност (*cybersecurity coordinator – cyber czar*).[85] Он треба да координира

[82]Barrett M., Bedford D., Skinner E., Vergles E., *Assured access to the global commons – Maritime, Air, Space*, *Cyber*, Norfolk (Virginia, USA), 3 April 2011, p. 37.

[83]Hale J., *Cyber Attack System Proliferation*, http://www.defensenews.com/story.php?!=4550692

[84]Clarke R., Knake R., *op.cit*, p. 96.

[85]Тренутно је *Howard Schmidt* на тој позицији. Shackelford S., *op.cit.*, p. 24.

рад Пентагона, Агенције за националну безбедност (*National Security Agency – NSA*), Министарство за унутрашњу безбедност (*Department of Homeland Security*) и других агенција. Фокус његов је на спречавању *spyware*, *malware*, *spoofing*, *phishing* и *bootnets*, односно ''оружја за масовно ремећење'' (*weapons of mass disruption*).[86]

Две водеће агенције у одбрани САД од сајбер претњи су Сајбер команда (*U.S.Cyber Command – CYBERCOM*) која се налази под командом Стратегијске команде (*US Strategic Command*) и која је одговорна за одбрану војске и Министарство за унутрашњу безбедност које је одговорно за заштиту других владиних агенција. Министарство за унутрашњу безбедност прати долазни и одлазни саобраћај федералних органа, тражи малициозне програме (рачунарске црве, вирусе…). Постоји интерес Конгреса и забринутост Националне агенције за безбедност да прошири своје способности да надгледа комуникације користећи напреднији систем назван Ајнштајн (*Einstein*)[87], са чијим се тестирањем почело 2009. године, а који би требало да детектује и обезбеди контра напад (*counter attack*) када су у питању федерални системи.[88] Систем "Ајнштајн 1" (*Einstein 1)* прати проток саобраћаја, "Ајнштајн 2" (*Einstein 2*) упаде и детекцију малициозних програма, "Ајнштајн 3" (*Einstein 3*) блокирање пакета са Интернета за које се процени да су малициозни програми.[89]

Генерал Александер Кејт (*Alexander Keith*) је први директор Сајбер команде. Он је уједно и директор Националне агенције за безбедност (*National Security Agency*) која има део одговорности за одобравање и извођење сајбер напада. Главни проблем који Сајбер команда мора да реши је дилема који ауторитет може одобрити сајбер нападе тактичког нивоа који

[86]*Information Management an Arma International Publication*, September/ October 2009, p. 16; www.arma.org

[87]То је систем за детекцију напада који надгледа мрежне пролазе (*gateways*) владиних органа и агенција САД када је у питању неовлашћени саобраћај. Софтвер је развијен од стране *United States Computer Emergency Readiness Team (US-CERT)* који је оперативна "рука" *National Cyber Security Division (NCSD)* а NCSD је у саставу Министарства унутрашње безбедности.

[88]Fulghum D., *Cyberwar Confusion*, Aviation Week & Space Technology, 19.04.2010, Vol. 172, Issue 15; Database: Computers & Applied Sciences Complete

[89]Clarke R., Knake R., *op.cit*, p. 101-102.

може бити лансиран са носача авиона са напредним радарима као што је EA-18G .[90]

Након формирања Сајбер команде, Сајбер команда ваздухопловних снага (*Air Force Cyber Command*) постаје *24th Air Force*, са штабом у ваздухопловној бази *Lackland* у Тексасу. Задатак јој је да обезбеди специјално обучене и оспособљене да изводе сајбер операције, потпуно интегрисане у ваздухопловне и спаце операције. Тамо је и формиран први сајбер специјализовани обавештајни центар (*specialized cyber intelligence center*) са почетних 400 припадника.[91]

Обамина администрација размишља и да успостави Војни штаб за сајбер операције (*U.S. military's cyber-operations headquarters*) који ће бити лоциран у *Fort Meade* (*Maryland*). [92]

Респектабилна институција са аспекта разматрања сајбер претњи у оквиру Министарства одбране Сједињених Америчких Држава је и Центар за сајбер криминал (*DoD Cyber Crime Centar*) за који су везани, поред осталих, (као потчињене структуре): Лабораторија за компјутерску форензику (*DoD Computer Forensics Laboratory*) и Институт за сајбер криминал (*DoD Cyber Crime Institute*).

На основу директиве Стратегијске команде постоји пет нивоа стања (*Information Operations Condition – INFOCON*) информационих (рачунарских) система у САД[93]:

- INFOCON 5: Нормална активност. Системи се надгледају и спроводе мере заштите.
- INFOCON 4: Повећан ризик од напада. Обавезно повећано надгледање система и сви крајњи корисници морају бити сигурни да су њихови системи сигурни. Коришћење Интернета може бити ограничено само на коришћење владиних сајтова. Наглашено чување резервних копија докумената на преносиве медијуме.

[90] *Idem.*

[91] Clarke R., Knake R., *op.cit*, p. 40.

[92] Fulghum D., *Lightening War*, Aviation Week & Space Technology, 22.03.2010, Vol. 172, Issue 12; Database: Computers & Applied Sciences Complete

[93] *Information Operations Condition (INFOCON) System Procedures*, Strategic Command Directive (SD) 527-1, Department of Defense, 27.01.2006, p. 8-9.

– INFOCON 3: Ризик је идентификован. Повећана пажња а провера безбедности рачунарских мрежа је приоритет. Све *unclassified dial-up* конекције су дисконектоване.
– INFOCON 2: Ограничен напад. Напад се десио али *Computer Network Defense System* није на највишем нивоу узбуне. Мање битне мреже могу бити *offline* и може бити примењен алтернативни вид комуникација.
– INFOCON 1: Општи напад. Узбуна је на највишем нивоу. Сви компромитовани системи су изоловани од остатка мреже.

За потребе војних операција изводе се посебне операције везане за рачунарске мреже (*Computer Network Operation – CNO*) које су подељене у Нападе на рачунарске мреже (*Computer Network Attack – CNA*), Одбрану рачунарских мрежа (*Computer Network Defense – CND*) и експлоатацију рачунарских мрежа (*Computer Network Exploitation – CNE*).

Напад на рачунарске мреже се састоји од акција предузетих помоћу рачунарских мрежа ради прекидања, деградирања или уништавања рачунарских система противника. Одбрана рачунарских мрежа подразумева акције предузете употребом рачунарских мрежа да заштите, надгледају, анализирају, детектују и реагују на наовлашћене активности у оквиру информационих система и рачунарских мрежа Министарства одбране. Експлоатација рачунарских мрежа је операција реализована кроз употребу рачунарских мрежа ради прикупљања података о одређеним циљевима или рачунарским мрежама противника.[94]

Сајбер напади могу довести до прекида функционисања критичних информационих инфраструктура као што је то био случај, према извештајима CIA-a, приликом напада на систем снабдевања електричном енергијом када је дошло до прекида у више региона.[95]

[94]Paul C., *Information Operations – Doctrine and Practice*, Praeger Security International, London, 2008, p. 93-96.

[95]*Cyberspace Policy Review – Assuring a trusted and resilient Information and Communications Infrastructure*, May 2009, www.whitehouse.gov; *CIA Confirms Cyber Attack Caused Multy-City Power Outage*, www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5, CIA presentation, SANS SCADA Security Summit, January 16, 2008.

Симулирани сајбер напад извршен је у фебруару 2010. године на телекомуникациону инфраструктуру САД а били су присутни и бивши, старији, административни службеници (*senior administration officials*) и експерти за националну безбедност. Резултат је да влада САД није припремљена за сајбер напад. Сценарио је назван *''Cyber ShockWave''*. Масовно су даунлодовали "*March Madness*", апликацију која је садржала *малициозни* програм.[96]

Министарство за унутрашњу безбедност је крајем септембра 2010. године реализовало вежбу Сајбер олуја III (*Cyber Storm III*) да би се тестирао национални одговор на сајбер напад тј. установила спремност на одговор и ојачале способности у будућности. Вежба је трајала три дана уз више хиљада учесника симулирајући широкораширени напад на критичне информационе инфраструктуре. У пракси су проверени елементи ново-развијеног Националног плана на за одговор на сајбер инцидент (*National Cyber Incident Response Plan – NCIRP*). То је била прва вежба на којој је тестиран Национални центар за сајбер безбедност и комуникације (*National Cybersecurity and Communications Integration Center – NCCIC*), формиран октобра 2009. године.

Експерти сматрају да се Влада САД креће веома споро у спречавању сајбер напада.[97] *Minihan* и *McConnel*, бивши директори Агенције за националну безбедност сматрају да новоформирана Сајбер команда не може одбранити САД од сајбер напада. Пре свега зато што постојећи планови те команде и Агенција за националну безбедност не пружају заштиту компанија и других цивилних инфраструктура.[98]

Комисија тј. група експерата ''Центра за стратегијске и међународне студије за обезбеђење сајбер простора за 44. председнички мандат'' формирана је у августу 2007. године са циљем да анализира постојеће планове и стратегија и да процени шта нова администрација мора да настави, шта да мења и које нове политике морају бити усвојене и шта нови органи морају тражити од Конгреса. Извештај преставља скуп препо-

[96]O'Rourke M., *op.cit.*, p. 80.
[97]Information Management an Arma International Publication, *op.cit.*, p. 16
[98]Clarke R., Knake R., *op.cit*, p. 43.

рука за свеобухватан национални прилаз у обезбеђењу сајбер простора. Три основна закључка Комисије су[99]:

- Безбедност сајбер простора је је један од главних проблема националне безбедности Сједињених Америчких Држава;
- Акцијама и одлукама мора се поштовати приватност и слобода грађана;
- Само свеобухватна стратегија националне безбедности која обухвата националне и међународне аспекте безбедности сајбер простора учиниће САД безбеднијом.

