УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

Марко М. Ракић

КРИЗНИ МЕНАЏМЕНТ У ФУНКЦИЈИ ЗАШТИТЕ КРИТИЧНИХ ИНФРАСТРУКТУРА У ЗЕМЉАМА У ТРАНЗИЦИЈИ

докторска дисертација

Београд, 2015

UNIVERSITY OF BELGRADE

FACULTY OF SECURITY STUDIES

Marko M. Rakić

CRISIS MANAGEMENT IN THE FUNCTION OF THE PROTECTION OF THE CRITICAL INFRASTRUCTURES IN THE TRANSITION COUNTRIES

Doctoral Dissertation

Belgrade, 2015

Ментор:

Др Желимир Кешетовић, редовни професор,

Универзитет у Београду − Факултет безбедности

Чланови комисије:

Др Владимир Јаковљевић, редовни професор,

Универзитет у Београду − Факултет безбедности

Др Озрен Џигурски, ванредни професор у пензији

Датум одбране:_____

КРИЗНИ МЕНАЏМЕНТ У ФУНКЦИЈИ ЗАШТИТЕ КРИТИЧНИХ ИНФРАСТРУКТУРА У ЗЕМЉАМА У ТРАНЗИЦИЈИ

Кризе се јављају и еволуирају паралелно са развојем људских друштава, тако да читава историја људске врсте представља хронологију догађања несрећа и невоља, и настојања да се оне што ефикасније отклоне. Промене почетком деведесетих година 20. века условљене су интензивним развојем технологије и економским, политичким, идејним, културолошким и војним повезивањем људи, чиме је аутоматски повећана способност човека да се супротстави кризама. Међутим, поред тога што савремени системи обезбеђују виши степен сигурности у свакодневном животу, "модерно доба" рађа разноврсне и бројне кризе чија је разорна моћ све већа. У земљама широм света не придаје се адекватан значај улози кризног менаџмента у заштити инфраструктура од виталног националног значаја, а на хоризонту се већ појављују извори и облици угрожавања безбедности који могу изазвати нове кризе: економска нестабилност, сајбер тероризам, техно тероризам, ширење оружја за масовно уништење, глобално отопљавање, климатске промене и др.

Измењена природа претњи глобалној безбедности условила је и развијање нових безбедносних концепција. Као један од примарних и најзначајнијих безбедносних изазова "новог доба" намеће се питање заштите критичних инфраструктура. Инфраструктуре попут саобраћајне мреже, воде, енергије, хемијске и нуклеарне индустрије, и ИКТ пружају основне услове за функционисање појединаца и група. Високо развијене земље дају предност информационим инфраструктурама и производњи, преносу и дистрибуцији нафте, гаса и електричне енергије, док се неразвијене и земље у транзицији сусрећу са егзистенцијалним питањима несташице воде и хране. Земље у транзицији, поред наведених отежавајућих околности, приликом преласка из једног друштвено-економског система у други суочене су и са бројним проблемима, као што су: укључивање у слободно тржиште без адекватне економске политике; технолошка заосталост; дотрајалост инфраструктурних објеката; нејасно идентификовани извори и облици угрожавања критичних инфраструктура; недовољно прецизна класификација критичних сектора; непостојање кохерентног правног оквира посебно у сфери јавно-приватног партнерства (*Private-Public Partnership* – PPP), недостатак финансијских средстава за унапређење технологије и спровођење нових

програма обуке запослених, што се све директно одражава на ефикасност система управљања кризама и заштиту критичних инфраструктура.

Чињеница је да земље у транзицији имају различита искуства за пример су узете оне земље које су биле најуспешније (Словенија и Бугарска). Истраживањем је сагледавано стање угрожености и заштите критичних инфраструктура и других проблема који се јављају у овој области и могућности унапређења кризног менаџмента у функцији заштите критичних инфраструктура. На основу добијених резултата, применом метода моделовања, изведени су и одређени закључци и предлози у вези са квалитетом, ефикасношћу и могућим недостацима заштите инфраструктура од виталног националног интереса Републике Србије.

Кључне речи: кризни менаџмент, критичне инфраструктуре, извори и облици угрожавања КИ, заштита КИ.

Научна област: Науке безбедности

Ужа научна област: Кризни менаџмент

УДК број: 005.334 (4-11)

CRISIS MANAGEMENT IN THE FUNCTION OF THE PROTECTION OF THE CRITICAL INFRASTRUCTURES IN THE TRANSITION COUNTRIES

Crises occur and evolve concurrently with the development of human societies, so the whole human kind history is a chronology of the occurrence of tragedies and misfortunes, as well as tendencies for them to be eliminated as efficient as possible. Changes in the early 1990s were established by an intensive development of technology and economic, political, conceptual, culturological and military connections among people, which has automatically increased human's capability of facing crises. However, besides the fact that modern systems provide a higher safety degree in everyday life, "modern age" gives birth to various and numerous crises whose ravaging power is getting more and more intensive. Worldwide countries do not give adequate significance to the role of crisis management in the protection of infrastructures of vital national importance, some sources and forms of safety disturbance which may cause new crises are already emerging on the horizon: economic instability, cyber-terrorism, techno-terrorism, spread of weapons of mass destruction, global warming, climate changes, etc.

