DOI: 10.5937/vojdelo1505167V

СМЕРНИЦЕ ЗА ИЗРАДУ СТРАТЕГИЈЕ ОБЕЗБЕЂЕЊА САЈБЕР ПРОСТОРА*

Дејан В. Вулетић**
Министарство одбране Републике Србије,
Институт за стратегијска истраживања

Стратегија за обезбеђење сајбер простора, настала као последица изазова модерног информационог друштва, проактивни је документ намењен да заштити организације и грађане од различитих облика угрожавања у сајбер простору. У раду су анализиране стратегије и политике обезбеђења сајбер простора одређених земаља у међународној заједници које су достигле висок степен развоја информационог друштва а изложене су бројним ризицима у сајбер простору. У завршном делу рада изнети су предлози који треба да помогну Републици Србији у изради националне стратегије обезбеђења сајбер простора.

Кључне речи: *сајбер простор, стратегија, сајбер безбедност, информационо-комуникациона технологија*

Увод

Модерно друштво зависно је од информације, као стратегијског ресурса и информационо-комуникационе технологије (ИКТ), којом се врши њен пренос, обрада и размена.

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[1] који обухвата становнике било ког дела света, свих старосних група и друштвених слојева.

Стратегије за обезбеђење сајбер простора[2] дају оквир у организовању и одређивању приоритета, смањивању националне рањивости напада на критичне информационе инфраструктуре и имплементацијом знатно доприносе повећању безбедности у сајбер простору.

* Рад је настао у оквиру научноистраживачког пројекта под називом „Смернице за израду националне стратегије Републике Србије за обезбеђење сајбер простора", а према Плану научноистраживачке делатности у МО (акт Управе за стратегијско планирање пов. бр. 18-80 од 08.03.2012. године).

** Потпуковник доц. др Дејан В. Вулетић; експертска област: Информационо ратовање и сајбер криминал; dejan.vuletic@mod.gov.rs

[1] Сајбер простор (*cyber space*) представља нематеријални, неограничени интерактивни простор креиран од рачунарских мрежа.

[2] Обезбеђење сајбер простора представља процес његове заштите од нежељене употребе или било ког облика угрожавања који може проузроковати штетне последице по податке, програме и процесе у рачунарским мрежама.

Као информационо друштво, Србија се ослања на информационо-комуникационе технологије (електронске комуникације, образовање, здравство, правосуђе, наука, култура, пословни сектор итд.) па је самим тим веома рањива на појаве које утичу на њихово функционисање. Осигурање безбедности друштва је кључни задатак владиних органа, па витални системи друштва морају функционисати у свим ситуацијама.

Циљ овог чланка јесте да се убрза и олакша процес доношења националне стратегије за обезбеђење сајбер простора, као предуслова за ефикасно и безбедно функционисање грађана, државног и приватног сектора.

Стратегија и политика обезбеђења сајбер простора у референтним земљама међународне заједнице

Стратегије обезбеђења сајбер простора почеле су да се појављују почетком двадесетпрвог века, као последица све већег броја различитих претњи по националну безбедност. Прва земља која је сајбер претње окарактерисала као проблем од националног стратегијског значаја јесу Сједињене Америчке Државе, публикујући, 2003. године, Националну стратегију за обезбеђење сајбер простора. Поменута стратегија представљала је део Националне стратегије за унутрашњу безбедност (National Strategy for Homeland Security), настале као одговор на терористичке нападе 11. 9. 2001. године [1].

Сједињене Америчке Државе

У најновијој Међународној стратегији за сајбер простор (*International Strategy for Cyberspace*), из маја 2011. године, наводи се да системи морају функционисати безбедно и поуздано како би се остварила права и потпуна корист од информационо-комуникационих технологија [2]. Грађани морају имати поверење и гаранције да ће њихове подаци и информације путовати поуздано до жељене дестинације без прекида. Обезбеђивање тока информација, безбедности и приватности, као и интегритета умреженог света, значајан је за америчку и светску економију, безбедност и промовисање универзалних вредности.

У поменутој стратегији наводи се да се САД обавезују да ће сачувати и повећати „добре стране" употребе рачунарских мрежа по њихово друштво и економију. Свесни су нових изазова, тј. да ће употреба све већег броја нових рачунарских мрежа довести до нових ризика по националну и економску безбедност и друштво у целини. Изазови се јављају у различитој форми: природне катастрофе, несрећни случајеви, саботаже каблова, сервера и рачунарских мрежа на територији САД и других земаља. Претње у сајбер простору могу угрозити међународни мир и безбедност на ширем подручју уколико се традиционалне форме сукоба прошире у сајбер простор [2].

