DOI: 10.5937/vojdelo1802100J

ИНФОРМАЦИОНА БЕЗБЕДНОСТ РУСКЕ ФЕДЕРАЦИЈЕ

Катарина Јонев
Универзитет у Београду, Факултет безбедности
Хатиџа Бериша
Универзитет одбране у Београду, Војна академија
Александар Ћираковић
Војска Србије, РВ и ПВО

Концепт сајбер безбедности је евалуирао из некада строго техничке дисциплине у стратешки, политички, војни и национални изазов. Са напретком информационо-комуникационих технологија владе држава све више улажу у безбедност својих мрежа, техничку обученост и инсистирају на међународној сарадњи када су у питању сајбер инциденти. Информациона безбедност у Руској Федерацији регулисана је различитим стратегијско-доктринарним документима и представља један од најбитнијих сегмената националне безбедности.

Кључне речи: *информациона безбедност, Руска Федерација, информационо ратовање, доктрина, сајбер простор*

Увод

Информације и комуникације увек су имале стратегијски значај. Међутим, данас су оне са помоћних позиција доспеле у први план. Проблем информационе безбедности постао је основни проблем. Информациона револуција је промена у процесу прикупљања података, у њиховој трансформацији у информације као и у даљој дистрибуцији тих информација. До информационе револуције довела је примена информационих технологија. Информационе технологије не познају државне границе и омогућавају повезивање целог света – држава, организација и појединаца. Међутим, уз све бенефите које нам је донео, сајбер простор носи и низ опасности које могу да угрозе грађане, друштво, али и државе.

Нова друштвено-економска формација друштва повлачи собом и нове опасности. Нове претње изискују нове приступе. У последње две деценије технологије су се развиле и постале интегрални део свакодневног живота. Трансформација је донела дигитализацију друштва, економске бенефите, док се администрација државе, као и основних услуга, ослања све више на ИКТ инфраструктуре, системе и податке. Сајбер простор друштву и грађанима мора да обезбеди сигурност. У случају нарушавања интегритета услед злонамерних намера и актера попут хакера, криминалаца, терориста, непријатељских држава или појединаца који на било који начин могу да изазову осцилације у функционисању система, нарушиће се сигурност, као и незадовољство друштва.

Заштита сајбер простора део је концепта сајбер безбедности и односи се у најширем смислу на заштиту система, инфраструктуре, података, али и услуга. У домену информационе сфере, с једне стране, потребно је обезбедити друштво информационим ресурсима а, са друге стране, формирати систем заштите информационих потенцијала. У случају потенцијалног сајбер ратовања потребно је обезбедити и заштиту државе и њеног сајбер простора.

Савремени информациони системи донели су многе погодности када је у питању пословање, затим аутоматизацији процеса у оквиру индустрије, саобраћаја и других видова класичне и критичне инфраструктуре. Интернет и ИКТ технологије постале су витални део националне инфраструктуре и кључни покретачи друштвено-економског раста, као и развоја држава.[1] Од тренутка настанка, националне владе и компаније прихватиле су Интернет као потенцијал за генерисање прихода. У неким земљама Интернет доприноси до 8% бруто домаћег производа (БДП).[2]

Међутим, поред свих предности које собом носи технолошки напредак, постоје и многе опасности у виду сајбер ризика и претњи. Интернет, заједно са информационом и комуникационом технологијом која га подупире, критичан је национални ресурс за државе. Сајбер простор представља нове могућности и нове изазове за државе подједнако на унутрашњем и спољнополитичком плану, укључујући и националну одбрану. Глобално разумевање треба да обухвати политичке, економске, правне, друштвене и технолошке аспекте који ће омогућити развој оперативних мера заштите свих учесника глобалне заједнице – држава, међународних организација, појединца, приватног и јавног сектора.

Важност сајбер стратегије за безбедност државе

Сајбер простор уједно представља и најсавременије питање које се тиче међународног права, међународних односа, а сајбер безбедност је камен темељац информационог друштва.

Претње у сајбер простору представљају све већу опасност по државу, друштво и грађане због сталног усавршавања технике, али и релативно једноставног извршења одређених дела. Вероватноћа да рачунарски систем постане мета различитих профила нападача се повећава, а највише напада дешава се на системе националне критичне инфраструктуре у које спадају, поред осталих, војни системи, енергетски сектор, водовод, телекомуникациони системи и транспорт. Велики системи поседују велике рачунарске мреже, а самим тим нуде и више могућности за напад. Комплексан систем има и већи степен рањивости. Осетљивост модерног друштва огледа се у великом број информационих структура. Појединци, организације и владе држава наоружани су алатима који могу компромитовати информационе системе. Стога је заштита информационих система постало питање од приоритетног значаја за државу.