У извештају се наводи да је штета од сајбер напада реалност. Министарство одбране, државна администрација, агенције одговорне за унутрашњу безбедност, НАСА, Национални универзитет за одбрану изложени су бројним нападима од стране различитих страних субјеката. Као најопаснији противници наводе се војне и обавештајне службе других држава. Они су софистицирани, добро опремљени и истрајни у својој намери. Нарочито су им ''интересантни'' војне технологије и вредна интелектуална имовина (дизајн, бизнис планови...).[100]

Као главни проблеми у актуелној федералној организацији наводе се: недостатак стратегијског фокуса, преклапање мисија (задатака), лоша координација и сарадња као и ''расута одговорност''.[101]

Савезна регулаторна агенција за енергетику *(Federal Electric Regulatory Agency)* је 2008. године захтевала од свих компанија из сектора енергетике да усвоје одређене мере из домена сајбер безбедности и упозорила компаније да могу бити кажњене новчаном казном од милион долара дневно ако то не учине.[102]

Дефанзивни напори у САД могу се поделити на три сегмента:[103]

---

[99]*Securing Cyberspace for the 44th Presidency, Center for Strategic and International Studies*, Washington, DC December 2008, p.1.

[100]*Idem*., p.12-13.

[101]*Idem*, p.34.

[102]Clarke R., Knake R., *op.cit*, p. 88.

[103]*Idem*, p. 131-134.

– Кичма (*Backbone*); два проблема – технички (велика количина саобраћаја) и политички (приватност). Министарство унутрашње безбедности има инсталиран систем ''Ајнштајн'' на местима где се министарства и владини огранi повезују на провајдере првог реда (*Tier 1*). Систем ''Ајнштајн'' само надгледа владине мреже. Министарство одбране има сличан систем на 16 локација где се некласификовани Интранет повезује на јавни Интернет.
– Заштита мреже снабдевања електричном енергијом. Без електричне енергије већина осталих система од којих зависе не може функционисати.[104]
– Трећи сегмент представља лична заштита (самозаштита) као што то чини Министарство одбране. Министарство одбране изводи вежбе, једном годишње, под називом ''*Cyber Storm*''. Централна обавештајна агенција (*Central Intelligence Agency – CIA*) такође, почев од 2007. године изводи вежбе ''*Silent Horizon*''.[105]

Одбрамбена тријада стопира малициозне програме са Интернета, очвршћује контролу енергетског система и повећава безбедност мрежа Министарства одбране и интегритет њеног наоружања.[106]

САД имају најсофистицираније и најкомплексније способности за сајбер ратовање, праћени Русијом, Кином, Француском... Сједињене Америчке Државе вероватно поседују најсофистицираније офанзивне способности за сајбер ратовање али постоје одређене слабости када је у питању одбрана. Кина је много више пажње посветила и одбрани и код њих одбрана значи одбрана нације а не војних мрежа. У Кини, мреже које чине кинеску инфраструктуру су контролисане од стране владе или кроз директно власништво или кроз блиско партнерство са приватним сектором. Кина има моћ да дисконектује ''свој део'' сајбер простора од остатка света што могу учинити и у евенту-

[104] *Idem*, 2010, p. 136.
[105] *Idem*, p. 146.
[106] *Idem*, p. 207.

алном конфликту. Сједињене Америчке Државе немају такве могућности и способности.[107]

Крајем 2009. године по први пут САД и Русија су отпочели разговоре о споразуму (*treaty*) око сајбер простора.[108]

Способности Кине за сајбер ратовање су у сталном порасту. У априлу 1997. године у оквиру Народноослободилачке Армије формирана је јединица за сајбер ратовање. Доминација у сајбер простору је део њиховог плана да надмаше своје противнике до 2050. године.[109]

Сајбер напади од стране Народне Републике Кине на Министарство одбране Сједињених Америчких Држава нагло су се повећали 2009. године, према изјавама у Конгресу, новембра 2009. године. Цитирајући податке добијене од Стратегијске Команде САД, у 2008. години било је 54.640 малициозних сајбер напада на Министарство одбране. Само у првој половини 2009. године било је 43.785 што представља повећање за 60%. Већина таквих активности потиче из Кине. Нагли пораст броја евидентираних напада лежи и у чињеници да су данас далеко веће могућности да се открију те претње. Према истом извештају, Војска САД потрошила је у периоду од септембра 2008. до марта 2009. године око 100 милиона долара да се одбрани од тих активности.[110]

Народна република Кина константно ради на изградњи офанзивних капацитета за сајбер ратовање као и на заштити од сајбер ратовања:

– Формирањем грађанских хакерских група;
– Бављење широкораширене сајбер шпијунаже;
– Предузимањем бројних мера у заштити властитог сајбер простора;
– Формирањем јединица за сајбер ратовање;
– Убацивањем логичких бомби у инфраструктуру САД.

[107]*Idem*, p. 121-122.
[108]Shackelford S., *op.cit.*, p. 26.
[109]*ROK Daily: China Wants Dominance in Cyber Space*, World News Connection, 21.09. 2007.
[110]McMillan R,, *Computer World*, December 7, 2009, Report: China Tied To Cyberattacks on U.S. Systems, p. 12., www.computerworld.com

Док се ангажује на изради сајбер стратегије, Народна република Кина оспособљава и хакерске групе спремне да се ангажују за државне интересе. Према подацима Комисије за економску и безбедносну оцену на релацији САД – Кина (*U.S. – China Economic and Security Review Commision*), процењује се да Кина има до 250 хакерских група, оспособљених довољно да могу представљати претњу по интересе САД у сајбер простору. Крајем 2003. године Кина је обелоданила да формира јединице за сајбер ратовање.[111]

У Уједињеном Краљевству (*United Kingdom – UK*) постоји 18 различитих организација које се баве претњама у сајбер простору. Формиран је и Центар за сајбер безбедност и операције (*Cyber Security Operations Centre – CSOC*), одговоран за координацију свих организација које се баве претњама у сајбер простору. Центар је лоциран на тајном владином месту за надгледање а фокус у раду је стављен на сајбер шпијунажу и тероризам.[112]

На нивоу Европске уније је, 1999. године основан и поново обновљен 2006. године, рад Европске радне групе о тимовима за одговор на рачунарски инцидент (*European Task Force on Computer Security Incident Response Teams, TF-CSIRT*). Поменута радна група обезбеђује форум где чланице ЕУ и суседне земље могу разменити искуства и знања. TF-CSIRT има активну улогу у формирању нових тимова за одговор на инцидент. Залажу се за стандардизацију поступака и процедура у случају одговора на инцидент у сајбер простору наводећи да се тиме значајно смањује време потребно за одговор на инцидент на ширем подручју. Последњи, 24. Састанак одржан је у Ослу, Норвешка маја 2008. године. Радна група организује обуку, семинаре, конференције, водиче и алате (као што је нпр. *Request Tracker for Incident Response – RTIR*, алат који помаже тимовима у свакодневном раду, евиденцији инцидентата, праћењу предузетих поступака приликом дешавања инцедената и слично.

Прва вежба у Европској унији *''Cyber Europe 2010''* реализована је крајем 2010. године с' циљем да се провери сарадња

[111]Clarke R., Knake R., *op.cit.*, p. 52-54.

[112]*Rally the troops for war on cyber crime*. Computing, 02.07.2009; Database: Computers & Applied Sciences Complete

између држава како би се избегао комплетан прекид међународних линкова (веза).[113] Симулацијом је постепено смањиван приступ критичним услугама да би се сагледало како државе реагују. Више од 150 експерата из 70 државних органа широм Европе учествовало је у вежби. Изложено је више од 320 инцидената. Вежба је била први, кључни корак ка повећању ''европске сајбер одбране''. Кључни изазов је био како ће државе чланице имплементирати ''научене лекције'' током вежбе. Европска агенција за информациону и безбедност мрежа (*European Network and Information Security Agency – ENISA*) ће помоћи свим земљама чланицама да изведу сличне вежбе на националном нивоу као и да побољшају заштиту критичним информационих инфраструктура.[114]

4.3 Мерење способности за сајбер ратовање

Поред САД, Русије, Кине Израела и Француске, према проценама стручњака са сајбер безбедност, постоји између 20 и 30 држава које имају респектабилне способности за сајбер ратовање (неколико држава чланица НАТО, Тајван, Иран, Аустралија, Јужна Кореја, Индија, Пакистан…)[115]Сједињене Америчке Државе су тренутно далеко рањивије на сајбер нападе од Кине и Русије. Претњу могу представљати земље и које немају развијене способности али које могу унајмити тим способних хакера. Евентуални сајбер рат у овом тренутку представља недостатак за САД, сматрају стручњаци за сајбер безбедност.[116]

Мера способности за сајбер ратовање, поред офанзивног аспекта подразумева и

[113]*First EU Cyber Security Exercise ''Cyber Europe 2010''*, http://www.enisa.europa.eu; *Europa simulates total cyber war*, http://www.bbc.co.uk/news/mobile/technology-11696249

[114]Организатори су били земље чланице, ENISA i Заједнички истраживачки центар Европске уније (*EU's Joint Research Centre – JRC*)

[115]Clarke R., Knake R., *op.cit.*, p. 59.

[116]*Idem*, p. 127-128.

– Одбрану – мера националне способности да предузме акције ако је нападнута, акције које ће блокирати или ублажити напад;
– Зависност – ослањање на рачунарске мреже и системе који могу бити рањиви на сајбер нападе.

Меру способности за сајбер ратовање *Clarke и Knake* су дали на бази процене офанзивне моћи, одбрамбених способности и зависности од рачунарских система. Зависност се односи на критичне информационе системе који немају праву замену а који су зависни од сајбер простора. Мање зависна нација добија већи резултат приликом рангирања.

– САД – сајбер напад = 8, сајбер зависност = 2, сајбер одбрана = 1; укупно: 11
– Русија – сајбер напад = 7, сајбер зависност = 5, сајбер одбрана = 4; укупно: 16
– Кина – сајбер напад = 5, сајбер зависност = 4, сајбер одбрана = 6; укупно: 15
– Иран – сајбер напад = 4, сајбер зависност = 5, сајбер одбрана = 3; укупно: 12
– С. Кореја – сајбер напад = 2, сајбер зависност = 9, сајбер одбрана = 7; укупно: 18

Кина има висок резултат за одбрану зато што има план и способности да дисконектује националне мреже од остатка сајбер простора. Сједињене Америчке Државе, према мишљењу аутора, немају ту могућност. Северна Кореја има само неколико система који зависе од сајбер простора тако да јој сајбер напад не би нанео озбиљније последице. Према мишљењу аутора од анализираних држава, највеће способности за сајбер ратовање има Северна Кореја, која има укупно 18 бодова.