Њихова међународна политика у сајбер простору у суштини представља обавезу заштите основних принципа: слободе, приватности и протока информација. Сједињене Америчке Државе ће деловати глобално, промовишући отворене, интероперабилне, безбедне и поуздане информационе и комуникационе инфраструктуре које ће олакшати међународну трговину, ојачати глобалну безбедност и подстицати

иновације. Да би то постигле, настојаће да изграде и одржавају окружење у којем ће норме одговорног понашања водити државне поступке, одржива партнерства и поштовање правних норми у сајбер простору [2].

Њихова улога у будућности сајбер простора у погледу промовисања позитивних норми комбиноваће дипломатију, одбрану и развој како би се повећао просперитет, безбедност и отвореност, тако да би сви имали користи од мрежне технологије. Дипломатија подразумева ојачавање партнерства, билатерална и мултилатерална партнерства, кроз међународне организације и сарадњу са приватним сектором [2].

Одбрана значи да ће САД заштитити своје мреже без обзира на то да ли претње долазе од терориста, сајбер криминалаца, држава или њихових помагача. Одбрана се постиже, пре свега, одвраћањем (добром заштитом мрежа, плановима за изоловање и ублажавање напада) и застрашивањем (нужно је обезбедити да ризик везан за напад и експлоатацију рачунарских мрежа увелико премашује евентуалну корист од таквих поступака; обезбеђивањем механизама да се инцидент може истражити а починиоци ухватити и процесуирати).

Развој подразумева отворен, интероперабилан, поздан и безбедан сајбер простор који треба да буде расположивији него што је то данас. Сједињене Америчке Државе имаће активну улогу у обезбеђивању знања и капацитета да се постојећи и нови системи дограде и заштите и да се државе чланице у међународној заједници понашају као одговорни субјекти. Сједињене Америчке Државе ће помагати у изградњи капацитета по том питању, ван својих граница, билатерално и кроз мултилатералне организације, тако да свака држава има капацитете да заштити своје информационе инфраструктуре, ојача глобалне мреже и изгради блискије партнерске односе.

Да би се у потпуности искористили потенцијали сајбер простора за све, Влада САД спроводи своје активности кроз седам узајамно повезаних области активности, при чему свака захтева сарадњу са владом, међународним партнерима и приватним сектором. Посматрани као целина, они представљају акционе линије стратегијског концепта [2]:

• Економија: промовисање међународних стандарда и иновација, отворена тржишта

– одржање окружења слободне трговине која ће подстицати технолошке иновације уз помоћ глобалних, међусобно повезаних мрежа

– заштита интелектуалне својине, укључујући пословне тајне од крађе

– обезбеђење примене безбедних и интероперабилних техничких стандарда, које су одредили технички експерти.

• Заштита рачунарских мрежа: повећање поузданости, безбедности и еластичности

– промовисање сарадње у сајбер простору, посебно норме понашања за државе и по питању сајбер безбедности, билатерално и оквиру мултилатералних организација и мултилатералног партнерства

– смањивање упада и ометања рачунарских мрежа у Сједињеним Америчким Државама

– обезбеђивање управљања инцидентима, еластичност и способност опоравка за информационе инфраструктуре

– побољшање безбедности ланца снабдевања високотехнолошких уређаја, у сарадњи са индустријом

• Криминалистичке службе (правосудни органи): проширивање сарадње и примене закона

– потпуна посвећеност развоју међународне политике по питању сајбер криминала

– хармонизација законодавства на међународном плану, повећањем броја земаља које су потписале Конвенцију Савета Европе о сајбер криминалу

– фокусирање на законе који санкционишу криминал а не забраном приступа интернету

– онемогућавање терориста и криминалаца да користе интернет за оперативно планирање, финансирање или реализацију напада.

• Војска: припрема за безбедносне изазове у 21. веку

– препознавање и прилагођавање све већим потребама војске за поузданим и безбедним мрежама

– изграђивање и ојачавање актуелних војних савезништава у супростављању потенцијалним претњама у сајбер простору

– проширивање сарадње у сајбер простору са савезницима и партнерима ради повећања колективне безбедности

• Управљање интернетом: промовисање ефективне и садржајне структуре

– стављање приоритета на отвореност и иновације интернета

– очување стабилности и безбедности глобалних мрежа

– промовисање и повећање дискусије различитих субјеката по питању управљања интернетом

• Међународни развој: изградња капацитета, безбедности и просперитета

– обезбеђивање неопходних знања, обуке и других ресурса ради подизања техничких и других капацитета по питању безбедности у сајбер простору

– непрекидан развој и размена искустава на међународном плану

– повећавање способности државе да се супротстави сајбер криминалу – укључујући обуку правосудних органа, форензичких специјалиста, судија...