[1] Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012, NATO Cooperative Cyber Defence Centre of Excellence str. 18

[2] David Dean et al., 'The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy,' BCG. Perspectives, 27 January 2012.

Дефинисање питања политике националне безбедности и одбране једне државе условљено је геополитичком стварношћу. Да би се остварила квалитетна анализа геополитичке позиције једне земље неопходно је приступити сагледавању стварности из више углова, као и синтези различитих дисциплина. Геополитика не обухвата нужно само војне или одбрамбене стратегије већ и историјске и политичке чињенице, економски, културолошки, социолошки аспект, становништво и географију. Међутим, са почетком 21. века геополитика се све више ослања управо на националну безбедност и одбрану. Може се рећи да је то узрочно-последични однос који се не може игнорисати. Јасно дефинисан систем националне безбедности једне државе представља управо један од суштинских елемената геополитичког позиционирања те земље, као што национална безбедност геополитички карактерише сваку државу на овом свету.

Чињеница је да државе имају све већу потребу да сајбер безбедност дефинишу на националном нивоу. Интернет, заједно са информационо-комуникационом технологијом (ИКТ) која га подупире, представља критични национални ресурс за државе. То је виталнн део националне инфраструктуре и кључни је покретач друштвено-економског раста и развоја. Државе су све забринутије за свој сајбер простор, па није чудно што су економски и војно-политички највеће државе света донеле неки вид сајбер стратегије у којима се дефинише како да се њихови национални и економски интереси заштите. Сајбер безбедност треба схватити као способност државе да се одупре или ублажи ефекте сајбер напада против својих интереса у сајбер простору. Држава за то треба да поседује одговарајућа средства, уз подршку правних, стратешких и организационих оквира.[3]

Политиком државе дефинишу се обавезе њених државних органа, институција и система кроз државне доктрине и нормативно-правну регулативу.[4]

Руска Федерација – сајбер сила

Сједињене Државе су и даље највећа сајбер суперсила. Међутим, последњих година бележи се раст „сајбер сила" које се појављују као потенцијални ривали Сједињеним Државама.[5] Бивши председник Барак Обама идентификовао је и два највећа супарника у сајбер простору – Народну Републику Кину и Руску Федерацију, назвавши их „агресивним" играчима у свету сајбер шпијунаже и упозорио да ће ове две државе наставити да на нелегалан начин краду индустријске и технолошке тајне Сједињених Америчких Држава.[6] У различитим извештајима Конгреса истиче се да је Русија веома способан сајбер актер, уз допуну да ће се њен „сајбер капацитет применити и за шпијунажу и за сајбер нападе".[7]

[3] Robert S. Dewar The "Triptych of Cyber Security": A Classification of Active Cyber Defence, 2014 6th International Conference on Cyber Conflict, 2014, NATO CCD COE Publications, Tallinn, str 10.

[4] Ковач, М., Стојковић, Б., Стратегијско планирање одбране, Војноиздавачки завод, Београд, 2009, стр.190.

[5] http://www.telegraph.co.uk/news/uknews/defence/8369520/Military-Balance-report-countries-creating-new-cyber-warfare-organisations.html, pristup internetu, 23.06.2017.

[6] http://m.guardian.co.uk/technology/2013/feb/21/white-house-cyber-threat-russia-china pristup internetu, 23.06.2017.

[7] „Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure," Committee on Homeland Security, 113th Congress (March 2013), http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg825-83/html/CHRG-113hhrg82583.htm. pristup internetu , 24.06.2017.

На међународном нивоу Руска Федерација представља значајног актера када је реч о сајбер простору. Она спада у групу држава које имају најбоље хакере на свету. Била је главни осумњичени у најпознатијем међународном сајбер нападу до данас – дигиталном нападу на Естонију 2007. године, а било је и наводних доказа о директној умешаности Кремља у сајбер операције током војне интервенције на Грузију 2008. године и у Украјини од 2014. године. Током избора за председника Сједињених Америчких Држава шпекулисало се о умешаности руских хакера у сам ток избора, као и да су својим дејствима у сајбер простору омогућили победу кандидата Доналда Трампа.

Став Руске Федерације по питању безбедности у сајбер простору умногоме се разликује од америчког, односно западног. Русија је забринута за принцип који охрабрује неконтролисану размену информација и ограниченост националних граница у сајбер простору. Проток информација које могу представљати опасност по руско друштво и државу кључни су проблем са којим се највећа држава света суочава. Русија се залаже за „национални суверенитет у сајбер простору" и најгласнији је заговорник за стварање глобалног одговора на сајбер претње.