III

ОДБРАНА ОД САЈБЕР НАПАДА

Безбедно окружење за све ресурсе подразумева да су ресурси (материјални нпр. хардвер или нематеријални нпр. подаци, информације) заштићени и од екстерних и од интерних претњи. Концепт сајбер безбедности подразумева заштиту материјалних или нематеријалних ИКТ ресурса од потенцијалних опасности.[117]

Приметно је појачано интересовање за сарадњом по питању сајбер безбедности, како од стране међународних организација тако и појединачних земаља, након догађаја у Естонији 2007. године.[118]

Представници Сједињених Америчких Држава, Кине, Русије, Велике Британије, Француске, Немачке, Естоније, Белорусије, Бразила, Индије, Израела, Италије, Катара, Јужне Кореје и Јужноафричке Републике су се сагласили да смање претње од сајбер напада. Споразум је потписан у седишту Уједињених нација у Вашингтону. Група је препоручила да УН направи норме прихватљивог понашања у сајбер простору. Поред тога препоручена је размена информација о националним регулативама

[117]Kizza J., *Guide to Computer Network Security*, Springer, London, 2009, p. 45-46; Solange G., *op.cit*, p.3.

[118]"Теорија црног лабуда" развијена је од стране *Nassim Nisholas Taleb*-а а односи се на непредвидиве, мало вероватне догађаје (у историји, науци, технологији..) који имају снажан утицај на људску заједницу и који након првог догађања постају вероватнији и предвидљивији. Nicholas N., *The Black Swon – The Impact of the Highly Improbable*, Random House, New York, 2007.

и стратегијама за обезбеђење сајбер простора као и повећање капацитета слабије развијених земаља у заштити њихових рачунарских система.

Негативан аспект за становишта система одбране лежи у чињеници да приватни сектор поседује око 85% глобалних рачунарских мрежа и да у пракси долази до неразумевања између државног и приватног сектора. Приватни сектор пре свега жели да спречи и избегне напад а државни да открије, гони и процесуира. починиоце. Приватни сектор може допринети у смислу пријављивања сумњивог понашања и инцидената везаних за сајбер простор односно да активно сарађују приликом процесуирања починилаца. Приватни сектор може помоћи војном сектору достављајући им податке о слабостима и пропустима њихових производа и услуга (у пракси је отежано пошто појединци тврде да се тиме нарушавају њихове пословне тајне).

Постоје бројна поља одговорности од стране различитих органа и служби. Проблем је недостатак свеобухватних информација о проблему, некоординације и неадекватне контроле (надзора).

Проблем се огледа у спорости приликом позива на акцију што је код сајбер напада нарочито изражено јер се захтева моменталан одговор.

1. Препоруке за одбрану од сајбер напада

Одбрана од сајбер напада је дуготрајан процес и захтева знатне финансијске и људске ресурсе.

Едукација професионалаца за сајбер безбедност је изузетно важна. Нужно је школовати, регрутовати и задржати експерте из домена сајбер безбедности, на универзитетима и истраживачким институцијама. Едукацијом јавног мњења је потребно радити на подизању свести о претњама у сајбер простору пошто, још увек, већи део јавности благонаклоно гледа на проблем угрожености сајбер простора.

Потребно је повећати државну новчану подршку за истраживања из домена сајбер безбедности. Нужно је реализо-

вати интезивна и непрестана истраживања нових технологија заштите које ће бити део система приликом његовог дизајнирања као и имплементација заједничких истраживачких пројеката (нпр. припрема и публикација јединственог речника термина из области сајбер безбедности). Такође је потребно повећати издвајања и ресурсе за сајбер форензику укључујући и дистрибуцију *honeypots* као замки ради неопходних анализа.

Попис ресурса и процена спремности је веома важна (процена ресурса на националном нивоу, савезника, потенцијалних непријатеља).

Нужно је имати ''Тим за одговор на инцидент'' (*Computer Incident Response Team – CIRT, Computer Emergency Response Team – CERT*) односно један ауторитет који би координирао одговором на националном нивоу. Национални тим за одговор на инцидент чини група експерата за информациону безбедност који проучавају рањивости рачунарских система, истражују дугорочне промене у мрежним системима, и пружају информације и обуку ради побољшања безбедности.

Нужно је подстицати размену информација и сарадњу између приватног и државног сектора. Потребно је, препорукама, иницијативама или законским регулативама обавезати институције у оба сектора да се придржавају одређених мера заштите информација и система.

Битан аспект је и како подстаћи земље за ниским степеном зависности од ИКТ што се реализује кроз помоћ у обуци, доношењу одговарајуће регулативе, и слично.

Потребно је имплементирати вишеструке, независне технологије заштите (*Firewall* се користи као филтер за ауторизоване кориснике; лозинка за идентификацију корисника, енкрипција спречава отицање података, бекаповање и рикавери опције су значајне ако су све баријере пробијене и уништени или модификовани подаци).[119]

Постављање сензора на право место је од изузетне важности. Идеално би било да се контролише целокупан саобраћај али је проблем огромна количина података. Смањење података кроз корелацију, фузију и визуелизацију може бити корисна

[119]Janczewski L., Colarik A., *Cyber Warfare and Cyber Terrorism*, IGI Global, Hersey (USA), 2008, p. 250.

у лоцирању проблема. Основна компонента сваког система надгледања је сензор. Сензор је уређај или програм који снима и реагује на одређене догађаје, у нашем случају мрежни саобраћај на рачунарским мрежама. Постоје различити типови система за надгледање саобраћаја са различитим функцијама као што су снимање, прикупљање, филтрирање и алармирање.[120]

Неопходно је перманентно пратити трендове о претњама и безбедности на Интернету.. Тренутно постоји неколико организација на Интернету које надгледају и обелодањују релевантне трендове и претње из домена безбедности рачунара. Неке од истакнутијих су *Computer Emergency Response Team – CERT* и *Internet Storm Center* који упозоравају о претњама на Интернету и слично. Здружени савез за анализу података на Интернету (*Cooperative Association for Internet Data Analysis – CAIDA*) је такође организација која обезбеђује алате и објављује резултате везане за надгледање Интернета. Европска унија тренутно покренула пројект (*Lobster*) за надгледање ''кичме'' (*backbone*) Интернет инфраструктуре.[121]

Хетерогеност је веома битна са аспекта спречавања искоришћавања пукотина и слабости система. Еластичност (способност враћања у претходно стање) и робустност система (да у случају напада не дође до деградације или пада целокупног система), редундантност (мултиплицирање кључних компоненти и информација), брз опоравак и реконструкција, сегментација (да одређени делови буду аутономни), централно управљање информационим ресурсима, располагање системима за одговор на инцидент су, такође, веома значајни.

Све то захтева организационе и оперативне промене. То захтева нове категорије официра и сарадника, који поседују обуку и знање како водити сајбер ратовање, офанзивно и дефанзивно. Ако њихова свест о типовима сајбер напада расте, то ће повећати њихову способност да одговоре на нове технолошке изазове.

Будуће администрације мораће да разматрају регулативе о томе који ниво сајбер напада може бити посматран као

[120] *Idem*., p. 274-276.
[121] *Idem*

чин објаве рата (*act of war*), и коју врсту војног одговора треба применити.[122] Нужно је усвојити и правила понашања за употребу ИКТ у оружаним конфликтима.

2. Заштита критичних информационих инфраструктура

Критичне инфраструктуре су ресурси, системи и мреже, физички или виртуелни, чије уништавање или онеспособљавање може ослабити националну безбедност, економску стабилност и утицати на друге аспекте нормалног функционисања друштва.

Критичне информационе инфраструктуре подразумевају услуге, рачунарске мреже и друге системе базиране на ИКТ значајни за функционисање одређене земље (економски, са аспекта безбедности и сл.). Критичне информационе инфраструктуре представљају ужи појам од критичних инфраструктура тј. представљају њихов неодвојиви део. Могу бити и у државном и у приватном сектору.

Заштита критичних инфраструктура се дефинише као стратегије, политике и спремност која је неопходна да би се одвратио, спречио или пружио одговор у случају напада на критичне ифраструктуре.[123] Заштита критичних информационих инфраструктура представља програме и активности реализовани од стране власника, корисника, оператера, научно-истраживачких институција, влада, регулаторних тела с циљем одржавања перформанси критичних информационих инфраструктура у случају отказа, напада или инцидената и минимизирање последица и времена опоравка.[124]

[122]Gates R., *Nuclear Weapons and Deterrence in the 21st Century*, address to the Carnegie Endowment for International Peace: October 28, 2008.

[123]Lewis G., *Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation*, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006, p. 4.

[124]*CI2RCO definition*, http://www.ci2rco.org

У Општем националном оквиру за заштиту критичне информационе инфраструктуре (*Generic National Framework For Critical Information Infrastructure Protection*)[125] Мануела Сутера, најбитнији задаци у заштити могу се сврстати у ''модел четири стуба'' (*four-pillar model*), као што је приказано на слици 3:

– Превенција и рано упозорење (*prevention and early warning*);
– Откривање (*detection*);
– Реакција (*reaction*);
– Управљање кризама (*crisis management*).

Слика 3: Четири стуба заштите критичних информационих инфраструктура[126]

Према истраживању компаније *Symantec*, више од половине (53%) критичних информационих инфраструктура имало је 2010. године проблема са сајбер нападима. Просечна цена напада износила је 850.000 америчких долара.[127]

[125]Suter M., *A Generic National Framework for Critical Information Infrastructure Protection*, Center for Security Studies, ETH Zurich, 2007, p. 1.

[126]Suter M., *A Generic National Framework For Critical Information Infrastructure Protection*, Center for Security Studies, ETH Zurich, 2007, p. 4.

[127]*2010 Critical Information Infrastructure Protection (CIP) Survey*, www.symantec.com Истраживање је обухватило 1580 одговора, шест различитих индустрија из 15 земаља.