– унапређивање контаката са доносиоцима одлука по питању изградње техничких капацитета, као и са експертима и релевантним субјектима

• Интернет слободе: подршка основним слободама и приватности

– подршка субјектима у цивилном друштву у стварању поузданe и безбедне платформе за слободу удруживања и изражавања

– сарадња са цивилним друштвом и невладиним организацијама у успостављању заштите њихових активности на интернету од незаконитих дигиталних упада

– подстицање сарадње по питању заштите приватности комерцијалних података

– обезбеђивање интероперабилности „с краја на крај" и омогућавање свима приступ интернету.

У завршном делу Стратегије наглашава се да она представља мапу која допушта владиним агенцијама и телима у САД да боље дефинишу и координирају њихову улогу у међународној политици по питању сајбер простора (*International Cyberspace Policy*), да сагледају путеве којима треба да се крећу и, у складу с тим, планирају имплементацију одређених мера. То је уједно позив приватном сектору, цивилном друштву и крајњим корисницима да повећају своје напоре кроз партнерство, свест и активности. Као најважнији елеменат наглашава се позив другим народима и државама да им се придруже у остваривању визије просперитета, безбедности и отворености у умреженом свету.

У Стратегији деловања Министарства одбране у сајбер простору наводи се да су „претње у сајбер простору једне од најозбиљнијих по националну безбедност, грађане и економске изазове са којима се они као нација суочавају." [3]

Поред осталих владиних министарстава и агенција и Министарство одбране зависи од сајбер простора. Министарство одбране САД функционише захваљујући хиљадама рачунарских мрежа, милионима рачунарских уређаја, стотинама постројења у великом броју земаља широм света. Министарство одбране користи сајбер простор како би остварило војне, обавештајне и друге операције, реализовало процес командовања и контроле широког спектра војних операција.

У Стратегији деловања Министарства одбране у сајбер простору наводи се да су Министарство одбране и нација у целини рањиви у сајбер простору, као и да многе стране обавештајне и друге организације покушавају да упадну у њихове рачунарске мреже. Да би се ефикасно супротставили актуелним и будућим ризицима у сајбер простору, наглашава се пет стратегијских иницијатива Министарства одбране [3]:

1. Министарство одбране ће третирати сајбер простор као једно од оперативних области (поред копна, мора, ваздуха и космоса) за који се треба оспособити и опремити, како би се остварило преимућство и искористили потенцијали овог простора. Државни секретар одбране одредио је одговорност за мисије у сајбер простору Стратегијској команди (*United States Strategic Command – USSTRATCOM*), другим борбеним командама и војним структурама. Услед потребе да се обезбеди способност ефикасног деловања у сајбер простору и искористе сопствени ресурси Министарство одбране је формирало Сајбер команду Сједињених Америчких Држава (*U.S. Cyber Command – USCYBERCOM*) као потчињену структуру Стратегијској команди. Стратегијска команда поверила је Сајбер команди одговорност за синхронизовање и координацију сваког вида војске (*U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. 10th Fleet, the 24th Air Force, U.S. Marine Corps Forces Cyber Command u U.S. Coast Guard Cyber Command*). Имајући у виду да је Сајбер команда лоцирана у оквиру Агенције за националну безбедност (*National Security Agency – NSA*), директор Агенције за националну безбедност је, такође, надређени Стратегијској команди (двострука надређеност).

2. Потребно је искористити нови концепт деловања како би се заштитиле рачунарске мреже и системи Министарства одбране. Поред тога, неопходно је искористити практична знања да би се побољшала безбедност у сајбер простору, спречиле и ублажиле унутрашње претње, развили нови концепти одбране и архитектуре система.

3. Партнерство са другим владиним министарствима и агенцијама, као и приватним сектором, омогућиће свеобухватну државну (националну) стратегију сајбер безбедности. Посебно се наглашава сарадња са Министарством за унутрашњу безбедност (*Department of Homeland Security – DHS*). Многе критичне функције и операције Министарства одбране зависе од комерцијалних субјеката као што су нпр. провајдери интернет услуга над којима ово министарство нема директне надлежности како би могло ефикасно да управља ризицима.

4. Изградња чврстих веза са савезницима и међународним партнерима ојачаће колективну сајбер безбедност. Развој међународних способности за упозоравање и обавештавање омогућиће колективну самоодбрану и одвраћање потенцијалних нападача.