Altered character of global safety threats has brought about the development of new safety conceptions. As one of primary and most significant safety challenges of "new age", issue of the protection of critical infrastructures is imposed. Infrastructures such as transportation network, water, energy, chemical and nuclear industry and the ICT offer basic conditions for individual and group functioning. Highly developed countries give preference to information infrastructures and production, transfer and distribution of oil, gas and electric energy, whereas undeveloped countries and transition countries face with existential issues of water and food scarcity. Besides mentioned impeding circumstances, transition countries, when transiting from one socio-economic system to another, also face with numerous problems, such as: joining free market with no adequate economic policy; technological underdevelopment; worn-out infrastructural facilities; vaguely identified sources and forms of the vulnerability of critical infrastructures; insufficiently precise classification of critical sectors; lack of a coherent legal framework, especially in the field of private-public partnership – the PPP, lack of financial funds for the improvement of technology and implementation of new training courses for employees, which directly reflects the efficiency of the system of crisis management and protection of critical infrastructures.

The fact that transition countries have different experience, the most successful countries (Slovenia and Bulgaria) were taken as an example. State of vulnerability and protection of critical infrastructures and other problems which occur in this field, as well as possibilities of the improvement of crisis management in the function of the protection of critical infrastructures were reviewed by means of research. Based on the obtained findings, by the application of modelling methods, certain conclusions and suggestions were derived referring to quality, efficiency and possible deficiencies of the protection of infrastructures of vital national interest of the Republic of Serbia.

Keywords: crisis management, critical infrastructures, sources and forms of vulnerability of critical infrastructures, protection of critical infrastructures

Scientific field: Security studies

Specialized scientific field: Crisis management

UDC No. 005.334 (4-11)

САДРЖАЈ

СПИСАК ТАБЕЛА

СПИСАК СЛИКА И ГРАФИКОНА

УВОД

Кризе се јављају и еволуирају паралелно са развојем људских друштава, тако да читава историја људске врсте представља хронологију догађања несрећа и невоља, и настојања да се оне што ефикасније отклоне. Временске епохе, које су обележиле различите кризе, проткане су бројним друштвено-културним променама. Те промене су почетком деведесетих година 20. века условљене интензивним развојем технологије и економским, политичким, идејним, културолошким и војним повезивањем људи, чиме је аутоматски повећана способност човека да се супротстави кризама. Међутим, поред тога што савремени системи обезбеђују виши степен сигурности у свакодневном животу, *модерно доба* рађа разноврсне и бројне кризе чија је разорна моћ све већа. Историја Евро-азијског континента, као колевка људске цивилизације, обилује бројним примерима најразноврснијих криза које су се јављале као последице деградације животне средине, нуклеарног застрашивања, разних пандемија, економских криза, тероризма. Док владе земаља широм света и даље не придају адекватан значај улози кризног менаџмента у заштити инфраструктура од виталног националног значаја, на хоризонту се појављују извори и облици угрожавања безбедности који могу изазвати нове кризе: економска нестабилност, сајбер тероризам, техно тероризам, ширење оружја за масовно уништење, глобално отопљавање и климатске промене.

Крах биполарног поретка, који је био праћен Хладним ратом, изменио је из корена природу претњи глобалној безбедности. Главна карактеристика постхладноратовског периода била је стављање нагласка на способност држава у суочавању са не-војним изворима и облицима угрожавања безбедности који могу изазвати веома сложене друштвено-политичке кризе. На ове промене у значајној мери утицали су догађаји као што су терористички напади (САД 2001, Мадрид 2004, Лондон 2005. и Париз 2015. године), разне пандемије (СИДА, САРС, болест *лудих крава*, птичији грип, свињски грип, Ебола) и други невојни извори и облици угрожавања безбедности који могу довести до сложених криза, како на националном тако и на наднационалном нивоу, као и индустријске и природне катастрофе са каскадним ефектима (Фукушима).

Измењена природа претњи глобалној безбедности условила је и развијање нових безбедносних концепција. Као један од примарних и најзначајнијих безбедносних изазова *новог доба* намеће се питање заштите критичних

инфраструктура, јер функционисање модерног друштва у великој мери зависи од ефикасне заштите значајних инфраструктурних објеката. Инфраструктуре попут саобраћајне мреже, воде, енергије, хемијске и нуклеарне индустрије, и информационих и комуникационих технологија пружају основне услове за функционисање појединаца и група.

Временом, инфраструктуре постају веома *критичне* за функционисање друштва, јер економски и друштвени процеси у великој мери зависе од услуга које пружају ови системи. Њиховим онеспособљавањем може се нанети велика штета локалним заједницама, државама и наднационалним организацијама. Свесне наведених чињеница, владе земаља широм света све више увиђају значај критичних инфраструктура, и почињу да раде на унапређењу поузданости и сигурности инфраструктурних система.