Другу тачку размимоилажења са земљама Европе и Северне Америке представља руска перцепција шта се све може дефинисати под појмом „претња"[8] у сајбер простору. За Руску Федерацију „претња представља употребу садржаја за ширење утицаја на области из социјално-хуманитарне сфере".[9] Русија снажно подржава идеју „Интернет суверенитета", односно националне контроле свих Интернет ресурса које леже унутар физичких граница државе. Такође, подржава концепт примене домаћег законодавства – „свака земља чланица има право да постави суверене норме у складу са својим националним законима".[10] Западне државе не слажу се са руским ставом државне контроле или супервизије Интернета.

На унутрашњем плану Руска Федерација је кроз основна стратегијско-нормативна докумената у области одбране – Стратегију националне безбедности и Војну доктрину регулисала сопствени сајбер простор, као и информациону безбедност.

Информациона безбедност Руске Федерације у 21. веку

Разматрање појма информациона безбедност у Руској Федерацији је новијег датума, а приступање овој области започето је деведесетих година прошлог века.

Руска влада је 1997. године ажурирала свој Кривични законик и уврстила борбу против сајбер криминала (ИТ криминала) као један од приоритета. Казне су установљене, поред осталог, за илегални приступ информацијама на рачунару, рачунарским системима и мрежама, као и за стварање, ширење и коришћење штетног софтвера и малвера, рачунарских система и мрежа, крађу интелектуалне својине, производњу и дистрибуцију дечје порнографије.[11]

[8] K. Giles, „Information Troops: A Russian Cyber Command?," in *Third International Conference on Cyber Confl ict*, CCDCOE, 2011, str. 5.

[9] Keir Giles, Russia's Public Stance on Cyberspace Issues, 2012 4th International Conference on Cyber Confl ict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 © NATO CCD COE Publications, Tallinn, str. 64

[10] Ибид, стр 67.

[11] http://www.russian-criminal-code.com/pristup intrentu, 26.06.2017.

Руску Федерацију одликује изузетно уређена област стратегијско-доктринарних докумената у области безбедности. Највиши стратегијски документ у сфери безбедности представља Стратегија националне безбедности, коју је потписао тадашњи председник Руске Федерације Димитрије Медведев, а ступила је на снагу 12. маја 2009. године.[12] Овај документ представља континуирани и логички наставак претходног стратешког документа – Концепције националне безбедности Русије из 2000. године. Међутим, нови документ опширније и детаљније говори о националним интересима, као и о областима које спадају у политику националне безбедности.

Стратегија националне безбедности до 2020. године, уз Концепције дугорочног социјално-економског развоја[13] коју је донео председник Русије 2008. године налазе се на самом врху хијерархије стратегијских докумената. Безбедност зависи не само од ефективног и функционалног система безбедности него и од „економског потенцијала земље".[14]

У остваривању националне безбедности у економској области као стратегијски циљ одређује се средњорочни задатак да Русија по обиму бруто унутрашњег производа постане једна од пет првих земаља у свету.

Највећи део Стратегије националне безбедности Русије, на један темељан начин дефинише националне интересе, односно изграђује систем националне безбедности. То је документ који представља смернице и политике државе из области одбране, економије, социјалне политике, спољне политике за период у наредних 10 година. Основни концепт јесте да се национална безбедност земље осигурава, превасходно на развоју економије и социјалне сфере.

Аутори Стратегије националне безбедности до 2020. године – чланови Савета безбедности и Научни савет Савета безбедности у писању стратегије водили су се чињеницом да је неопходно обезбедити политичку стабилност у друштву, развити националну економију, побољшати квалитет и услове живота грађана, ојачати националну одбрану, државну безбедност, као и правни поредак и вратити међународни углед Руској Федерацији.

Стратегија је и полазна тачка из које су се развиле потоње стратегије ужих области, докумената, закони, доктрине. Национална безбедност одређује се као „област заштите личности, друштва и државе од унутрашњег и спољашњег угрожавања, обезбеђењем заштите устава, слободе, квалитета живота грађана, суверенитета и територијалног интегритета, као и одрживом одбраном и безбедношћу државе и одрживим развојем Руске Федерације".[15] Уз то, дефинишу се и појмови као што су: наци-

[12] Припрема стратегије трајала је пет година.

[13] Концепция долгосрочного социально-экономического развития Российской Федерации до 2020 г. http://www.intelros.ru/subject/ross_rasput/2026-koncepcija-dolgosrochnogo-socialno.html intrentu, 26.06.2017

[14] Стратегија националне безбеднности РФ до 2020 поглавље IV (*Обеспечение национальной безопасности*), тачка 25.

[15] Стратегија националне безбеднности РФ до 2020. (Стратегия национальной безопасности Российской Федерации до 2020 года). Документ је утврђен указом председника Медведева, 12. маја 2009. године. Претходна Концепција је стављена ван снаге. Документ видети на официјелном сајту Савета безбедности РФ: http://www.scrf.gov.ru/documents/99.html, pristup interentu, 27.06.2017.