Услед актуелности, значаја и озбиљности проблема, заштита критичних информационих инфраструктура је постао предмет рада многих међународних и националних организација и институција што доприноси његовом бољем познавању и сагледавању друштвене опасности.

2.1 Међународне организације и форуми

Глобална, међусобна повезаност рачунарских мрежа, захтева глобалну повезаност и у решавању проблема заштите критичних информационих инфраструктура. Међународне организације и форуми предузимају бројне активности, кроз различите иницијативе, скупове, директиве, упутства, препоруке, помоћ националним организацијама и телима. На међународном плану су предузете бројне активности, у вези са заштитом критичних информационих инфраструктура, пре свега од стране Уједињених нација, Европске уније, Организације за економску сарадњу и развој, Групе 8 и Форума за одговор на инциденте и безбедносни тимови

2.1.1 Уједињене нације (*United Nations*)

Значају улогу у оквиру Организације уједињених нација имају ''Посебне снаге за информационо-комуникационе технологије'' (*United Nations Information and Communication Technologies Task Force – UN ICT TF*) које су формиране новембра 2001. године. Основна намена UN ICT TF је да се владама и међународним организацијама обезбеди саветодавна политика ради превазилажења ''дигиталне поделе'' на глобалном нивоу.

Међународна телекомуникациона унија (*International Telecommunication Union – ITU*), са седиштем у Женеви и у чијем је чланству преко 190 земаља, је специјализована агенција Уједињених нација, одговорна за информационо-комуникационе технологије. Међународна телекомуникациона унија предузи-

ма бројне активности у циљу побољшања телекомуникационе инфраструктуре, развоја међународних стандарда, размене идеја, знања и технологија.

2.1.2 Европска унија *(European Union)*

На нивоу Европске уније предузете су бројне активности у заштити критичних информационих инфраструктура с циљем да се повећа њихова безбедност.

Акциони план, усвојен 30.03.2009. године од стране Европске Комисије базира се на пет стубова: спремност и превенција (*preparedness and prevention*), детекција и одговор (*detection and response*), ублажавање последица и одговор (*mitigation and recovery)*, међународна сарадња (*international cooperation*) и критеријуми за европске критичне инфраструктуре ин области информационо-комуникационих технологија (*Criteria for European Critical Infrastructures in the field of ICT*).[128]

Планиране активности у Акционом плану су комплементарне са ''Европским програмом за заштиту критичних инфраструктура'' (*European Programme for Critical Infrastructure Protection – EPCIP*). Кључни елемент Европског програма за заштиту критичних инфраструктура је ''Директива о идентификацији и означавању европских критичних инфраструктура'' (*Council Directive on the identification and designation of European Critical Infrastructures*), који експлицитно наглашава да је ИКТ сектор део критичних инфраструктура којима треба посветити нарочиту пажњу.[129]

Предложене акције су у складу са мерама сарадње полиције и правосудних органа у откривању, спречавању и процесуирању криминалних и терористичких активности које имају

[128] *CIIP Action Plan in its Communication on Critical information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and cyber-disruptions: enhancing preparedness, security and resilience' – COM(2009) 149*; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[129] *Council Directive on the identification and designation of European Critical Infrastructures*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

за циљ угрожавање критичних информационих инфраструктура.

Европска Комисија је, 31.03.2011. године, усвојила саопштење ''Достигнућа и следећи кораци: према глобалној сајбер безбедности'' (*Achievements and next steps: towards global cyber-security – COM(2011) 163)*. У саопштењу се описују следећи кораци који су планирани за сваку акцију на Европском и међународном плану. Дат је фокус на глобалну димензију за одговор и важност сарадње између држава чланица и приватној сектора на националном, европском и међународном плану.[130]

У Талину је 27–28. априла 2009. године одржана Министарска конференција ЕУ о заштити критичних национални инфраструктура. Закључено је, између осталог, да упркос постигнутом напретку на нивоу ЕУ и земљама чланицама мора се повећати ниво безбедности, спремности и еластичност критичних информационих инфраструктура. Констатовано је да треба порадити и на побољшању координације и сарадње уз подршку ''Агенције за европске мреже и информациону безбедност'' (*European Network and Information Security Agency – ENISA*).[131] Агенција европска мрежа и информациона безбедност формирана је са циљем обезбеђивања високог степена мрежне и информационе безбедности на нивоу Европске уније.

Поред мреже ЕНИСА значајну улогу у заштити критичних информационих инфраструктура на нивоу ЕУ има и ''Информациона мрежа за упозоравање критичних инфраструктура'' (*Critical Infrastructure Warning Information Network – CIWIN*) која помаже земљама чланицама, институцијама Европске уније, корисницима и оператерима критичних инфраструктура, да размењују информације о претњама, рањивостима и одговарајућим мерама и стратегијама за смањене ризика и заштиту критичних информационих инфраструктура.

[130]*Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security" – COM(2011) 163*; http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

[131]*European Union Ministerial Conference on Critical Information Infrastructure Protection*, Tallinn, 27-28 April, 2009.

2.1.3 Организација за економску сарадњу и развој (*Organization for Economic Cooperation and Development – OECD*)

Развој политика за заштиту критичних информационих инфраструктура (*Development of Policies for Protecting of Critical Information Infrastructure*), публикован 18. децембра 2007. године, приказује компаративну анализу политика заштите критичних информационих инфраструктура у Аустралији, Канади, Кореји, Јапану, Холандији, Великој Британији и Сједињеним Америчким Државама.[132]

Препоруке ''Комитета за информације, рачунаре и политику комуникација'' (*Committee for Information, Computer and Communication Policy – ICCP Committee*) Организације за економску сарадњу и развој, усвојене су 30. априла 2008. године предлажу низ мера за заштиту критичних информационих инфраструктура, на националном и међународном плану.[133]

2.1.4 Група 8 (G-8)

Са аспекта заштите критичних информационих инфраструктура значајан документ представљају ''Принципи за заштиту критичних информационих инфраструктура'' (*G8 Principles for Protecting Critical Information Infrastructures*) којима се препоручује да:[134]

- Државе треба да имају мреже за упозоравање по питању ранивости, претњи и инцидената;
- Државе треба да раде на подизању свести имаоца и корисника критичних информационих инфраструктура и њиховој улози у заштити истих;

[132] *Development of Policies for Protecting of Critical Information Infrastructure*, www.oecd.org/dataoecd/25/10/40761118.pdf

[133] *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*, www.oecd.org/dataoecd/1/13/40825404.pdf

[134] Principi su usvojeni 5. maja 2003. godine od strane ministara pravde i unutrašnjih poslova zemalja članica G-8. http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf

– Државе треба да испитају своје инфраструктуре и идентификују међузависности између њих да би се побољшала заштита тих инфраструктура;
– Држава треба да промовише партнерство између заинтересованих страна и државно-приватно партнерство;
– Државе треба да формирају, одржавају и тестирају кризне комуникационе мреже које ће функционисати и у случају непредвиђених ситуација;
– Државе треба да предузимају мере да се актуелне политике и друге мере примењују у заштити критичних информационих инфраструктура;
– Државе треба да помогну у праћењу трагова нападача на критичне информационе инфраструктуре и када је неопходно пруже помоћ другим државама;
– Државе треба да раде на образовању и обуци да би се увећале способности за одговор, тестира функционисање планова континуитета функционисања и подржи заинтересоване стране у сличним активностима;
– Државе треба да усвоје одговарајућу правну регулативе, примењу конвенција као што је Конвенција Савета Европе о сајбер криминалу и оспособи правна лица да могу ефикасно процесиурати починиоце;
– Државе треба да се ангажују у међународној сарадњи, размени информација, међусобној помоћи, у складу са домаћим законодавством;
– Државе треба да промовишу националне и међународне научно-истраживачке пројекте, примену одговарајућих стандарда и система за заштиту.

2.1.5 Форум за одговор на инциденте и безбедносни тимови (*Forum for Incident Response and Security Teams – FIRST*)

Форум за одговор на инциденте и безбедносни тимови[135] је широкопозната организација као глобални лидер у одговору на инцидент и обједињавању различитих тимова за одговор на инцидент (*Computer Security Incident Response Teams – CSIRTs*) у оквиру влада, трговине и економских орга-

[135] *FIRST*, www.first.org

низација. FIRST је намењен да подржи сарадњу и координацију у превенцији инцидената, брзу реакцију у случају инцидента и промовише размену информација међу члановима и што шире заједнице.

2.2 Националне организације

Анализом заштите критичних и критичних информационих инфраструктура приметно је да није дефинисана јасна разлика у многим земљама као и да не постоји званична листа критичних информационих инфраструктура. Друштвено политички, историјски, географски и други фактори у значајној мери утичу на то да ли је неки сектор критичан или не. Само неколико земаља (САД, Француска…) имају централизоване владине организације за заштиту критичних информационих инфраструктура. У већини земаља, одговорност лежи у више ауторитета и организација у више владиних институција. Општи тренд по питању раног упозоравању у случају угрожавања критичних информационих инфраструктура јесте у формирању централних тачака за безбедност информационих система и мрежа. То су најчешће различите форме Тимова за одговор на инцидент који пре свега размењују информације у оквиру FIRST.[136]

2.2.1 Сједињене Америчке Државе

За координацију заштите критичних инфраструктура (критичних информационих инфраструктура) одговорно је Министарство унутрашње безбедности (*Department of Homeland Security – DHS*) које је формирано 2002. године а на основу Националне стратегије за унутрашњу безбедност (*National Strategy for Homeland Security*)[137] и Акта унутрашње безбедности (*Homeland Security Act*).[138]

[136]Bruner E., Suter M., *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich, p. 527-544.

[137]*National Strategy for Homeland Security*, www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

[138]*Homeland Security Act*, www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

Заштита критичних инфраструктура је комплексан задатак. Већина критичних инфраструктура у САД је у приватном власништву што има за последицу да је државно-приватно партнерство битно за заштиту и отпорност критичних инфраструктура као и за ефикасан одговор.