5. Уздизање (утицај) националне проницљивости кроз специјализоване сајбер снаге и брзе технолошке иновације. Министарство одбране ангажоваће научне и економске ресурсе како би се дошло до одређеног броја војног и цивилног особља које ће деловати у сајбер простору и помоћи да се реализују циљеви Министарства одбране. Такође, подржаће и иницирати брзе иновације како би се обезбедиле ефикасне сајбер операције. Поред тога, инвестираће у људство, технологију, истраживање и развој како би се створиле и одржавале способности деловања у сајбер простору које су од виталне важности за националну безбедност. Рад у Министарству одбране мора бити конкурентан како би привукао младе кадрове, технички оспособљено људство да уђу у службу на дужи период. Министарство ће се фокусирати на регрутовање и ангажовање таквог људства у раном периоду у складу са председничком иницијативом (*2010 Presidential Initiative*), као и на изградњи механизама размене талената између приватног и државног сектора без казнених последица по таква лица. Дефинисаће се и процес занављања ИТ ресурса и скратити период употребе. То подразумева циклус промена од 1 до 3 године, а не 7 до 8 као што је раније био случај.

Кина

Народноослободилачка армија Кине активно развија способности за операције у рачунарским мрежама (*Computer Network Operations – CNO*) и израду стратегијских водича, алата и оспособљеног људства неопходног да се ангажује као подршка традиционалном начину ратовања [4].

У кинеској Стратегији операција у рачунарским мрежама (*Chinese Computer Network Operations Strategy*) наводи се да се применом операција у рачунарским мрежама, у фази отпочињања конфликта, могу деградирати информациони системи противника, што је знатно ефикасније од класичних напада, нарочито ако је противник технолошки напреднија сила, као што су Сједињене Америчке Државе [4].

У НР Кини је усвојена званична стратегија информационог ратовања (*Integrated Network Electronic Warfare – INEW*) којом се учвршћују принципи информационог ратовања, под 4th Department Генералштаба Народне ослободилачке војске Кине [5].

Интегрисано мрежно-електронско ратовање (*Integrated Network Electronic Warfare*) представља комбиновану примену операција у рачунарским мрежама и електронског ратовања ради координираног или једновременог напада на непријатељске рачунарске системе.

Кинеска званична политика промовише безбедност кроз одбрамбене активности, настоји да промовише мир кроз сарадњу и обезбеђује слободу говора и приступа интернету.

Русија

У Руској Федерацији у употреби су термини информациона безбедност и информациони простор (шире значење), насупрот америчком сајбер безбедност и сајбер простор, који су примарно технолошки. Под информационом безбедношћу подразумевају „заштиту националних интереса у информационој сфери".

У Доктрини информационе безбедности Руске Федерације разрађени су различити проблеми – од заштите података, заштите приватности до неовлашћеног приступа државним тајнама. Доктрина је усвојена 2000. године и у њој се, поред осталог, наводи [6]:

– ситуација по питању безбедности података, који представљају државну тајну, погоршава се;

– заостајање у развоју ИКТ доводи до тога да је влада присиљена да купује страну опрему, што је негативно са аспекта безбедности и повећава вероватноћу неовлашћеног приступа;

– зависност Русије од страних произвођача рачунарске и телекомуникационе опреме је у порасту;

– претња употребе информационог оружја против Русије је повећана;

– не постоји довољна координација, као ни финансијска средства за национални одговор на наведене претње, ако се тако нешто буде захтевало;

– не посвећује се довољно пажње развоју система за извиђање и електронско ратовање.

Председник Медведев је 2009. године потписао нову Стратегију националне безбедности Руске Федерације до 2020. године. У Стратегији се наводи да ће вероватан негативан утицај, поред осталог, представљати различите незаконите активности у области кибернетике и високих технологија. Такође, истиче се да претња војној безбедности може бити остварена применом информатичке и других средстава информационе технологије [7].

Немачка

Напади на информационе инфраструктуре су, последњих година, постали све чешћи и комплекснији, а починиоци све професионалнији. Сајбер напади су извршавани са територије Немачке, као и ван ње. Са технолошког становишта, малициозни програми су све софистицираниј, те је теже супротставити им се и пратити их. Све је теже открити идентитет и позадину напада. Криминалци, терористи и шпијуни користе сајбер простор за своје активности и не стају на државним границама [8].