Последњих година, бројни програми заштите критичних инфраструктура покренути су како на националном тако и на наднационалном нивоу. Већина земаља чланица Савета евроатлантског партнерства је започела поступак израде националних мапа критичне инфраструктуре. Поред НАТО-а, сличне програме покренули су и Европска унија, Уједињене нације, Организација за економску сарадњу и развој, низ регионалних организација итд. На глобалном нивоу воде се озбиљне расправе о редоследу приоритета у заштити критичних инфраструктура. Високо развијене земље Европе и Северне Америке дају предност информационим инфраструктурама и производњи, преносу и дистрибуцији нафте гаса и електричне енергије, док се неразвијене земље сусрећу са егзистенцијалним питањима несташице воде и хране.

Када је реч о односу кризе и заштите критичних инфраструктура треба имати у виду да криза у овим ентитетима има посебан значај у првом реду због изузетне важности ових виталних система за функционисање целог друштва.[1] Стога су успешна превенција и управљање кризним ситуацијама у директној вези са ефикасним системом заштите критичних инфраструктура. Мере попут превенције, припремљености и адекватног одговора на кризу повећавају степен сигурности критичних инфраструктура.

Практични примери криза које могу угрозити критичне инфраструктуре су многобројни: пожари и експлозије у нуклеарним или хемијским комплексима, незгоде приликом транспорта и складиштења отровних материја, злоупотреба сајбер простора

[1] Кешетовић, Ж., (2008), *Кризни менаџмент*, Факултет безбедности, Службени гласник, Београд, стр. 43

за различите субверзије. Многи научници сматрају да је дошло до пораста кризних ситуација које могу изазвати катастрофу овог типа. Иако теоретичари имају различита објашњења за ово повећање, њихово интересовање је првенствено усмерено на разлоге због којих је дошло до катастрофе и на управљање кризом након инцидента.

Данас, када отрови испуштени у нуклеарним или хемијским удесима могу изазвати масовну смрт и болест (као што је то био случај са Чернобилом и Фукушимом), када разне пандемије и еколошке катастрофе попут АИДС-а и *ефекта стаклене баште* могу угрозити читаву планету, потребно је изградити један шири приступ ради успешније превенције криза које ови безбедносни ризици могу изазвати. Поред тога, како појединачне економије постају све више уплетене у светску економију, свако друштво постаје све рањивије на светску економску кризу. Такође, и међусобно повезивање рачунара путем телекомуникационе мреже отвара простор за угрожавање критичних инфраструктура. Последице оваквих напада могу бити и фаталне уколико се угрозе поједине инфраструктуре, као што су, на пример, системи за контролу копненог и ваздушног саобраћаја, хидроцентрала, нуклеарних електрана, безбедносних и здравствених служби или служби за дистрибуцију електричне енергије.Тако да се у новом контексту мења и круг субјеката који почињу да се баве кризним менаџментом, као и сама природа односа који се успостављају између ових субјеката.

1. ТЕОРИЈСКО-МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

1.1. Проблем истраживања

Нова констелација снага у међународним односима и нови извори и облици угрожавања безбедности доводе до промене унутрашњег система вредности, друштвених и државних приоритета и структура. Ови процеси условили су и промену схватања саме суштине кризе, као и концепција везаних за управљање кризама и заштиту критичних инфраструктура. Наиме, претње су биле присутне и за време Хладног рата, али биле су конципиране искључиво на војном нивоу. Уласком у транзицију мења се начин заштите критичних инфраструктура као и приступ управљању кризама.

У наведеном контексту земље у транзицији налазе се у специфичном положају, суочавајући се са дубоком трансформацијом у свим сферама. Ове земље улажу велике напоре како би успоставиле демократске институције и превазишле бреме комунистичког наслеђа, јер је изградња демократских структура један од предуслова за ефикасно решавање конфликтних ситуација кроз усвајање различитих резолуција. Елементи резолуција које се тичу конфликата и успостављања мира и стабилности, као што су преговарање, дијалог и изградња поверења кључни су за успешан прелазак на демократски систем уређења.[2]

Због недовољне развијености демократских институција земље у транзицији су склоније избијању криза. Ову чињеницу потврђују бројне студије кризног менаџмента у земљама Централне и Источне Европе које сведоче о повишеној учесталости кризних ситуација у односу на развијене земље Западне Европе.[3] Поред тога, идентификовани су и специфични услови за практиковање кризног менаџмента у земљама у транзицији. Првенствено реч је о изразитој политизацији и медијализацији криза у овим земљама, као и о сукобу националних и европских норми које се директно тичу решавања одређених кризних ситуација, односно правца реорганизовања система и институција кризног менаџмента.[4] Отежавајућу околност представља и инертност, односно корени старог система.

Земље у транзицији, поред наведених отежавајућих околности, приликом преласка из једног друштвено-политичког система у други суочене су и са бројним

[2] Engelbrekt, K., Fröberg, M., (2005), *Managing Political Crises in Bulgaria: Pragmatism and Procrastination*, Elanders Gotab, Stockholm, p. 7-8
[3] Ibid, p.13
[4] Brändström, A. and Malešič, M., (eds.) (2004), *Crisis Management in Slovenia: Comparative Perspectives*, Stockholm: Crismart, National Defence College, pp 19-23, 348-356

проблемима који такође не постоје у стабилним демократским државама. Укључивање у слободно тржиште, углавном без адекватне економске државне политике, доводи до ширења сиромаштва и разочарења широких друштвених слојева, што главне доносиоце политичких одлука ставља у веома тешку ситуацију. Лоша економска ситуација често може бити узрок избијања криза.