"Преседничка директива о унутрашњој безбедности" (*Homeland Security Presidential Directive – (HSPD-7)*[139] идентификује 17 критичних инфраструктурних сектора. Наведена директива допушта Министарству унутрашње безбедности да идентификује празнине у постојећим систему организовања критичних инфраструктура и формира нове секторе да би се попунила та празнина. На основу тога је, марта 2008. године формиран, нови 18.-и, Сектор критичне производње (*Critical Manufacturing Sector*). За сваки од 18 сектора формира се посебна агенција (*Sector-Specific Agencies*) која израђује специфичне планове (*Sector-Specific Plan*) за примену Националног плана заштите инфраструктуре за сваки сектор. Секторе критичних инфраструктура чине:[140]

– Пољопривреда и храна (*Agriculture and Food*);
– Комерцијална постројења (*Commercial Facilities*);
– Бране (*Dams*);
– Енергија (*Energy*);
– Информациона технологија (*Information Technology*);
– Поштански и шпедитерски сектор (*Postal and Shipping*);
– Банкарство и финансије (*Banking and Finance*);
– Комуникације (*Communications*);
– Постројења одбрамбене индустрије (*Defense Industrial Base*);
– Објекти Владе (*Government Facilities*);
– Национални споменици и обележја (*National Monuments and Icons*);
– Транспортни системи (*Transportation Systems*);

[139] *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*; http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

[140] *Critical Infrastructure Sector*, http://www.dhs.gov/files/programs/gc_1189168948944.shtm

– Хемикалије (*Chemical*);
– Критична производња (*Critical Manufacturing*);
– Енергетске услуге (*Energy Services*);
– Здравствена заштита и јавно здравље (*Healthcare and Public Health*);
– Нуклеарни реактори, материјали и отпад (*Nuclear Reactors, Materials and Waste*);
– Вода (*Water*).

Идентификација претњи и рањивости, државно-приватно партнерство као и друге значајне активности остварују се кроз "Национални план заштите инфраструктуре" (*National Ifrastructure Protection Plan – NIPP*)[141] и низ других програма и активности. Национални план заштите инфраструктуре успоставља партнерство између 18 критичних инфраструктурних сектора за идентификацију ресурса, система, мрежа и функција чији губитак или компромитовање представља највећи ризик. Национални план заштите инфраструктуре обезбеђује основ за повећање способности за одговор и опоравак у случају ванредних догађаја. Анексом "Критична инфраструктура и подршка кључним ресурсима" (*Critical Infrastructure and Key Resources Support Annex*) успостављена је веза између "Националног плана заштите инфраструктуре" и "Оквирног националног одговора" (*National Response Framework – NRF*).[142]

У оквиру Министарства унутрашње безбедноста постоји "Директорат за анализу информација и заштиту инфраструктуре" (*Directorate for Information Analysis and Infrastructure Protection – IAIP*) у чије саставу је "Одељење за националну сајбер безбедност" (*National Cyber Security Division – NCSD*) намењено да идентификује, анализира и смањи сајбер претње и рањивости, шаље информације о упозоравању и координира одговор на инцидент и пружа помоћ у изради планова за обезбеђивање континуитета функционисања и опоравка. Оперативно тело "Одељења за на-

[141] *National Infrastructure Protection Plan*, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[142] Оквир за национални одговор (*National Response Framework – NRF*) односи се на управљање унутрашњим инцидентима (*domestic incident management*).

ционалну сајбер безбеднодност" представља "Тим за одговор на инцидент" (*US Computer Emergency Readiness Team – US CERT*).

Поред Министарства унутрашње безбедности значајну улогу у заштити критичних информационих инфраструктура имају и други федерални органи: Национални институт за стандарде и технологију (*National Institute of Standards and Technology – NIST*), Министарство правде (*Department of Justice – DoJ*), Министарство одбране (*Department of Defense – DoD*)...

У оквиру Министарства правде постоји Национални центар за заштиту инфраструктуре (*National Infrastructure Protection Center – NIPC*) и Федерални истражни биро (*Federal Bureau of Investigation – FBI*). У оквиру Министарства одбране, значајну улогу има Агенција за развој напредних истраживања из области одбране (*Defense Advanced Research Projects Agency – DARPA*), Тим за одговор на инцидент у копненој војсци (*Army Emergency Response Team – ACERT*), Тим за одговор на инцидент у ваздухопловним снагама (*Air Force CERT*).

Систем за управљање, контролу и прикупљање података (*Supervisory, Control And Data Acquisition – SCADA*) представља дистрибуирани контролни систем (*Distributed Control System – DCS*) кога чини скуп хардверских и софтверских компоненти, политика, стандарда и процедура. Ослања се на комуникационе мреже које повезују удаљене терминалске јединице (*Remote Terminal Units – RTUs*) са главном терминалском јединицом (*Master Terminal Unit – MTU*) из које се надгледају и контролишу удаљени елементи.[143]

2.2.2 Русија

"Доктрина информационе безбедности Руске Федерације" усвојена је 9. септембра 2000. године и представља проширење "Националног концепта безбедности" (*National Security Concept*) који је усвојен 10. јануара 2000. године с циљем да ојача државну политику по питању информационе безбедности.[144]

Главне организације одговорне за информациону безбедносту у Русији су Савет за безбедност Руске Федерације (*Security*

[143]Lewis G., *op.cit.*, p. 223.
[144]Bruner E., Suter M., *Idem*, p. 339.

Council of the Russian Federation), Федерална служба безбедности (*Federal Security Service of the Russian Federation – FSB*), Федерална гарда (*Federal Guard Service of the Russian Federation*), Федерална техничка и служба контроле извоза (*Federal Technical and Export Control Service*) и Министарство информационих технологија и комуникација (*Ministry of Information Technologies and Communications*). За државно-приватну сарадњу одговорно је Руско удружење мрежа и услуга (*Russian Association of Networks and Services – RANS*) и Програм електронског развоја (*Russian e-Development Partnership – PRIOR*).[145]

На националном нивоу у Руској Федерацији постоји Тим за одговор на инцидент (*Computer Security Incident Response Team – RU CERT*).

2.2.3 Велика Британија

У Великој Британији, главна одговорност за заштиту критичних информационих инфраструктура је на Секретару за унутрашњу политику (*Home Secretary*). Многи други органи имају улогу у заштити различитих сектора. Њихова координација се врши од стране Центра за заштиту националних инфраструктура (*Centre for the Protection of the National Infrastructure – CNPI*).[146] Центар за заштиту националних инфраструктура је формиран 1. фебруара 2007. године спајањем Центра за координацију безбедности националних инфраструктура (*National Infrastructure Security Co-ordination Centre – NISCC*) и Центра за саветовање по питањима националне безбедности (*National Security Advice Centre – NSAC*). Политика заштите критичних информационих инфраструктура је донешена и дистрибуирана од стране више владиних органа и тела укључујући Центар за заштиту националних инфраструктура, Централну подршку за информационо обезбеђење (*Central Sponsor for Information Assurance – CSIA*), Владино одељење за безбедносну политику (*Cabinet Office Security Policy Division*), Канцеларију за унутрашњу политику (*Home Office*), Владин штаб за комуникације (*Government Communications Headquarters – GCHQ*).[147]

[145] *Idem*, p. 347.
[146] *Centre for the Protection of the National Infrastructure,* www.cnpi.gov.uk
[147] Bruner E., Suter M., *op.cit*, p. 424.

2.2.4 Француска

У Француској, Генерални секретар националне одбране (*Secretary-General of National Defense – SGDN*), који је везан за Кабинет премијера, има комплетну одговорност за заштиту критичних инфраструктура. У оквиру министарства одбране, кључне организације одговорне за заштиту критичних (информационих) инфраструктура су Централни директорат за безбедност информационих система (*Central Directorate for Information Systems Security – DCSSI*) и саветодавна Канцеларија (*Advisory Office*) док Централна служба за борбу против високотехнолошког криминала (*Central Office for the Fight Against Hi-Tech Crime*) има главну улогу у оквиру Министарства унутрашњих послова. За реализацију сарадње између државног и приватног сектора одговоран је Стратегијски саветодавни одбор за информационе технологије (*Strategic Advisory Board on Information Technologies – CSTI*).[148]

2.2.5 Немачка

Потпуна одговорност за заштиту критичних (информационих) инфраструктура је на Министарству унутрашњих послова (*BMI*), заједно са неколико својих потчињених агенција, као што је Федерална служба за информациону безбедност (*BSI)*, Федерална служба за заштиту цивила и помоћ у несрећама (*BBK*), Федерална агенција криминалистичке полиције (*BKA*) и Федерална полиција (*BPOL*). За координацију између наведених агенција, у Министарству унутрашњих послова, формирана је, 2002. године, Посебна јединица за заштиту критичних инфраструктура (*AG KRITIS*). Развој стратегија и других активности се координирају са другим федералним министарствима (Федерално министарство одбране, Федерално министарство правде, Федерално министарство иностраних послова, Федерално министарство економије и технологије и других релевантних агенција.[149]

У Националној стратегији за заштиту критичних инфраструктура Савезне Републике Немачке се наводи да критичне

[148]Bruner E., Suter M., *op.cit*, p. 150.
[149]*Idem*, p. 169.

инфраструктуре чине организационе и физичке структуре и средства од виталне важности за друштво и економију тако да њихово прекидање и деградирање може довести до недостатка њиховог напајања, значајног ремећења друштвене сигурности или других драматичних последица.[150]

Критичне инфраструктуре могу бити изложене спектру претњи коју се могу, условно, сврстати у следеће групе:[151]

– Елементарне непогоде (екстремни временски услови, пожари, потреси, епидемије, пандемије, космички догађаји и сл.);
– Технички пропусти/људске грешке (системски пропусти, немар, организациони пропусти и сл.);
– Тероризам, криминал, рат.