Сајбер безбедност заснива се на свеобухватном приступу, што подразумева бољу координацију и размену информација. Базира се, пре свега, на мерама и приступима који се односе на цивилни сектор. Оне су комплементарне са мерама које предузима *Bundeswehr* (Оружане снаге Савезне Републике Немачке) у заштити својих ресурса [8].

У Стратегији сајбер безбедности Немачке наводе се следећи циљеви и мере [8]:

– заштита критичних информационих инфраструктура;

– обезбеђивање ИТ система у Немачкој;

– подизање нивоа безбедности ИТ система у државној администрацији;

– формирање Националног центра за сајбер одговор (*National Cyber Response Centre*);

– формирање Националног савета за сајбер безбедност (*National Cyber Security Council*);

– ефикасна контрола криминала и у сајбер простору;

– ефикасне координиране акције чији је циљ обезбеђење безбедности сајбер простора у Европи и свету;

– употреба поуздане и сигурне информационе технологије;

– оспособљавање људства у федералним органима;

– алати за одговор на сајбер напад.

У Националној стратегији за заштиту критичних инфраструктура Савезне Републике Немачке наводи се да критичне инфраструктуре чине организационе и физичке структуре и средства од виталне важности за друштво и економију, тако да њихово прекидање и деградирање може довести до прекида напајања, значајног ремећења безбедности друштва или других драматичних последица [9].

Критичне инфраструктуре могу бити изложене спектру претњи које се могу, условно, сврстати у следеће групе [9]:

– елементарне непогоде (екстремни временски услови, пожари, потреси, епидемије, пандемије, космички догађаји итд.);

– технички пропусти/људске грешке (системски пропусти, немар, организациони пропусти и друго);

– тероризам, криминал, рат.

Да би заједничка акција била успешна неопходне су стратегијске смернице за заштиту критичних инфраструктура, а које се тичу свих релевантних ризика. На основу смерница могуће је утврдити потциљеве, који ће бити специфицирани и имплементирани кроз програме и планове. У ИТ сегменту такав документ већ постоји у облику Националног плана за заштиту информационих инфраструктура (*National Plan for Information Infrastructure Protection – NPSI*). 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*) [9].

У Стратегији се захтева заједничко ангажовање и имплементација Стратегије на федералном и локалном нивоу, у складу са областима одговорности. Сет инструмената за имплементацију Стратегије подразумева [9]:

– програме и планове (нпр. *Network Control Program*);

– одређене препоруке за деловање (нпр. *National Baseline Protection Concept* као основни водич за физичку заштиту критичних инфраструктура);

– стандарде, норме и регулативе (нпр. *BSI Information Security Standards*).

Услед повећања комплексности и рањивости информационих инфраструктура, ситуација по питању сајбер безбедности биће од критичне важности у будућности. У Немачкој приватни и државни сектор, као и друштво у целини, могу бити циљани и угрожени таквим нападима.

Француска

Француска влада знатно подиже способности по питању сајбер одбране. Томе је, у великој мери, допринело формирање Агенције за мрежну и информациону безбедност (*French Network and Information Security Agency – ANSSI*) 2009. године, као први корак у том процесу [10].

У Стратегији Француске – одбрана и безбедност информационих система, као могућа претња на националну инфраструктуру предвиђа се и широкораширени (*large-scale*) сајбер напад. Наведена стратегија заснива се на четири циља [11]:

– постати светска сила у сајбер одбрани;

– осигурати способност Француске за доношење одлука о заштити информација које се тичу њеног суверенитета;

– побољшати безбедност критичних (информационих) инфраструктура;

– осигурати безбедност у сајбер простору.

Да би се то постигло, препознаје се седам подручја деловања [11]:

– праћење развоја технологија, предузимање активности и анализа;

– детекција, упозоравање и одговор;

– јачање и стално оснаживање научне, техничке, индустријске и људске способности;

– заштита информационих система државних органа и критичних инфраструктура;

– прилагођавање француског законодавства;

– развој међународне сарадње;

– комуникација, размена информација и саопштења, подизање свести и мотивације појединаца и организација.

Велика Британија

У Стратегији сајбер безбедности Велике Британије наводи се да расте број непријатеља у сајбер простору који покушавају да украду, компромитују или униште критичне податке. Све већи степен зависности значи да просперитет, функционисање критичних инфраструктура, радна места и места становања могу бити угрожени. Управо зато, Национална стратегија безбедности (*National Security Strategy*) идентификује сајбер нападе као *Tier 1* претње, односно као једну од претњи највишег нивоа. Као потенцијални починиоци идентификовани су криминалци, државе, терористи итд. Сајбер простор својим растом постаје подручје где стратегијска предност, индустријска или војна, може бити добијена или изгубљена. Растућа употреба и зависност од сајбер простора значи да његово прекидање може утицати на способност државе да ефикасно функционише у случају кризе [12].