онални интереси, претња националној безбедности, стратегијски национални приоритети, снаге и средства којима се остварује национална безбедност, итд.[16]

Савет националне безбедности има улогу да обједини, даје инструкције и координира секторима спољне политике и безбедности. При Савету је формиран и Научни савет који чини преко 150 академика, професора, чланова академија наука, декани факултета и руководиоци научних института. У надлежности Савета националне безбедности је и задатак усвајања стратегија, концепција и доктрина.

На сајту Савета безбедности[17] проблеми безбедности сврстани су у неколико области и делатности у којима се прати развој Стратегије кроз израду других стратегија, концептуалних и доктринарних докумената и политика за њихово спровођење. То су:

1. војна и одбрамбено-индустријска безбедност,
2. међународна безбедност,
3. економска безбедност,
4. државна и јавна безбедност,
5. анти терористичка активност и
6. информациона безбедност.

У сфери одбране валидан стратегијско-доктринарни документ је Војна доктрина коју је донео председник Руске Федерација, 26. децембра 2014. године,[18] на основу тадашњих околности у вези са ситуацијом у Украјини и процени да приближавање НАТО инфраструктуре границама Русије представља директну војну претњу.

Стратегија информационе безбедности Руске Федерације

У Војној доктрини и Доктрини информационе безбедности Руске Федерације[19] нису коришћени темини са префиксом сајбер (безбедност, ратовање или операција) већ искључиво термини информациона безбедност и информационо ратовање. Руски војни аналитичари углавном користе термине сајбер (cyber/kiber) или сајбер ратовање (cyberwarfare/kibervoyna), осим када се говори о западним или другим страним изворима. Технички садржи холистички приступ који укључује рачунарске мреже, информациони рат, као и психолошке, односно пропагандне операције. Под тим се подразумева да је безбедност у сајбер простору део укупне информационе безбедности.

Појам информационе безбедности у Русији односи се на заштиту интереса појединца и његових права у информационој сфери, као и на заштиту друштва у целини и државе од унутрашњих и спољашњих опасности. Информациона безбедност

[16] Стратегија националне безбеднности РФ до 2020. (Стратегия национальной безопасности Российской Федерации до 2020 года). Документ је утврђен указом председника Медведева, 12. маја 2009. године. Претходна концепција је стављена ван снаге. Документ видети на официјелном сајту Савета безбедности РФ: http://www.scrf.gov.ru/documents/99.html tačke 4-6, pristup interentu, 27.06.2017.

[17] http://www.scrf.gov.ru/documents/6/, pristup interentu, 27.06.2017.

[18] Претходна Војна доктрина донета је 2010. године, а нове смернице за њену измену донете су још средином 2013. године. Коначна верзија усвојена је на седници Савета националне безбедности РФ 19.12. 2014. године.

[19] Доктрина Руске Федерације објављена 2010 године http://news.kremlin.ru/ref_notes/461.

је, у доктринарним документима Руске Федерације, дефинисана као „стање заштићености животно важних интереса личности, друштва и државе у информационој сфери од спољашњих и унутрашњих опасности (ризика)", односно „као стање заштићености информационе средине друштва које омогућава њено формирање, коришћење и развој у интересу грађана, организација и државе".

Као полазно становиште при дефинисању појма узет је интердисциплинарни приступ, тј. општа наука о безбедности. Уочава се да се у Доктрини информационе безбедности Руске Федерације термин информациона безбедност користи у ширем смислу, док је у западним изворима реч о ужем смислу појма, јер се односи само на информације и информационе системе.

Информациона стратегија безбедности Руске Федерације (2000) до недавно је била основни документ којим се Русија руководила по питањима безбедности информација. Намера документа је, поред осталог, била „да се осигурају уставна права и слободе човека и грађанина, слободно траже, примају, преносе, стварају и преносе информације законитим средствима".[20] Информациона безбедност је, према Стратегији, кључни елемент у животу друштва у Русији и има снажан утицај на стање економских, политичких и одбрамбених компоненти безбедности државе.

Сама доктрина издваја четити компоненте националних интереса Русије:

1. Прва компонента националних интереса у информационој сфери јесте поштовање уставних слобода и права човека и грађанина да прима и користи информације.

2. Друга компонента односи се на информациону подршку државне политике Русије која подразумева преношење информација о државној политици и друштвено значајним догађајима у руском и међународном животу.

3. Трећа компонента обухвата промовисање савремених информационих технологија и подстицање информационе индустрије.

4. Четврта компонента националних интереса Руске Федерације обухвата заштиту информационих ресурса од недозвољеног приступа и безбедност постојећих и будућих телекомуникационо-информационих система.