Да би заједничка акција била успешна, непходне су стратегијске смернице битне за заштиту критичних инфраструктура а које се тичу свих релевантних ризика. На бази смерница, могуће је утврдити подциљеве, који ће бити специфицирани и имплементирани кроз програме, планове или концепте. Тако у ИТ сегменту, такав план већ постоји у облику Националног плана за заштиту знформационих знфраструктура (*National Plan for Information Infrastructure Protection – NPSI*).[152]

Конзистентна имплементација циљева реализује се у форми кружног циклуса управљања ризицима у критичним инфраструктурама: Превенција – Имплементација – Вежбе – Одговор – Анализа – Евалуација (*Prevention – Implementation, Exercises – Response – Analysis – Evaluation*).[153]

У Стратегији се захтева заједничко ангажовање и имплементација Стратегије на федералном и локалном нивоу, у складу са областима одговорности. Сет инструмената за имплементацију Стретегије подразумева[154]:

– Програми и планови (нпр. *Network, Control Program, Packet Switching Interface – NPSI*);

[150] *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Ministry of Interior, Federal Republic of Germany, Berlin, 17th June, 2009, p. 4.
[151] *Idem*, p. 9.
[152] *Idem*, p. 12.
[153] *Idem*, p. 13.
[154] *Idem*, p. 16-17.

– Одређене препоруке за деловање (нпр. *National Baseline Protection Concept* као основни водич за физичку заштиту критичних инфраструктура);
– Стандарди, норме и регулативе (нпр. *BSI Information Security Standards*).

2.2.6 Италија

Главно владино тело у Италији одговорно за заштиту критичних информационих инфраструктура је Министарство унутрашњих послова (*Postal and Communications Police*) и Министарство иновација и технологија (*Ministry of Innovation and Technologies*). Министарство комуникација је такође укључено у различитим активностима у циљу побољшања информација и комуникационих мрежа. За остваривање сарадње између државног и приватног сектора најважнију улогу има Удружење италијанских експерата за критичне инфраструктуре (*Associazione Italiana Esperti in Infrastrutture Critiche*), тј. Експертска група практичара из државног и приватног сектора.[155]

2.2.7 Норвешка

У Норвешкој, министарство или орган који је одговоран за функционисање институције на цијем је челу у мирнодопско време такође је одговоран и за њено функционисање у време кризе или рата. То се такође односи и на заштиту критичних информационих инфраструктура. За координацију у цивилном сектору је одговорно Министарство правде и полиције. Општи ауторитет за безбедност ИКТ је Министарство администрације Владе и реформе (*Ministry of Government Administration and Reform*). Министарство одбране је одговорно за безбедност у војном сектору. Министарство транспорта и комуникација има одговорност за комуникациони сектор у Норвешкој укључујући све аспекте безбедности. У циљу промовисања државно-приватног партнерства, Национали координациони савет за информациону безбедност (*National Information Security Coordination Council – KIS*) сарађује са приватним сектором.[156]

[155]Bruner E., Suter M., *op.cit*, p. 215
[156]*Idem*, p. 314.

2.2.8 Република Србија и земље у окружењу

Иако је последњих година у Републици Србији и земљама у окружењу постигнут значајан напредак у развоју информационог друштва и употреби информационо-комуникационих технологија приметно је да тај део Европе, ''каска'' у активностима по питању заштите критичних информационих инфраструктура, нарочито у односу на земље чланице Европске уније (Мађарска, Словенија, Бугарска, Румунија) и Хрватске која је најприближнија остварењу тог циља. Нити у једној од разматраних земаља (Србија, Мађарска, Румунија, Бугарска, Хрватска, Словенија, Босна и Херцеговина, Македонија, Црна Гора, Албанија) не постоји попис критичних информационих инфраструктура. Министарство или орган који је одговоран за функционисање институције на чијем је челу у мирнодопско време такође је одговоран и за њено функционисање у време кризе или рата. То се такође односи и на заштиту критичних информационих инфраструктура.

Од земаља у окружењу Тим за одговор на инцидент имају Мађарска (*Hungarian governmental Computer Emergency Response Team*), Румунија (*CERT-DRT*), Бугарска (*CERT Bulgaria*), Хрватска (*Croatian National CERT*, *Croatian Academic and Research Network – CARNet CERT*) и Словенија (*Sl-CERT*). Тимови за одговор на инцидент обезбеђују смернице, препоруке и помоћ у примени превентивних мера заштите, националних, јавних информационих система као и одговор на инцидент у случају да се деси, пре свега ако се једна од страна у инциденту налази у националном домену односно националном IP адресном простору.

Проблем заштите критичних информационих инфраструктура у Републици Србији и окружењу представљају следеће чињенице:

- Недостатак националне организације за координацију заштите критичних информационих инфраструктура;
- Недостатак обученог људства;
- Недостатак неопходних техничких алата за одговор у случају напада на критичне информационе инфраструктуре;
- Недостатак механизама за контакт за релевантним институцијама у земљи и регији;

– Недостатак националне стратегије за одбрану од претњи у сајбер простору (изузев Румуније).

Позитиван помак у заштити критичних информационих инфраструктура и смањивању претњи у сајбер простору представља чињеница да је у Републици Србији и земљама у окружењу потписана и ратификована Конвенције Савета Европе о сајбер криминалу.

3. Стратегије за обезбеђење сајбер простора

Стратегије за обезбеђење сајбер простора дају оквир у организовању и одређивању приоритета, смањивању националне рањивости напада на критичне информационе инфраструктуре и имплементацијом, значајно доприносе повећању безбедности у сајбер простору.

У Стратегији националне безбедности Руске Федерације до 2020. године, наводи се да на заштиту националних интереса Руске Федерације могућ негативан утицај могу имати, поред осталих, и различите незаконите активности из домена кибернетике, односно високих технологија.[157]

3.1 Национална стратегија за обезбеђење сајбер простора (National Strategy to Secure Cyberspace) Сједињених Америчких Држава

Национална стратегија за обезбеђење сајбер простора дефинише почетне циљеве за организацију и додељивање приоритета. Нуди смернице министарствима и агенцијама које имају своју улогу у обезбеђењу сајбер простора. Такође указује на кораке које локалне власти, приватне компаније и организације, грађани могу да следе да би побољшали безбедност у

[157] *Стратегији национал но безопасности Росси ско Федерации до 2020 года*, http://www.scrf.gov.ru/documents/99.html

сајбер простору. Стратегија истиче значај повезивања јавног и приватног сектора. Наглашава се да ће динамичност промена у сајбер простору захтевати преправке и амандмане у Стратегији током времена.[158]

Америчка економија и национална безбедност потпуно зависе од информационе технологије и информационе инфраструктуре. У самом средишту информационе структуре од које зависе је Интернет. Мноштво злонамерних учесника изводи нападе на критичне информационе инфраструктуре. Од највећег значаја је претња од организованих напада у сајбер простору који су у стању да онеспособе националне инфраструктуре, економију или националну безбедност.[159]

Током оружаног сукоба или кризе, непријатељ може покушати да застраши политичке лидере нападима на критчне инфраструктуре и кључне економске функције или рушећи поверење људи у информационе системе. Сајбер напади на рачунарске системе САД могу имати озбиљне последице попут ометања критичних операција, узрокујући губитак прихода и интелектуалне својине, или чак губитком живота.[160]

У Стратегији се наводи да критичне инфраструктурне чине јавне и приватне институције у секторима пољопривреде, прехране, воде, здравства, хитних служби, владе, одбране, информација и телекомуникација, енергетике, саобраћаја, банкарства и финансија, хемијских и опасних материјала, поште и шпедиције. Сајбер простор је њихов нервни систем – контролни систем државе.[161]

Као стратегијски циљеви у ''Националној стратегији за обезбеђење сајбер простора'' се наводи следеће[162]:

– Спречити сајбер нападе на америчке критичне инфраструктуре;

– Смањити националну рањивост на сајбер нападе и

[158]*The National Strategy to Secure Cyberspace*, The White House, February 2003, p. 8. www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[159]*Idem.*

[160]*Idem*

[161]*Idem*, p. 7.

[162]*Idem* p. 8.

– Минимизирати штету и време потребно за опоравак уколико се деси напад.

Као приоритети за повећање безбедности у сајбер простору наводе се следећи елементи:[163]

– Национални систем за одговор по питању безбедности у сајбер простору:
– Национални систем за смањивање безбедносних претњи и рањивости у сајбер простору;
– Национални програм обуке и подизања свести по питању безбедности у сајбер простору;
– Заштита рачунарских система Владе у сајбер простору;
– Сарадња на националном и међународном нивоу по питању безбедности у сајбер простору.

3.2 Стратегија сајбер безбедности Велике Британије (Cyber security strategy of the UK)

Безбедност сајбер простора је поред тероризма и пандемије грипа, једна од главних опасности наводи се у Националној стратегији безбедности Велике Британије (*National Security Strategy of the United Kingdom*).

Зависност Велике Британије од сајбер простора расте тако да безбедност сајбер простора постаје све битније питање по нацију. Претње из сајбер простора варијају од фишинга до шпијунаже. Такве активности могу утицати на организације, појединце, критичне инфраструктуре, пословање, функционисање владе. Стратегија препознаје изазове сајбер безбедности и потребе да им се посвети пажња. То условљава потребу свеобухватног приступа сајбер безбедности у којем Влада, организације, грађани као и међународни партнери имају своју улогу.[164]

[163] *Idem*, p. 10.

[164] Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space, *op.cit.*, p. 3.

Стратегија наглашава потребу да се Влада, организације кроз секторе, међународни партнери и грађани ангажују заједно на реализацији стратегијских циљева смањивања ризика и искоришћавању прилика побољшањем знања, способностима и доношењем одлука ради обезбеђивања преимућства (надмоћи) у сајбер простору.[165]

Смањивање ризика се остварује:

– Смањивањем мотивације и способности непријатеља;
– Смањивањем рањивости сајбер простора;
– Смањивањем утицаја сајбер операција на интересе Велике Британије;
– Искоришћавањем прилика у сајбер простору;
– Прикупљањем обавештајних података о актерима који представљају претњу;
– Пружањем подршке за политике Велике Британије;
– Интервенисањем против непријатеља;
– Побољшањем знања, способности и доношења одлука;
– Унапређењем знања и подизањем свести;
– Развојем доктрине и политике;
– Развојем управљања и доношења одлука;
– Повећањем техничких и људских способности.