Одређене државе користе сајбер простор за непријатељске активности, при чему негирају да то чине. Поред одбрамбених и заштитних способности, Велика Британија мора бити способна да одбрани властите интересе у сајбер простору. Растућа употреба интернета и употреба нових дигитално повезаних технологија чини сајбер простор комплексним и стално промењивим окружењем, што доноси нове изазове [12].

Њихова визија је да ће Велика Британија 2015. године постићи велики економски просперитет, висок ниво националне безбедности и снажно друштво.

У Стратегији сајбер безбедности Велике Британије наглашавају се њени следећи циљеви [12]:

– мора да се супротстави сајбер криминалу и постане једно од најсигурнијих места на свету за пословање у сајбер простору;

– мора бити отпорнија на сајбер нападе и имати веће способности да заштити сопствене интересе у сајбер простору;

– треба да помогне развоју отвореног и стабилног сајбер простора који грађани могу безбедно користити и који подстиче отвореност друштва:

– треба да поседује темељна и разнородна знања, вештине и способности како би се помогло остваривању циљева сајбер безбедности.

Као основни принципи наводе се [12]:

– приступ базиран на процени ризика (*a risk-based approach*);

– рад са партнерима;

– балансирање безбедности са једне, и слободе и приватности са друге стране.

Улоге и одговорности у том процесу имају [12]:

– појединци;

– приватни сектор;

– влада.

Прегледом стратегијске одбране и безбедности (*Strategic Defence and Security Defence and Security Review*) из 2010. године, влада је наменила 650 милиона фунти за Програм националне сајбер безбедности (*National Cyber Security Programme – NCSP*) [13]. Тај новац намењен је да трансформише одговор Владе по питању сајбер претњи и распоређен је министарствима и агенцијама који имају улогу у том процесу.

Обавештајне агенције и Министарство одбране имају главну улогу у смањивању рањивости и претњи у сајбер простору Велике Британије. Владин штаб за комуникације (*Government Communications Headquarter*s – *GCHQ*) одређен је као централна тачка у тим напорима. Међутим, Министарство унутрашњих послова (*Home Office*), Кабинет (*Cabinet Office*) и Институција за британске стандарде (*British Standards Institution – BIS*) такође добијају одређена средства да побољшају своје капацитете у том сегменту [12].

Програм националне сајбер безбедности предвиђа и едукацију експерата из домена сајбер безбедности, мултидисциплинарна истраживања и друго. Поред осталог, Програмом се предвиђа, уз помоћ владиног штаба за комуникације, оснивање истраживачког института из сајбер безбедности, са оквирним буџетом од 2 милиона фунти за 3,5 године [12].

Препоруке за израду стратегије обезбеђења сајбер простора у Републици Србији

Све већом применом информационо-комуникационих технологија, Република Србија биће рањивија и осетљивија на евентуалне нападе. Организације и појединци у Републици Србији биће изложенији бројнијим и софистицираним претњама у сајбер простору, који могу потицати из различитих извора.

Правна регулатива, закони, упутства и други документи из области телекомуникација морају бити усклађени са стратегијом за обезбеђење сајбер простора. Приликом израде стратегије за обезбеђење сајбер простора треба да буду узете у обзир и одлуке, декларације и опредељења међународних институција чији је Република Србија члан или је на путу да то постане. У том смислу, треба имати у виду следећа документа:

– директиве, одлуке и препоруке Европске уније;
– одлуке и препоруке Међународне телекомуникационе уније (ИТУ);
– Стратегију развоја информационог друштва у Републици Србији до 2020. године („Службени гласник РС”, број 51/10);
– Стратегију националне безбедности Републике Србије („Службени гласник РС”, број 88/09);
– Стратегију научног и технолошког развоја Републике Србије у периоду од 2010. до 2015. године („Службени гласник РС”, број 13/10);
– Закон о заштити података о личности („Службени гласник РС”, бр. 97/08 и 104/09);
– Закон о потврђивању Конвенције о високотехнолошком криминалу и Закон о потврђивању додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршене употребом рачунарских система („Службени гласник Републике Србије”, број 19/09);
– Закон о Војнобезбедносној и Војнообавештајној агенцији;
– Закон о тајности података („Службени гласник”, број 104/09);
– Закон о телекомуникацијама („Службени гласник”, број 44/03, 36/06 и 50/09);
– Закон о одбрани („Службени гласник РС”, 116/07, 88/09, 104/09).