Национална информациона безбедност неодвојива је од националне безбедности. Са напретком технологија та зависност ће јачати. Информациона безбедност у Русији односи се на заштиту интереса појединца и његових права у информационој сфери, као и на заштиту комплетног друштва и државе у целини од опасности које прете на унутрашњем и спољњем плану. Не може да се сведе на традиционални појам заштите информација већ је неопходно шире ангажовање друштвених и државних структура.

Доктрина предвиђа одређено опхођење медија, како у државном, тако и у приватном власништву. Документ охрабрује развој метода за повећање ефикасности ангажовања државе „у формирању политике јавног информисања јавних медијских кућа".[21] Разлог због којег се доктрина бави медијима јесте спречавање пропагандних активности које би имале за циљ негативне ефекте и ширење дезинформација о унутрашњој политици Русије,"[22] као и „развој законских и институционалних меха-

[20] http://www.scrf.gov.ru/documents/5.html члан I, део 1 , приступ интеренту, 29.2017.

[21] http://www.scrf.gov.ru/documents/5.html члан I, део 4, приступ интеренту, 29.2017.

[22] http://www.scrf.gov.ru/documents/5.html члан II , део 6, приступ интеренту, 29.2017.

низама које треба да спрече нелегални утицај на колективну свест друштва ширењем дезинформација".[23]

Документ се осврће и на друге облике претњи по информациону/сајбер безбедност државе: претње према уставним правима и слободама, затим претње усмерене ка информационој безбедности државне политике, према националној информационој и телекомуникационој индустрији, према безбедности информација и информационих система.[24]

Руска Федерација заступа став да свака информациона операција коју покреће нека држава или савез држава против друге државе треба да буде квалификована као акт мешања у унутрашње послове и суверенитет. Према Војној доктрини Руске Федерације из 2010. године, једна од карактеристика модерних оружаних сукоба јесте „претходна примена мера информационог рата како би се без употребе војне силе остварио политички циљ".[25]

Информациони рат је, према ставу Руске Федерације, „конфликт између две или више држава у информационом простору са циљем наношења штете информационим системима, процесима и ресурсима од кључног значаја и других објеката, подривање политичког, економског и друштвеног система, масивни психолошки рад на становништву како би се дестабилизовало друштво и држава, и вршење притиска на владу да донесе одлуке супротне својим интересима".[26]

Једна од потенцијално највећих опасности у сајбер простору по државе представља дело сајбер шпијунаже. Руска Федерација је, поред осталих, била мета у једној од највећих, ако не и највећој сајбер шпијунској операцији названој „Red October"[27] (Црвени октобар). Напад који је имао за циљ крађу информација из компјутера влада држава широм света активан је од 2007. године. Касперски лабораторија, која је и открила напад, саопштила је да су у изузетно напредној софистицираној сајбер операцији, поред дипломатских и владиних агенција земаља широм света, на мети биле истраживачке институције, агенције за енергетику, нуклеарне групе, војни центри, нафтне и гасне компаније. „Rocra" (скраћено од „Red October") заразио је на стотине рачунара широм света. Касперски истраживање указује на то да је идентификовано 55.000 мета унутар 250 различитих ИП адреса.[28] Процењује се да је украдено неколико терабајта података[29] током периода од најмање пет година. Већина идентификованих инфекција лоциран је, углавном, у Источној Европи, затим у Северној Америци и земљама западне Европе – Луксембургу,[30] Швајцарској, Казахстану и Грчкој.[31]

---

[23] http://www.scrf.gov.ru/documents/5.html član II deo 7, pristup interentu, 29.2017.

[24] http://news.kremlin.ru/ref_notes/461 pristup interentu, 29. 2017.

[25] The Military Doctrine of the Russian Federation, approved by Russian Federation presidential edict on February 5, 2010 http://carnegieendowment.org/files/ 2010russia_military_doctrine.pdf.

[26] http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

[27] Red October , који је добио име по руској подморници из романа Tom Clanci „Lov na Crveni oktobar".

[28] http://www.dailymail.co.uk/sciencetech/article-2263322/Operation-Red-October-revealed-The-astonishing-hacker-attack-infiltrated-55-000-high-level-government-computers.html#ixzz3KHY4XBY1

[29] Ибид.

[30] http://securelist.com/blog/incidents/57647/the-red-october-campaign

[31] http://www.dailymail.co.uk/sciencetech/article-2263322/Operation-Red-October-revealed-The-astonishing-hacker-attack-infiltrated-55-000-high-level-government-computers.html#ixzz3KHY4XBY1

Након детекције „Црвеног октобра" и чињенице да су се шпијуни инфилтрирали у рачунарске системе влада и амбасада широм бившег совјетског блока, укључујући и Русију, председник Владимир Путин је наредио властима да се повећа ниво заштите државе сајбер средствима од могућих сајбер напада.