Да би се бавила изазовима по безбедност у сајбер простору, Влада Велике Британије ће:[166]

– Успоставити међувладин програм који упућује на приоритетне области у испуњавању циљева из домена сајбер безбедност, укључујући обезбеђивање додатних средстава за развој нових технологија за заштиту мрежа у Великој Британији; развој и унапређење раста критичних вештина.
– Развити блиску сарадњу са ширим јавним сектором, индустријом, групама које се баве грађанским слободама, грађанима и међународним партнерима.
– Успоставити Уред за сајбер безбедност (*Office for Cyber Security – OCS*) да би се обезбедило стратегијско вођење и доследност у Влади

[165] *Idem*, p. 4.
[166] *Idem*, p. 5.

– Креирати Оперативни центар за сајбер безбедност (*Cyber Security Operations Centre – CSOC*) који ће: активно надгледати сајбер простор и координирати одговор на инцидент; омогућити боље разумевање напада на мреже и кориснике у Великој Британији; анализирати трендове и побољшати координацију одговора на инцидент; обезбедити боље саветовање и информисање о ризицима за пословање и грађане.

Влада годинама предузима мере да заштити сајбер простор. Стратегија националне информационе сигурности (*National Information Assurance Strategy*), представља први корак за Велику Британију у обезбеђењу интегритета, расположивости и поверљивост информационо-комуникационих система и информацијама којима се уз помоћ истих приступа.[167]

У Стратегији се наводи да Велика Британија све више зависи од сајбер простора. Сајбер простор се константно шири, омогућавајући бројне и различите користи. Међутим, са растућом зависношћу долази и до већих претњи и ризика. Зато, Велика Британија мора водити доследан (*coherent*) одговор на безбедносне изазове који проистичу из ризика и претњи а стратегијски приступ је основа за постизање тог циља.[168]

3.3 Стратегија сајбер безбедности Немачке (Cyber security strategy for Germany)

У Стратегији сајбер безбедности Немачке се наводи да је расположивост сајбер простора и интегритет, поверљивост и доступност података и информација у сајбер простору, од виталног значаја у 21. веку. Стога, безбедност сајбер простора представља централни изазов за државе, пословање и друштва уопште, како на националном тако и на међународном плану. Стратегија за обезбеђење сајбер простора представља оквир који то омогућава. Повећање комплексности и рањивости ин-

[167]Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space, *op.cit*, p. 11.

[168]Idem, p. 9.

формационих инфраструктура условиће да безбедност у сајбер простору буде веома значајно питање и у будућности.[169]

Основни принципи безбедности у сајбер простору су: свеобухватни приступ, размена информација, координација.[170]

Фокус у повећању безбедности у сајбер простору дат је на 10 стратегијских циљева:

– Заштита критичних информационих инфраструктура;
– Заштита ИТ система у Немачкој;
– Побољшање ИТ безбедности у државној администрацији;
– Формирати Национални центар за одговор (*National Cyber Response Centre*);
– Формирати Национални савет за сајбер безбедност (*National Cyber Security Council*);
– Ефикасно контрола криминала и у сајбер простору;
– Ефикасна координација акција да би се осигурала безбедност сајбер простора у Европи и свету;
– Употреба поузданих и поверљивих информационих технологија;
– Развој особља за рад у федералним органима;
– Алати за одговор на сајбер напад.[171]

У Стратегији се наводи да и да ће услед сталних промена у сајбер простору, Федерална Влада преко Националног савета за сајбер безбедност ће прилагодити циљеве и мере датим околностима и условима.[172]

[169]*Cyber Security Strategy for Germany*, Federal Ministry of Interior, February 2011, p. 2-3; www.bmi.bund.de
[170]*Idem*, str. 4-5.
[171]*Idem*, str. 6-12.
[172]*Idem*, str. 13.

ЗАКЉУЧАК

Развојем информационо-комуникационе технологије појавили су се нови облици друштвених активности који утичу на сваки сегмент живота људи. Информационо-комуникациона технологија довела је до бројних предности, али носи и одређене опасности у сајбер простору, окружењу које формирају рачунарске мреже. Сајбер простор, својим карактеристикама, пружа повољне услове за криминално понашање појединаца или група.

Докле год војна и економска моћ зависи од рачунарских мрежа, и нарочито ако им је могуће приступити с вана, ризик постоји. Услед тренда све веће економске, војне и уопште друштвене зависности од информационо-комуникационе технологије и тренда међусобног повезивања рачунарских мрежа, претње у сајбер простору представљају проблем који ће расти великом брзином и у догледној будућности.

Утицај информационо-комуникационе технологије се не сме потцењивати. Познавањем ИКТ и могућности злоупотребе представља полазну основу у избору средстава и метода за њихово успешно онеспособљавање. Пример свакако представљају *firewall* и системи за детекцију напада који су све бољих карактеристика, веће стабилности и обухватности. Трендови су усмерени и на интеграцију система заштите, развој нових протокола и система криптовања.

У супростављању претњама у сајбер простору посебан акценат је дат на проактивно деловање. У случају да поред предузетих мера дође до инцидента мора постојати оспособљено

људство које ће прикупити све релевантне податке о инциденту који могу довести до починиоца и процесуирања случаја. Подаци се могу добити са различитих мрежних уређаја (*firewall*, рутери, сервери, системи за детекцију напада) и оперативних система. Оспособљено људство је неопходно и ради конфигурације и инсталације наведених елемената да би се такве активности детектовале и прикупили релевантни и прихватљиви докази.

Најбоље резултате у истрази даје тимски рад при чему је сваки сегмент веома важан да би се процесуирали починиоци. Због саме природе дигиталних доказа (неопипљив, осетљив, тешко видљив) њихово прикупљање није ни мало лако и захтева оспособљено људство које их неће обрисати или оштетити да би били прихватљиви, као доказни материјал, на суду. Због тога, прикупљање дигиталних доказа не захтева само техничко знање већ и познавање закона који се односе на доказе. Чак и уколико се догоди да се подаци обришу или оштете, применом одређених алата могу се вратити у претходно стање. Да би докази били прихватљиви на суду, важан корак представља и придржавање прописаних стандарда као и употреба лиценцираних и проверених алата.

Важан корак у супростављању претњама у сајбер простору представља и повећање свести корисника о његовој штетности јер је у информационом друштву информација постала роба која се скупо плаћа. Од стратегијског значаја је и идентификовање критичних националних инфраструктура које могу бити угрожене, стална размена информација и искустава као и сарадња између приватног и државног сектора.

Да би се могло ефикасно супроставити претњама у сајбер простору нужно је стално оспособљавати људство, формирати специјалне тимове (националне и мултинационалне – *Multinational Computer Emergency Response Team – MCERT*) и предузимати друге активности како би се стално ''држао корак'' са развојем информационо-комуникационе технологије (побољшати безбедност производа и услуга, формирати национални центар за упозорење и др.).

Изузетно важан корак у супростављању претњама у сајбер простору јесте усвајање националне стратегије за обезбеђење сајбер простора и одговарајуће законске регулативе.

Упркос напорима оних који се баве безбедношћу, ни један степен јачања система не може са сигурношћу обезбедити да ће систем који је прикључен на отворену мрежу бити нерањив на нападе. Не постоји нити један рачунарски систем који је у потпуности безбедан и који нема рањивости тј. апсолутна заштита није могућа.

Напади на војне системе су најефикаснији када су део борбених операција. Тешко је одредити колике штете од сајбер напада могу бити. Оне варирају од неколико милијарди долара до неколико стотина милијарди долара годишње. Сајбер ратовање је нејасно и веома ретко је могуће одредити шта су намерне а шта колатералне штете. Идентитет као и мотивацију нападача је, такође, тешко одредити.

На основу свега изнетог, може се закључити да су претње у сајбер простору у сталној еволутивности. Галопирајући развој ИКТ, која преображава нашу планету, чини претње у сајбер простору недовољно истраженим, што може послужити као основ за даља истраживања.

ЛИТЕРАТУРА

1. Алексић Ж., Миловановић З., *Лексикон криминалистике*, Глосаријум, Београд, 1995.
2. Anil S., *NATO's New Cyber Defence Concept and Roadmap (Power Point Pesentation)*, Cyber Terrorism Course, Center of Excellence Defence Against Terrorism, Ankara, 15.03.2011.
3. Barrett M., Bedford D., Skinner E., Vergles E., *Assured access to the global commons – Maritime, Air, Space*, *Cyber*, Norfolk (Virginia, USA), 3 April 2011.
4. Berkowitz B., Hahn R.**,** *Cyber security: Who's watching the store?***,** Issues in Science and Technology, www.issues.org/19.3/berkowitz.htm
5. Blyth A., Kovacich G., *Information Assurance*, Springer, London, 2006.
6. Bruner E., Suter M., *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich.
7. *Centre of Excellence Defence Against Terrorism*, Responses to Cyber Terrorism, IOS Press, Ankara (Turkey), 2007.
8. *Centre for the Protection of the National Infrastructure,* www.cnpi.gov.uk
9. Цетинић М., *Комйуйерска кривична дела и њихови йојавни облици*, Правни живот бр 10, Удружење правника Србије, Београд, 1998.

10. *CIA Confirms Cyber Attack Caused Multy-City Power Outage*, www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5, CIA presentation, SANS SCADA Security Summit, January 16, 2008.
11. *CI2RCO definition*, http://www.ci2rco.org
12. *CIIP Action Plan in its Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attack and cyber-disruptions: enhancing preparedness, security and resilince' – COM(2009) 149,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
13. Clarke R., Knake R., *Cyber War – The next treat to National Security and What to do about it*, HarperCollins e-books, 2010.
14. Collin B., *The Future of Cyberterrorism*, http://afgen.com/terrorism1.html
15. *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security" – COM(2011) 163*; http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm
16. *Computing Dictionary* http://computingdictionary.thefreedictionary.com/cyberspace
17. Conway M., *Reality Bytes: Terrorist Use of Internet*, http://www.firstmonday.dk/issue7_11/conway
18. *Council Directive on the identification and designation of European Critical Infrastructures*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
19. Coyne R., *Designing information technology in the postmodern age: From method to metaphor*, MIT Press, Cambridge, 1995.
20. *Critical Infrastructure Sector*, http://www.dhs.gov/files/programs/gc_118916 8948944.shtm
21. *Cyberspace Policy Review – Assuring a trusted and resilient Information and Communications Infrastructure*, May 2009, www.whitehouse.gov
22. *Cyber Operations and Cyber Terrorism*, DCSINT Handbook No. 1.02, 15 August 2005.