Један од проблема са којим су суочене земље у транзицији, а који је повезан са стопом економског развоја, је технолошка заосталост у односу на развијене земље Западне Европе и света. Нагли и све бржи развој информационо-комуникационе технологије, сателитских комуникација и Интернета захтева континуирани технолошки развој као и константну обуку запослених, што изискује значајна финансијска средства. Земље у транзицији најчешће нису у могућности да издвоје потребна новчана средства за унапређење технологије и спровођење нових програма обуке запослених, што се директно одражава на ефикасност система управљања кризама и заштите виталних инфра-структура.[5]

Даље, већина земаља у транзицији нема јасно идентификоване изворе и облике угрожавања критичних инфраструктура, као ни прецизну класификацију критичних сектора.[6] Један од главних разлога оваквом стању у овој области јесте дотрајалост инфраструктура које не могу одговорити захтевима прописаним од стране НАТО-а и Европске уније. Застарели програми заштите критичних инфраструктура, који датирају још из доба социјализма и почивају на хладноратовским поставкама (војни извори и облици угрожавања безбедности су доминантни), не могу стати на пут савременим безбедносним изазовима и обезбедити ефикасно функционисање инфраструктура од виталног значаја.[7] За успостављање ефикасне заштите критичних инфраструктура у земљама у транзицији неопходна је модернизација застарелих инфраструктурних објеката, која захтева високе инвестиције за реконструкцију читавих сектора.[8]

Такође један од значајнијих проблема са којим се сусрећу земље у транзицији, када је у питању управљање кризама и заштита критичних инфраструктура, је трансформација сектора безбедности. Приватна безбедност је уско повезана са заштитом критичних инфраструктура, јер је велики број ових инфраструктурних

[5] Вулетић, Д., (2011), *Заштита критичних информационих инфраструктура*, Зборник радова са Конференције о безбедности информација, Универзитет Метрополитан, Београд, стр. 59
[6] Ibid
[7] Hirschhausenand, von C., Berit, M., (2001), *Infrastructure Policies and Liberalization in the East European Transition Countries: Would Less Have been More?,* Proposal for the Annual Congress of the European Economic Association Université de Lausanne, Switzerland, p. 3-5
[8] Ibid

објеката под заштитом приватних безбедносних компанија. Успешно функционисање сектора приватне безбедности у већини земаља Западног Балкана онемогућено је услед непостојања правних основа и теоријске подршке.[9] Непостојање кохерентног правног оквира у овој сфери отежава сарадњу између приватног и јавног сектора, а та сарадња је заправо кључ успешне заштите критичних инфраструктура и ефикасног деловања у кризним ситуацијама.[10]

Овај проблем додатно је отежан неефикасним јавно-приватним партнерством (*Private-Public Partnership*). У већини земаља у транзицији значајан део инфраструктуре је у приватном власништву или у процесу приватизације, а сарадња власника инфраструктура са државним институцијама је веома лоша. Један од главних разлога оваквог стања је непостојање законског оквира који би приморао власнике и оператере да учине потребне кораке зарад ефикасне сарадње са државним институцијама.[11]

Приликом идентификовања наведених проблема са којима је суочена већина земаља у транзицији, веома је важно имати у виду да свака од ових земаља има одређене специфичности (величина територије, економски развој, политичке и историјске околности, међународни статус, култура, традиција и слично), и да је због тога заиста тешко изводити универзалне закључке и правити генерализације. Чињеница је да ове земље имају различита искуства везано за пролазак кроз период транзиције, и да за пример треба узимати оне земље које су биле најуспешније (Словенија). Искуства успешних транзиционих земаља могу бити од велике користи државама које су у фази развоја система за решавање кризних ситуација и политике заштите инфраструктура од виталног националног интереса.

Што се тиче Републике Србије, иако је криза постала начин живота на овим просторима, теоријска мисао и пракса управљања кризама и заштите критичних инфраструктура налазе се на самом почетку. У већини кризних ситуација практично поступање је често било неосмишљено и панично, односно веома слично инстиктивном реаговању, при чему критичне инфраструктуре нису биле заштићена на адекватан начин. Може се рећи да је за врема социјалистичког самоуправљања постојао релативно функционалан систем за управљање кризама и да су значајне

[9] Талијан, М., *Менаџмент и безбедност: Прве установе приватне безбедности у Србији*, Видети на: http://www.gmbusiness.biz/index.php/arhiva/31-40/gm_32/prve_ustanove_privatne_bezbednosti_u_srbiji.html
[10] Nickolov, E., (2005), *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations,* Information and Security Journal, Vol. 17, p. 118
[11] Tagarev, T. and Pavlov, N., (2007), *Planning Measures and Capabilities for Protection of Critical Infrastructures*, Information and Security Journal, Vol. 22, p. 39

инфраструктуре биле заштићене на одговарајући начин. Међутим, са уласком у процес транзиције у Србији се овај систем урушава и настаје вакуум. У већини кризних ситуација у разним областима практичари су реаговали исхитрено, без стратешке визије и било каквог плана. Оваквим приступом и деловањем, у покушајима успостављања демократског друштва, долази до тога да су од 1990. године па на даље кризе сустизале једна другу и постале свакодневница српског друштва.