У јануару 2013. године председник Путин је одобрио декрет којим је додељено пуно овлашћење Федералној служби безбедности (ФСБ) да „створи државни систем за откривање, спречавање и ликвидацију ефеката компјутерских напада на информационе системе Руске Федерације".[32] У декрету се каже да највећу опасност Русија види у Интернет технологијама које могу да се користе као информационо оружје за мешање у унутрашње послове државе. Документ има назив „Основе државне политике Руске Федерације у области међународне информационе безбедности у периоду до 2020. године" и представља одговор на документ „Међународна стратегија деловања у сајбер простору" Сједињених Америчких Држава.[33]

Кључне инфраструктуре, дипломатска представништва и обавештајне структуре морају бити заштићени од било каквог напада. Главни страни извори претњи су: препознате активности страних политичких, економских, војних, обавештајних и информативних структура усмерене против Руске Федерације, настојање неких држава да доминирају у светској информационој сфери и делују против интереса Русије, активности међународних терористичких организација, обавештајне активности страних држава и развој концепата информационог ратовања страних држава усмерених ка другим државама, нарушавању нормалног функционисања информационих и комуникационих система, информационих ресурса и неовлашћеног приступа тим ресурсима. По декрету Русије идентификоване су четири највеће опасности у сфери међународне информационе безбедности:

1. Коришћење ИКТ технологија, као оружја за војно-политичке сврхе, са циљем да се изврши агресија.
2. Примена ИКТ у терористичке сврхе.
3. Опасност од растућих облика сајбер криминала.
4. Мешање у унутрашње послове државе.

Нова стратегија информационе безбедности Руске Федерације

Током децембра 2016. године председник Владимир Путин потписао је нову Доктрину о информационој безбедности Руске Федерације, замењујући Доктрину из 2000. године. То је један од стратешких и планских докумената и, као такав, изражава званичан став о управљању системом националне безбедности у информационој сфери државе. Реторички, текст подсећа на Стратегију националне безбедности, која је указивала на повишен ниво потенцијалних претњи усмерених према

[32] http://thebricspost.com/putin-orders-to-strengthen-cyber-security/#.VPx8AvnF_fI

[33] По овом документу диверзије у сајбер простору могу и биће сматране као традиционална војна дејства и САД имају право да бране свој сајбер простор свим средствима, укључујући и примену нуклеарног оружја.

Русији, и истиче значај очувања стратешке стабилности. Сходно томе, дух нове доктрине је мало оштрији, а претње су конкретније описане.

Информациона сфера дефинисана је у ширем смислу него у претходној доктрини. Кључни термин у овом смислу је „информационализација", који се односи на друштвене, економске и техничке процесе за усвајање и проширење информационих технологија у друштву и држави у целини, као и за обезбеђивање приступа информацијама. Ова промена указује на признање улоге у информационој сфери технолошког развоја, али, што је најважније, као средство којим се може промени друштвена структура.

Доктрина описује како су ИКТ технологије постале алат који се користи у интересу националне безбедности Русије и позива на већу улогу Интернета и управљање сигурношћу информација и домаћој производњи информационих технологија.

Поглед на претње из претходне доктрине појачава могућност претњи у погледу безбедности информација и угрожавања сајбер простора Русије. Могућност повећања броја и ефективности сајбер напада у војне сврхе, који долазе из иностранства, идентификовани су као главни негативни фактор. У Стратегији се, такође, наводи да је интензивирана сајбер шпијунажа према руским државним органима, научним институцијама и одбрамбеној индустрији. Према Доктрини, обим информација које психолошки утичу или могу утицати на становништво Руске Федерације расте, као и број сајбер криминалних активности, а наручито у финансијском сектору.

Када је реч о развоју сопствених технологија, Русија није успела да смањи вођство западних земаља. На пример, један од главних недостатака је развој сопствених, руских суперкомпјутера. Ова тема нашла се у нацрту доктрине, али је ипак уклоњена из коначне верзије документа. Зависност од информационих технологија које долазе из других држава чини друштвени и економски развој Русије „зависним од геополитичких интереса страних земаља".[34] Развојем сопствених хардвера и софтвера она жели да ублажи технолошку инфериорност, као што и приличи статусу моћне државе у 21. веку.

Нова доктрина идентификује заштиту права и слободе људи у информационој сфери, укључујући приступ информацијама и коришћења података као питања од националног интереса. Истовремено, предложено је да треба пронаћи биланс између права грађана на слободну размену информација и ограничења проузрокована потребом за националном безбедношћу у информативној сфери.

У тексту се указује и на потребу за континуираним праћењем претњи по информациону безбедност, као и на контролу над руским сајбер простором од стране органа безбедности. Контрола би се спроводила као део одговора на унутрашње и спољашње претње по информативну сферу и сајбер простор Руске Федерације.