Стратегијом се мора захтевати заштита система ради очувања тајности, интегритета и расположивост осетљивих информација. Заштиту рачунарских система треба стандардизовати и регулисати на тај начин да она постане обавеза свих ималаца рачунарских система. Нарочита пажња треба да буде посвећена имаоцима критичних информационих инфраструктура. Препоручљиво је да се стратегијом наглашавају периодичне, годишње или чешће анализе стања по питању заштите ималаца критичних информационих инфраструктура.

Стратегију треба развијати у више фаза (анализа, формулисање и имплементација стратегија, контрола). Стратегијском анализом идентификују се садашње и будуће шансе и претње које могу утицати на способност достизања постављених циљева. Формулисање стратегије обухвата утврђивање различитих путева (начина), односно различитих стратегијских опција за реализовање мисије и циљева. Имплементација стратегије је фаза која обухвата употребу менаџерских и организационих алата како би се усмерили ресурси према постизању стратегијских циљева. Контрола подразумева активности надгледања, оцене, мерења и побољшања различитих активности с циљем да се идентификују учинци и предузму корекције, уколико је потребно.

Пре израде стратегије неопходно је извршити анализу стања и процену ризика којима је Република Србија изложена. Потребно је наглашавати непрестане промене у сајбер простору, што ће имати за последицу да се Стратегија посматра као „живи” документ и да има одређени временски оквир, тј. да буде флексибилна и динамичка. Потребно је наглашавати важност подизања свести грађана о ризицима и претњама у сајбер простору.

Неопходно је стално наглашавати и подстицати сарадњу и дељење ресурса између државног и приватног сектора кроз различите облике: форуме, размене информација, заједничке конференције, семинаре и слично. Поред тога, међународна сарадња и размена информација са одговарајућим субјектима ван државних граница допринеће бољем разумевању и одговору на стално промењиве претње.

Потребно је утврдити критеријуме за избор људства, нарочито за администраторе рачунарских система (нпр. потпуна безбедносна провера која подразумева безбедносне провере у евиденцијама службе безбедности, правосудних и органа унутрашњих послова, разговор са лицем итд.). Неопходно је дефинисати потребе за новим профилима специјалиста и програма обуке који ће подићи ниво оспособљености, како ИТ професионалаца, тако и корисника. Обука треба да буде свеобухватна, да обезбеди знање и вештине о најновијим програмским алатима и платформама, праксу и тимски рад.

Стратегијом је неопходно идентификовати критичне информационе инфраструктуре у Србији, укључујући материјалне ресурсе, услуге, као и међусобне зависности. Нужно је и посебно наглашавати да заштита тих инфраструктура представља питање од националног значаја.

Нужно је дефинисати ко је надлежан, а ко сарађује у изради и имплементацији стратегије (међусекторско тело, Министарство трговине, туризма и телекомуникација или неко трећи). То тело, орган или радна група има улогу координатора и потпуну одговорност за животни циклус и документовање стратегије. Структура, одговорности, међусобне релације и друго морају бити прецизно дефинисани. У стратегији је нужно навести дефиницију сајбер безбедности и других термина који ће се користити у њој.

Стратегијом је нужно направити равнотежу између безбедности и приватности, што у одређеним случајевима може представљати проблем. У актуелној пракси јављају се проблеми када се одређене мере тајног прикупљања података спроводе, од стране обавештајних и служби безбедности у складу са законским овлашћењима, без одлуке суда, што узрокује кршење људских права и слобода који су зајамчени Уставом Републике Србије.

Стратегијом треба идентификовати општа начела за примену националне стратегије и унети у њен текст (нпр. одговорност). Тим начелима треба се руководити приликом утврђивања стратегијских циљева и дефинисања конкретних мера. За сваки стратегијски циљ треба утврдити низ мера које морају бити тако дефинисане да дају ефикасне резултате. На основу индикатора (објективни, мерљиви, релевантни и прецизни показатељи) нужно је пратити примену мера и остварене резултате.

Стратегијом треба наглашавати неопходност формирања националног тима за одговор на компјутерски инцидент[3], са циљем да превентивно делује и координира решавање безбедносних инцидената у сајбер простору. Поред тога, треба указивати и на значај формирања компјутерских тимова за одговор на компјутерски инцидент и код других ималаца информационих инфраструктура. Неопходно је да се захтева успостављање и примена јединственог начина извештавања о инцидентима у сајбер простору.