На прагу 21. века Република Србија се налази на новој прекретници, као једна од последњих европских земаља у транзицијизи она покушава да успостави везу са модерним европским демократијама, развије концепт владавине права, реформише законску регулативу и укључи се у регионалне и светске токове. Стога се питање изградње адекватног система кризног менаџмента и заштите инфраструктура од круцијалног значаја намеће само по себи, како на државном нивоу тако и у јавним предузећима, профитном сектору, образовању, туризму, спорту и другим областима.

Имајући у виду наведене чињенице, можемо закључити да у контексту савремених глобалних претњи, управљање кризама и успостављање заштите критичних инфраструктура представља приоритетан задатак заједница локалне самоуправе, сваке државе, као и наднационалних творевина, тако да ће основно питање које сагледава овај рад гласити: *Како посредством кризног менаџмента успоставити ефикасније мере заштите критичних инфраструктура у земљама у транзицији?* Одговор на формулисано проблемско питање омогућиће комплексну анализу и оцену безбедносних претњи и ризика и давање препорука за превенцију и управљање кризама и успостављање ефикасне заштите критичних инфраструктура.

1.2. Предмет истраживања

На основу претходно формулисаног проблема, **предмет овог истраживања биће сагледавање стања угрожености и заштите критичних инфраструктура у земљама у транзицији, основних проблема који се јављају у овој области и могућности унапређења кризног менаџмента у функцији заштите критичних инфраструктура у овим земљама.**

С обзиром на уочене недостатке у досадашњој тематизацији проблема истраживања, сматрамо да је неопходно заузети холистички приступ у истраживању кризног менаџмента у функцији заштите критичних инфраструктура. Такав би приступ подразумевао интегративно проучавање које би обухватило све димензије ових појава. Узимајући у обзир фрагментарност досадашњих истраживања, недовољну развијеност

теоријског оквира и непостојање јасно дефинисаних основних појмова, ми ћемо се усредсредити на исцрпну дескрипцију и класификацију манифестних облика ових концепата са аспекта безбедносних наука у циљу синтетизовања полазне грађе за будуће теоријске и емпиријске радове који ће се бавити овом тематиком.

На основу прегледа домаће[12] и иностране,[13] научне и стручне литературе, могу се уочити одређене, битне, тенденције кризног менаџмента у функцији заштите критичних инфраструктура. Намера нам је да интегришемо тенденције у један оквир показујући тиме како је управљање кризама од изузетног значаја за заштиту критичних инфраструктура.

Ради прецизнијег одређења самог предмета истраживања неопходно је, полазећи од теоријских сазнања, утврдити и операционалне дефиниције основних појмова.

Како би се ускладиле различите перспективе, термин *криза* се често користи у широком значењу, односно као концепт који обухвата све типове негативних догађаја. У још ширем значењу термин *криза* се примењује на ситуације које су нежељене, неочекиване, непредвидиве и тешко замисливе, а узрокују неверицу и несигурност.[14]

Ауторитети из области кризног менаџмента износе различите дефиниције термина *кризе*. Тако на пример, Хамблин кризу дефинише као "ургентну ситуацију у којој се сви чланови групе сусрећу са заједничком претњом". С друге стране, Паучант и Митроф кризу виде као "поремећај који физички погађа систем као целину и угрожава његове темељне претпоставке, његову самобитност и суштину". Финк тврди да је криза сваки

[12] Из прилично оскудног домаћег фонда издвајамо: Кешетовић, Ж., (2008), *Кризни менаџмент*, Факултет безбедности, Службени гласник, Београд; Кешетовић, Ж., Кековић, З., (2006), *Кризни менаџмент 1, Превенција кризе*, Факултет безбедности, Београд; Кешетовић, Ж., *Управљање кризним ситуацијама као део система безбедности Републике Србије*, у Гаћиновић, Р., (2010), *Србија – Изградња националне безбедности*, Зборник радова, Институт за политичке студије, Београд, стр. 235-250; Keković, Z. et al, *National Critical Infrastructures – Regional Perspective*, Faculty of Security Studies, Belgrade/Institute for Corporative Security Studies, Ljubljana.