Као додатне правне мере за управљање информационом безбедношћу, у јулу 2016. године председник Путин је потписао амандмане Савезног закона „о сузбијању тероризма", као и допуне Кривичног законика. Ови амандмани, под називом „Yarovaya Laws", захтевају да оператери мрежа и Интернет провајдери поседују и чувају податке о корисницима, корисничким активностима и комуникацији корисника на територији Руске Федерације у периоду од годину дана, што многи заговорни-

[34] http://isnblog.ethz.ch/intelligence/russias-new-information-security-doctrine-guarding-a-besieged-cyber-fortress

ци слободе говора на Интернету сматрају драстичним.[35] Такође, захтева се да се чува садржај корисничких комуникација на територији Русије у трајању до шест месеци, почевши од јула 2018. године, као и да се омогући руским безбедносним агенцијама да приступе и дешифрују преписке.

Иако је овакав потез врха Руске Федерације наишао на неодобравање појединих група, које наводе да се тиме повећава надзор коју институције спроводе у сфери сајбер простора, у питању је стратешки потез, као и аспирација да се задржи статус велике силе. Такође, оваква метода може уједно да спречи и предупреди потенцијалне терористичке активности, како на територији државе, тако и у регион и свету, али и да смањи финансијске губитке које сајбер криминал односи собом.

Активност Русије на међународном нивоу

Руска Федерација се изузетно залаже за међународну сарадњу на пољу сајбер, односно информационе безбедности. Русија је дала допринос регулисању нових међународних претњи које проистичу из употребе информационо-комуникационих технологија подношењем предлога резолуције током 53. заседања Генералне скупштине УН 1998. године.

Под покровитељством Руске Федерације, 4. децембра 1998. године, поднета је резолуција 53/70, која се бави „прогресивним кретањем у области информисања и телекомуникацијама у контексту међународне безбедности". Русија се још у то време залагала за формирање међународне регулативе, схватајући да наука и технологија имају важну улогу у међународној безбедности. Информациона технологија је, ипак, рањива и склона злоупотребама криминалаца, криминалних група и потенцијално терориста. Ова почетна иницијатива представила је основне принципе обезбеђивања међународне безбедности у области информационе безбедности.

Генерална скупштина УН је 2001. године успоставила Групу владиних експерата за развој у области информација и телекомуникација у контексту међународне безбедности која је заседала у периоду 2004–2005. године.[36] Предлогу руске резолуције Доприноси у пољу информација и телекомуникација у контексту међународне безбедности на Генералној скупштини УН 2008. године придружило се још 22 државе, док је на коначном гласању поводом резолуције, 167 држава прихватило овај предлог, док су против биле једино САД.[37] Руски став подржава много шири круг држава, укључујући њене најближе савезнике, већину држава трећег света, као и БРИКС партнери – Кина, Бразил и Индија.

Руска Федерација је активни заговарач формирања међународне регулативе која се односи на информациону, односно сајбер безбедност. Више од деценије и по Русија се

[35] https://www.rferl.org/a/russia-yarovaya-law-religious-freedom-restrictions/27852531.html

[36] General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/56/19,
http://daccess-dds ny.un.org/doc/UNDOC/GEN/N01/476/28/PDF/N0147628.pdf?OpenElement

[37] Драган Д. Младеновић, Мирјана Дракулић, Данко Јовановић, Дефинисање сајбер ратовања, Војнотехнички гласник, 2012, Vol. LX, No. 2, стр. 102.

труди да придобије међународну подршку за ове норме. Ипак, постоји Конвенција која се тиче регулисања сајбер криминала – Будимпештанска конвенција Савета Европе.

Савет Европе (СЕ) је у јулу 2004. године усвојио Конвенцију о високо технолошком криминалу, која представља прву међународну конвенцију за решавање овог проблема. Конвенција садржи релативно висок стандард међународне сарадње за истрагу и кривично гоњење за извршиоце дела високо технолошког криминала. Конвенција је истакла радње које држава треба да предузме за спречавање, вођење истраге и кривично гоњење одговорних за дела која укључују, поред осталог, кршење ауторских права, рачунарске преваре, дечију порнографију и кршења безбедности на мрежи.[38] Наведено је које радње се сматрају делима против поверљивости, интегритета и доступности компјутерских података и система (за, на пример, илегални приступ, илегална прислушкивања, недозвољено мењање података, злоупотребе уређаја[39]). Са друге стране, садржи и низ овлашћења и поступака, као што су претрес рачунарских мрежа и пресретања.