Стратегијом треба потенцирати важност подизања капацитета правосудних органа кроз доношење нових или промену актуелних закона, оспособљавање лица

[3] Компјутерски тим за одговор на компјутерски инцидент (*Computer Emergency Response Team – CERT*) јесте тим за спречавање, подршку и одговоре на компјутерске нападе на рачунарске системе. Главна улога CERT-а је координација и дељење информација са заинтересованим странама и циљним групама у државном и приватном сектору, као и са међународним партнерима. Национални CERT доноси упутства, смернице, препоруке, савете и мишљења у случају инцидената у сајбер простору који су од значаја за информациону безбедност земље.

које учествују у процесуирању починилаца и друго. Стратегијом је неопходно регулисати доношење акционих планова који ће обухватати практичне, додатно разрађене мере које ће бити задате различитим службама и појединцима. Акциони план ствара услове за материјализацију визија, предлога и смерница и постизања жељеног стања у Србији по питању сајбер безбедности.

Стратегијом треба развијати или унапређивати припремљеност, одговор и опоравак рачунарских система, односно повратак у претходно стање[4] (нпр. заједничким вежбама, удруживањем расположивих капацитета).

Поред наведеног, стратегија треба да:

– буде фокусирана на кључне проблеме и понуди решења за те проблеме;

– обезбеди добру сарадњу између државног и приватног сектора и онемогући преклапање надлежности;

– подстиче одговорност, подизање техничких капацитета и оспособљеност људства, истраживања и развој;

– подстиче процену ризика и разраду могућих сценарија угрожавања;

– дефинише институционални оквир, тј. да именује тело које треба да буде носилац у изради и осталим фазама;

– буде актуелна и да обухвати период од наредних 5 до10 година.

У наредном периоду неминовно се намећу следећи приоритети:

– заштита критичних информационих инфраструктура;

– борба против високотехнолошког криминала;

– унапређење правног и институционалног оквира;

– научноистраживачки рад итд.

Закључак

Развој националне стратегије обезбеђења сајбер простора је велики изазов који захтева координацију између различитих националних субјеката, у државном и приватном сектору.

Стратегија за обезбеђење сајбер простора везана је за националну стратегију безбедности. Представља институционални оквир који мора бити стално процењиван и ажуриран.

Стратегија неће само побољшати безбедност и отпорност националних инфраструктура и сервиса у сајбер простору већ и поверење и подизање свести грађана.

Смерницама за израду стратегије за обезбеђење сајбер простора дефинишу се опредељења и утврђују правци заштите информационих инфраструктура у Републици Србији.

У чланку су изнети предлози који треба да помогну Републици Србији у изради националне стратегије обезбеђења сајбер простора, али и да се корисницима ИКТ пруже смернице и обезбеде услови за заштиту сајбер простора, као предуслова за ефикасно и безбедно функционисање грађана, државног и приватног сектора.

[4] Опоравак је способност одржавања основних услуга током напада, ограничавање штете и поновно успостављање свих услуга након напада.

Литература

[1] *National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace*, European Network and Information Security Agency, 2012.

[2] *INTERNATIONAL STRATEGY FOR CYBERSPACE - Prosperity, Security and Openness in a Networked World*, May 2011.
http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[3] Department of Defense Strategy for Operating in Cyberspace, July 2011.;
http://www.defense.gov/news/d20110714cyber.pdf

[4] Krekel B., *US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, McLean, VA: RAND Corporation, 2009.p. 68-74.

[5] Sharma D., *Integrated Network Electronic Warfare: China's New Concept of Information Warfare*, Journal of Defence Studies, Institute for Defence Studies and Analyses, New Delhi, Vol 4. No 2. April 2010, p. 38-39.

[6] Brunner E., Suter M., *"Russia—Critical Sectors,"* in An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, ed. Andreas Wenger, Victor Mauer, and Myriam Dunn, Center for Security Studies, Zurich, 2008, p. 342.

[7] С Т Р А Т Е Г И Я национальной безопасности Российской Федерации до 2020 года, http://www.scrf.gov.ru/documents/99.html

[8] *Cyber Security Strategy for Germany*, Federal Ministry of the Interior, February 2011; www.bmi.bund.de

[9] *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Ministry of Interior, Federal Republic of Germany, Berlin, 17th June, 2009.

[10] *French Network and Information Security Agency,* www.ssi.gouv.fr/en/

[11] *Information systems defence and security – Frances's strategy*, The French Network and Information Security Agency, February 2011.

[12] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, Cabinet Office, London, November 2011.

[13] *Strategic Defence and Security Review*, www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-defence-security-review.pdf