[13] Из иностране литературе издвајамо: Macaulay, T., (2008), *Critical Infrastructure - Understanding Its Component Parts,Vulnerabilities, Operating Risks and Interdependencies*, CRC Press, London; Gottschalk, J., (2002), *Crisis Management*, Capstone Publishing, Oxford; Borodzicz, E., (2005), *Risk, Crisis and Security Management*, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,; Боин, А., Харт, П., Штерн, Е., Санделијус, Б., (2010), *Политика управљања кризама*, Факултет безбедности, Службени гласник, Београд; Brändström, A., Malešić, M., (2004), *Crisis Management in Slovenia: Comparative Perspectives*, Slovenian Ministry of Defense and SEMA, Stockholm; Engelbrekt, K., Förberg, M., (2005), *Managing Politicial Crises in Bulgaria: Pragmatism and Procrastination*, Swedish National Defense College/Swedish Emergency Management Agency/Ministry of Foreign Affairs Sweden, Stockholm; Perrow, C., (1984), *Normal Accidents: Living with High-Risk Technologies*, Basic Books, New York; Haimes, Y.Y., Longstaff, T., (2002), *The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism*, Risk Analysis, Vol. 22, No.3, Oxford; Radvanovsky, R., McDougall, A., (2010), *Critical Infrastructure, Homeland Security and Emergency Preparedness,* Second edition, CRC Press, Taylor & Francis Group, New York; Caleta, D. and Shemella, P., Counter Terrorism Challenges Regarding the Process of Critical Infrastructure Protection for Corporative Security Studies/Center for Civil-Military Relations, Ljubljana/Monterey.

[14] Кешетовић, Ж., (2008), *Кризни менаџмент*, Факултет безбедности, Службени гласник, Београд, стр. 15

догађај који може ескалирати у интензитету, доћи у жижу интересовања медија и владе, ометати нормалне пословне операције и погодити имиџ и профит компаније. У Лондонској школи за односе с јавношћу (LSPR) кризу одређују као стварни инцидент који утиче на човекову безбедност, околину, производе или углед организације. Коначно, Персон и Клер дефинишу кризу као "догађај мале вероватноће и великих последица који угрожава живот организације, а карактеришу га нејасни узроци, ефекти и средства за решење, као и уверење да се одлуке морају доносити брзо".[15]

Савремену дефиницију кризе изводи Пол Харт наглашавајући да је она "непријатан догађај, који представља изазов за доносиоце одлука, искушава их да поступају у условима угрожавања, временске стиске и неспремности". Он кризу види као "озбиљну претњу основним структурама или фундаменталним вредностима и нормама социјалног система која, у условима временског притиска и веома несигурних околности, захтева доношење критичних одлука". Хартова дефиниција има две значајне карактеристике. Прво, њена предност је у томе што се може применити на све врсте поремећаја (еколошке претње, сломове информационо-комуникационих система, економске кризе, унутар државне конфликте, побуне у затворима, регионалне ратове, експлозије фабрика и природне катастрофе). Друга значајна карактеристика ове дефиниције је у томе што нашу пажњу усмерава на процес доношења одлука, односно посматра кризе као прилику за доношење критичних одлука.[16]

За потребе овог истраживања под појмом *кризе* подразумева се сложени концепт који укључује низ претњи нормалном функционисању инфраструктура од круцијалног националног интереса. Кризе обухватају елементарне непогоде, катастрофе које захтевају ванредне активности и координацију различитих сектора како би се елиминисале или спречиле штетне последице. Дакле, неизвесност, претња виталним вредностима система и ограничено време за акцију представљају основне карактеристике кризе.

Код кризних ситуација најважније је разумети које су то активности у оквиру кризног менаџмента и који људи су задужени за те активности. Постоје бројне дефиниције кризног менаџмента. Издвојићемо једну у којој Ћиљоти и Роналд кризни менаџмент одређују као способност организације да поступа брзо, ефикасно и ефективно у могућим операцијама које имају за циљ смањивање претњи људском здрављу и безбедности, умањење штете на јавној или корпорацијској имовини и смањивање негативног утицаја на наставак нормалног пословања или неких други

[15] Ibid, 15-16
[16] Ibid, 16

операција.[17] Сличне концепте кризног менаџмента предложили су и многи други аутори, изједначавајући га са поступањем у непредвиђеним ситуацијама. Овакви приступи могу бити неефективни, јер не узимају у обзир многе друге значајне аспекте интегрисаног плана за управљање кризама. Тако да је исправније кризни менаџмент одредити као скуп функција или процеса који имају за циљ да "идентификују, изуче и предвиде могуће кризне ситуације и успоставе посебне начине који ће организацији омогућити да спречи кризу или да се са њом избори и да је превазиђе уз минимизирање њених последица и што бржи повратак у нормално стање".[18] У овом истраживању *кризни менаџмент* ће се посматрати као општи процес планирања и имплементације одређених активности ради превенције или успостављања нормалног функционисања критичних инфраструктура угрожених различитим врстама криза.

Појам *критичне инфраструктуре* односи се на имовину која укључује физичке и компјутерске системе који су од есенцијалног значаја за обезбеђивање економске и политичке стабилности земље.[19] Оне заправо представљају оквир међузависних мрежа и система који обухватају одређене индустрије, институције (укључујући људе и процедуре) и капацитете за дистрибуцију који пружају поуздан проток производа и услуга који су неопходни за одбрамбену и економску сигурност земље, неометано функционисање власти на свим нивоима, и друштва у целини. Критичне инфраструктуре обухватају, али нису искључиво ограничене на, енергетске системе, телекомуникације, саобраћај, воду, храну, банкарске системе и финансије, цивилну администрацију, укључујући и владин и приватни сектор.[20] Ниједна подела критичних инфраструктура није апсолутна и углавном је заснована на проценама стручњака и/или доносиоца политичких одлука. У овом истраживању, због специфичне ситуације у којој се налазе земље у транзицији (демокра-тизација друштва, превазилажење ауторитарног наслеђа, дотрајалост инфраструктура, технолошка заосталост итд), нагласак ће бити стављен на следеће инфраструктуре: енергетске системе, телекомуникације, саобраћај, воду и храну.