Иако је Русија добила позив да постане страна уговорница, она константно одбија да ратификује споразум, иако је сагласна са потенцијалном сарадњом. Главни разлог за негодовање односи се на члан 32 Конвенције у којем се каже: „Држава може, без одобрења других страна ... приступити или примити, кроз компјутерски систем на својој територији, сачуване рачунарске податке који се налазе у некој другој држави, ако их држава добије на законитим и добровољним пристанком особе која има законско овлашћење да обелодани податке државе тог компјутерског система".[40] Кључни израз на који руска страна ставља примедбу је: „без одобрења друге стране", што је по њој недопустиво кршење принципа суверенитета једне државе.[41]

Закључак

Информације и комуникације увек су имале стратегијски значај. Међутим, данас су оне са помоћних позиција доспеле у први план. Проблем информационе безбедности постао је основни проблем међународне заједнице. Информационе технологије не познају државне границе и омогућавају повезивање целог света – држава, организација и појединаца. Међутим, уз све бенефите које нам је донео, сајбер простор носи и низ опасности које могу да угрозе грађане, друштво, али и државе.

Нова друштвено-економска формација друштва повлачи за собом и нове опасности. Нове претње изискују нове приступе. У домену информационе сфере, с једне стране, потребно је обезбедити друштво информационим ресурсима а, са друге стране, формирати систем заштите информационих потенцијала. У случају потенцијалног сајбер ратовања потребно је обезбедити и заштиту државе и њеног сајбер простора.

На примеру Руске Федерације уочава се заинтересованост за даље развијање ове области, а представљени су и начини на које највећа држава света штити своје интересе

[38] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[39] Ibid.

[40] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[41] Keir Giles, Russia's Public Stance on Cyberspace Issues, 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 © NATO CCD COE Publications, Tallinn, str. 65- 67.

у сајбер простору. Сајбер ратовање је за Русију питање од геостратешког значаја и једна од највећих претњи по национални суверенитет, као и међународну заједницу у целини.

Међународна заједница мора да прихвати нова правила игре када је у питању сајбер безбедност и међународним одговором регулише сајбер нападе као једну од потенцијално највећих претњи по државе. Од Руске Федерације, као сајбер силе, може се и у будућности очекивати да ће бити активан актер у сајбер простору и покушати да наметне међународно решење пред међународним организацијама, пре свих у Уједињеним нацијама.

Литература

[1] Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn, 2012, NATO Cooperative Cyber Defence Centre of Excellence

[2] General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/56/19, http://daccess-ddsny.un.org/doc/UNDOC/GEN/N01/476/28/PDF/N0147628.pdf?OpenElement

[3] Dragan D. Mladenović, Mirjana Drakulić, Danko Jovanović, Definisanje sajber ratovanja, Vojnotehnički glasnik, 2012, Vol. LX, No. 2,

[4] David Dean et al., 'The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy,' BCG. Perspectives, 27 January 2012.

[5] Doktrina Ruske Federacije objavljena 2010. godine http://news.kremlin.ru/ref_notes/461

[6] http://www.intelros.ru/subject/ross_rasput/2026-koncepcija-dolgosrochnogo-socialno.html

[7] http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

[8] http://www.dailymail.co.uk/sciencetech/article-2263322/Operation-Red-October-revealed-The-astonishing-hacker-attack-infiltrated-55-000-high-level-government-computers.html#ixzz3KHY4XBY1

[9] http://thebricspost.com/putin-orders-to-strengthen-cyber-security/#.VPx8AvnF_fI

[10] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[11] http://isnblog.ethz.ch/intelligence/russias-new-information-security-doctrine-guarding-a-besieged-cyber-fortress

[12] https://www.rferl.org/a/russia-yarovaya-law-religious-freedom-restrictions/27852531.html

[13] http://www.parlament.gov.rs/akti/doneti-zakoni/doneti-zakoni.1033.html

[14] http://www.telegraph.co.uk/news/uknews/defence/8369520/Military-Balance-report-countries-creating-new-cyber-warfare-organisations.html

[15] http://www.ratel.rs/informacije/novosti.234.html?article_id=1724

[16] http://m.guardian.co.uk/technology/2013/feb/21/white-house-cyber-threat-russia-china

[17] K. Giles, "Information Troops: A Russian Cyber Command?," in Third International Conference on Cyber Conflict, CCDCOE, 2011.

[18] Keir Giles, Russia's Public Stance on Cyberspace Issues, 2012 4th International Conference on Cyber Confl ict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012, NATO CCD COE Publications, Tallinn.

[19] Kovač, M., Stojković, B., Strategijsko planiranje odbrane, Vojnoizdavački zavod, Beograd, 2009.

[20] Концепция долгосрочного социально-экономического развития Российской Федерации до 2020 г, Strategija nacionalne bezbednnosti RF do 2020. (Strategiя nacionalьnoй bezopasnosti Rossiйskoй Federacii do 2020. goda) http://www.scrf.gov.ru/documents/99.html

[21] Robert S. Dewar The "Triptych of Cyber Security": A Classification of Active Cyber Defence, 2014 6th International Conference on Cyber Confl ict 2014, NATO CCD COE Publications, Tallinn.