23. *Cyber Security Strategy*, Ministry of Defence Estonia, Tallinn, 2008.
24. *Cyber Security Strategy for Germany*, Federal Ministry of Interior, February 2011, www.bmi.bund.de
25. *Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space*, UK Office of Cyber Security – UK Cyber Security Operations Centre, June 2009.
26. Denning D., *Is Cyber Terror Next?*, New York, U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm
27. Denning D., *"Reflections on Cyberweapons Controls"*, www.cs.georgetown.edu/~denning/infosec/cyberweapons-controls.doc
28. *Development of Policies for Protecting of Critical Information Infrastructure*, www.oecd.org/dataoecd/25/10/40761118.pdf
29. Дракулић М., Дракулић Р., *Сајбер криминал*, www.bos.org.yu/cepit/idrustvo/sk/cyberkriminal.pht
30. *Encarta encyclopedia*, http://encyclopedia.msn.com/encyclopedia_761582824/Cyberspace.html
31. Eriksen T., *Tiranija trenutka: brzo i sporo vreme u informacionom društvu*, biblioteka XX vek, Beograd, 2003.
32. *EU Agency analysis of Stuxnet malware: a paradigm shift in threats and Critical Information Infrastructure Protection*, European Network and Information Security Agency, http://www.enisa.europa.eu
33. *Europa simulates total cyber war*, http://www.bbc.co.uk/news/mobile/technology-11696249
34. *European Union Ministerial Conference on Critical Information Infrastructure Protection*, Tallinn, 27-28 April, 2009.
35. *FIRST*, www.first.org
36. *First EU Cyber Security Exercise "Cyber Europe 2010"*, http://www.enisa.europa.eu
37. Fulghum D., *Cyberwar Confusion*, Aviation Week & Space Technology, 19.04.2010, Vol. 172, Issue 15; Database: Computers & Applied Sciences Complete

38. Fulghum D., *Lightening War*, Aviation Week & Space Technology, 22.03.2010, Vol. 172, Issue 12; Database: Computers & Applied Sciences Complete
39. Gates R., *Nuclear Weapons and Deterrence in the 21st Century*, address to the Carnegie Endowment for International Peace: October 28, 2008.
40. *G8 Principles for Protecting Critical Information Infrastructures*, http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf
41. Hale J., *Cyber Attack System Proliferation*, http://www.defense-news.com/story.php?!=4550692
42. Hendershot M., *''CyberCrime 2003 – Terrorists' Activity in Cyberspace''*, http://www.isedj.org/3/44/Jain.v1.txt
43. *Homeland Security Act*, www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf
44. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*; http://www.dhs.gov/xabout/laws/gc_1214597 989952.shtm
45. *Hutchinson encyclopedia*, http://encyclopedia.farlex.com/cyberspace
46. *Information Management an Arma International Publication*, September/October 2009; www.arma.org
47. *Information Operations Condition (INFOCON) System Procedures*, Strategic Command Directive (SD) 527-1, Department of Defense, 27.01.2006.
48. Janczewski L., Colarik A., *Cyber Warfare and Cyber Terrorism*, IGI Global, Hersey (USA), 2008.
49. *Joint Publication 1-02*, DoD Dictionary of Military Terms, Washington, D.C.: Joint Staff, Joint Doctrine Division, J-7, October 17, 2008. www.dtic.mil./doctrine/jel/new_pubs/1_02.pdf
50. Jones S., *Virtual Culture – Identity and Communication in Cybersociety*, SAGE Publications, London, 1997.
51. Karatzogianni A., *The Politics of Cyberconflict*, Routledge, London, 2006.
52. Kizza J., *Guide to Computer Network Security*, Springer, London, 2009.

53. Kollock P., Smith M., *Communities in cyberspace*, Routledge, New York, 2001.

54. Kshetri N., *Pattern of global cyber war and crime: A conceptual framework*, Journal of International Management, The Fox School of Business and Management – Temple University, Greensboro (USA), No. 11, 2005.

55. Кукрика М., *Уīрављање сиīурношћу информација*, ИНФОхоме Пресс, Београд, 2002.

56. Lewis J., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington, 2002.

57. Lewis G., *Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation*, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006.

58. Libicki M., *Cyberdeterrence and Cyberwar*, RAND Project Air Force, RAND Corporation, 2009.

59. Lynn W., *Defending a New Domain*, www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

60. Marcella A., Greenfield R., *CYBER FORENSICS: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes*, CRC Press, New York, 2002.

61. Marks P., *Fighting wars in cyber space*, New Scientist, 14.03.2009, Vol. 201, Issue 2699; Database: Computers & Applied Sciences Complete

62. McMillan R,, *Computer World*, December 7, 2009, Report: China Tied To Cyberattacks on U.S. Systems, p. 12., www.computerworld.com

63. Мимица А., Богдановић М., *Социолошки речник*, Завод за уџбенике, Београд, 2007.

64. Mors M., *''Sajber-predeli, kontrola i transcendencija: estetika virtuelnog''*, Kultura, br. 107-108, Zavod za proučavanje kulturnog razvitka, Beograd, 2004.

65. *National Infrastructure Protection Center*, www.nipc.gov

66. *National Infrastructure Protection Plan*, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

67. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Ministry of Interior, Federal Republic of Germany, Berlin, 17th June, 2009.
68. *National Strategy for Homeland Security*, www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf
69. *NATO 2020: Assured security – dynamic engagement*, Analysis and recommendations of the group of experts on a new strategic concept for NATO, 17 May 2010; www.nato.int/strategic-concept/expertsreport.pdf
70. Nicholas N., *The Black Swon – The Impact of the Highly Improbable*, Random House, New York, 2007.
71. *Origins of the word cyberspace*, http://encyclopedia.thefreedictionary.com/cyberspace
72. *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*, www.oecd.org/dataoecd/1/13/40825404.pdf
73. O'Rourke M., *The Real Enemy*, Risk and Insurance Management Society (RIMS), New York, 2010.
74. Parsons T., *Društva*, August Cesarec, Zagreb, 1998.
75. Patrick A., *Information Operations Planning*, Artech House, Boston-London, 2007.
76. Paul C., *Information Operations – Doctrine and Practice*, Praeger Security International, London, 2008.
77. Петровић С., *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004.
78. Pollitt M., *''Cyberterrorism – fact or fancy?''*, www.cs.georgetown.edu/~denning/infosec/pollitt.html
79. *Rally the troops for war on cyber crime*. Computing, 02.07.2009; Database: Computers & Applied Sciences Complete
80. Речник српскохрватског књижевног језика (књига пета), Матица српска, Нови Сад, 1973.
81. *ROK Daily: China Wants Dominance in Cyber Space*, World News Connection, 21.09. 2007.
82. *Securing Cyberspace for the 44th Presidency*, Center for Strategic and International Studies, Washington, DC December 2008.

83. Shackelford S., *Estonia three years later: A progress report on combating cyber attacks*, Journal of Internet Law, February 2010.

84. Shinder D., *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland (USA), 2002.

85. Solange Ghernaouti-Helie, *Cybersecurity Guide for Developing Countries*, International Telecommunication Unione, Geneva, 2009.

86. *Statement of Dorothy Denning*, www.house.gov/hasc/testimony/106thcongress/ 00-05-23denning.htm

87. Stephenson P., *Investigating Computer-Related Crime: A Handbook for Corporate Investigators*, CRC Press, New York, 2000.

88. *Стратеiи национал но безопасности Росси ско Федерации до 2020 iога*, http://www.scrf.gov.ru/documents/99.html

89. Suter M., *A Generic National Framework for Critical Information Infrastructure Protection*, Center for Security Studies, ETH Zurich, 2007.

90. Stytz M., *Cyberwarfare Distributed Training*, Military Technology (MILTECH), 11/2006.

91. Тасић В., Бауер И., *Речник комiјутерских термина*, Микро књига, Београд, 2003.

92. *TheFreeDictionary*, http://www.thefreedictionary.com/cyberspace

93. *The National Strategy to Secure Cyberspace*, The White House, February 2003, www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

94. *The Simple Economics of Cybercrimes*, IEEE Security & Privacy, january/february 2006, www.computer.org/security

95. Tipton H., Krause M., *Information Security Management Handbook (fifth edition)*, CRC Press, New York, 2004.

96. Томић З., *''Сајбер-iростор и iроблеми разiраничења''*, Култура, бр. 107-108, Завод за проучавање културног развитка, Београд, 2004.

97. Требјешанин Ж., *Речник iсихолоiије*, Стубови културе, Београд, 2004.

98. Винер Н., *Кибернетика или управљање и комуникација код живих бића и машина*, Издавачко-информативни центар студената, Београд, 1972.

99. Винер Н., *Кибернетика и друштво – људска употреба људских бића*, Нолит, Београд, 1973.

100. Вирилио П., *Информатичка бомба*, Светови, Нови Сад, 2000.

101. Zekos G., State cyberspace juristiction and personal cyberspace juristiction, International Journal of Law and Information Technology, Oxford University Press, London, Vol. 15 No. 1, 2007.

102. Wellman B., Gulia M., ''*Virtual communities as communities – Net surfers don't ride alone*'', Kollock P., Smith M., (ed) Communities in cyberspace, Routledge, New York, 2001.

103. Xingan Li, *Cybercrime: An Introduction*, www.studycrime.com/crime/cybercrime.php

104. *2010 Critical Information Infrastructure Protection (CIP) Survey*, www.symantec.com

ЦИП – Каталогизација у публикацији
Народна библиотека Србије, Београд

343.533::004
007:004.056

ВУЛЕТИЋ, Дејан, 1972-
Одбрана од претњи у сајбер простору / Дејан Вулетић. - Београд : Институт за стратегијска истраживања, 2011 (Београд : Институт за стратегијска истраживања). - 88 стр. : илустр. ; 30 цм

Тираж 20. - Напомене и библиографске референце уз текст. - Библиографија: стр. 81-88.

ISBN 978-86-81121-09-2

a) Рачунарска технологија - Злоупотреба
b) Информациона технологија - Безбедност

COBISS.SR-ID 187712780