Следећи појам који се тиче критичних инфраструктура је њихова заштита. Појам *заштита критичних инфраструктура* (ЗКИ) је први пут употребио председник Клинтон 1996. године, након терористичког акта на Федералну зграду Алфреда П.

[17] Ibid, 74-75
[18] Ibid, 75
[19] Radvanovsky, R., McDougall, A., (2010), *Critical Infrastructure, Homeland Security and Emergency Preparedness,* Second edition, CRC Press, Taylor & Francis Group, New York, p. 3
[20] Ibid

Мараха у Оклахоми 1995. године (Извршна наредба, јул 1996). Овом наредбом истакнуте су одређене националне инфраструктуре, које су од изузетног значаја за САД, и чије би онеспособљавање или уништење имало велики утицај на одбрану, економску сигурност и благостање грађана.

У САД појам критичне инфраструктуре односи се на системе и средства, било физичка или виртуелна, од виталног значаја за националну безбедност земље, њиховим онеспособљавањем или уништењем угрозио би се ниво достигнуте безбедности, економска сигурност земље, јавно здравље или неки други значајан сегмент.[21] На основу ове дефиниције, идентификовано је 17 критичних инфраструктура и кључних ресурса, и одређене улоге и одговорности за заштиту ових сектора (*Homeland Security Presidential Directive 7 (HSPD-7), December 2003*).[22] Одељење за националну безбедност, у марту 2008. године, идентификовало је још један критичан сектор (сектор за производњу критичних производа). Уз могућност даље трансформације листе критичних сектора, следећи сектори су тренутно наведени као кључни за ефикасну заштиту критичних инфраструктура: информационе технологије; телекомуникације; хемијска постројења; пословна постројења; бране; комерцијални нуклеарни реактори, материјали и отпад; владина постројења; транспорт; хитне службе; поштанске и доставне услуге; пољопривреда и храна; јавно здравље и здравство; пијаћа вода и системи за пречишћавање обичних вода; енергија, укључујући производњу, прераду, складиштење и дистрибуцију нафте и гаса, електро-привреду; банкарство и финансије; национални споменици и знаменитости; одбрамбена индустријска база; производња критичних производа.[23]

Иначе, заштита критичних инфраструктура се односи на активности које се тичу заштите инфраструктура од круцијалног значаја. Ту спадају људи, физичка имовина и информационо-комуникациони системи који су неопходни за националну и наднационалну безбедност, економску стабилност и јавни и правни поредак и безбедност. Методе и средства заштите критичних инфраструктура одвраћају или ублажавају нападе на критичне инфраструктуре од стране људи (терористи, криминалци, хакери итд), природних катастрофа (земљотреси, олујни ветрови, поплаве итд), пожара и експлозија у нуклеарним или хемијским комплексима. У суштини,

[21] Brunner, E.M. and M. Suter, (2009), *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich, p. 433
[22] Ibid
[23] Ibid, p. 434-435

заштита критичних инфраструктура подразумева заштиту имовине од непроцењиве друштвене вредности.[24]

Заштита критичних инфраструктура у земљама у транзицији, због дубоке трансформације у свим областима, захтева израду специфичне поделе критичних инфраструктура и развијање посебних стратегија за превенцију криза. Главни проблеми који утичу на ефикасну заштиту критичних инфраструктура су: лоша комуникација државних органа са власницима одређених инфраструктура (већина значајних инфра-структура су у приватном власништву), дотрајалост инфраструктура и технолошка заосталост.

Под *земљама у транзицији* подразумевају се земље у којима је до последње деценије 20. века постојао социјалистички друштвено-политички систем са планском привредом и једнопартијским системом владавине, уз доминантан утицај комунистичке идеологије и широко распрострањену праксу кршења људских права и слобода. Ове државе са симболичким рушењем Берлинског зида 1989. године почињу да напуштају социјалистички систем и изграђују тржишну привреду и демократски плуралистички политички поредак.

Предмет истраживања, са временског аспекта, тежишно обухвата период од друге половине деведесетих година 20. века до 2010. године. За почетак расправе о заштити критичних инфраструктура узима се 1996. година, када је председник САД Клинтон, услед последица терористичког напада у Оклахоми 1995. године, први пут употребио овај појам.

Просторно предмет истраживања, поред Републике Србије и још неких земаља у транзицији (чија се искуства могу искористити за израду ефикасних модела превенције криза и заштите критичних инфраструктура у Србији), обухвата и неке од развијених земаља света које поседују развијене моделе кризног менаџмента и политике заштите критичних инфраструктура, који се могу прилагодити специфичним условима транзиције и применити за израду националне стратегије заштите критичних инфраструктура у Републици Србији.

Предмет истраживања је превасходно лоциран у пољу интересовања безбедносних наука, али нам то не даје за право да унапред судимо да је одређење научног истраживања монодисциплинарно. Напротив, будући да ово истраживање захвата и области многих других наука и научних дисциплина попут политике,

[24] Radvanovsky, R., McDougall, A., (2010), *Critical Infrastructure, Homeland Security and Emergency Preparedness,* Second edition, CRC Press, Taylor & Francis Group, New York, p. 4

менаџмента, социологије, информационих, војних, правних, криминалистичких и криминолошких наука и других, предмет истраживања је мултидисциплинарног карактера.

1.3. Циљеви истраживања

С обзиром на то да је у домаћој научној литератури феномен међузависности кризног менаџмента и заштите критичних инфраструктура недовољно обрађиван, *научни циљ* овог истраживања биће дескрипција, анализа и сагледавање резултата, домета, ефикасности и примене концепта кризног менаџмента у функцији заштите критичних инфраструктура у земљама у транзицији.

Спроведена анализа би, такође, требало да допринесе разјашњењу појмовног и терминолошког корпуса ове специфичне области.

На *практичном нивоу*, резултати овог истраживања могли би допринети развијању стратегија превенције, сузбијања и управљања кризама како на националном тако и на наднационалном нивоу. На основу добијених резултата истраживања извешће се и одређени закључци и предлози у вези са квалитетом, ефикасношћу и могућим недостацима заштите инфраструктура од виталног националног интереса Републике Србије.

Концепт заштите критичних инфраструктура са аспекта националне безбедности Републике Србије, пак, захтева усаглашавање националног законодавства са постојећим међународним стандардима. С обзиром на кораке које Србија чини како би постала чланица Европске уније и на убрзану информатизацију друштва, процес стандардизације у овој области намеће се као један од приоритетних задатака Републике Србије у блиској будућности.

1.4. Хипотетички оквир истраживања

С обзиром на претежно квалитативни и експлоративни карактер ово истраживање, је засновано на генералном, широком и неспецифичном хипотетичком оквиру који обухвата испитивање сета следећих претпостављених односа:

1. Критичне инфраструктуре у земљама у транзицији изложене су специфичним изворима и облицима угрожавања, у политичком, економском, културно-перцептуалном и организационом погледу, при чему се у већини случајева занемарује значај њихове заштите. Сходно томе, у већини транзиционих

земаља системи заштите критичних инфраструктура су недовољно ефикасни у односу на системе у развијеним земљама.

2. И поред специфичности које су карактеристичне за сваку транзициону земљу оне су у већој или мањој мери суочене са сличним проблемима: нестабилна регулативно-институционална сфера, ограниченост ресурса, дотрајалост инфра-структура, остаци социјализма, промена медијске културе, нарушени међуна-родни односи.
3. Поједине земље су током транзиционог периода успешно унапредиле системе управљања кризама и политике заштите критичних инфраструктура, и израдиле сопствене моделе на искуствима развијених земаља, уважавајући властите специфичности извора и облика угрожавања критичних инфраструктура који могу изазвати кризе великих размера.
4. Република Србија није трансформисала и јасно одредила систем кризног менаџмента и стратегију заштите критичних инфраструктура, тако да теорија и пракса у овим областима заостају у односу на већину земаља у транзицији.

1.5. Методе и начин истраживања

Истраживање феномена кризног менаџмента у функцији заштите критичних инфраструктура у земљама у транзицији нужно намеће мултиметодски приступ и захтева комплементарну анализу доступних и новостворених извора података. Реч је о доминантно квалитативном истраживачком приступу, а недовољна теоријска изграђеност на пољу заштите критичних инфраструктура у земљама у транзицији је условила претежно експлораторну природу успостављених истраживачких захтева.

Начин истраживања и избор метода одређени су дефинисаним проблемом истражи-вања, теоријским и операционализованим предметом истраживања, претпостављеном хипотетичком основом и комплексношћу предмета истраживања.

Сагледавање стања угрожености и заштите критичних инфраструктура у земљама у транзицији, као и могућности унапређења кризног менаџмента у функцији заштите критичних инфраструктура у овим земљама захтева употребу одговарајућих научних метода којима ће бити обухваћени сви релевантни извори сазнања. Дефинисани предмет истраживања сложено је поље за проучавање, и за његову ваљану и обухватну анализу неопходно је користити различите методе и теоријска знања из више научних дисциплина.

Због комплексности проучаваног феномена, односно указивања на потенцијалну међузависност концепата кризног менаџмента и заштите критичних инфраструктура, у раду су анализирани подаци из различитих извора. Базична искуствена евиденција је креирана из постојећих извора података:

- научних и стручних радова који се, посредно или непосредно, баве феноменом кризног менаџмента и заштите критичних инфраструктура у земљама у транзицији;
- научних и стручних истраживачких пројеката спроведених у транзиционим земљама из области управљања кризама и заштите критичних инфраструктура;
- позитивноправних прописа (националних, регионалних и међународних), где је посебан нагласак стављен на анализу правног оквира Републике Србије на пољу заштите критичних инфраструктура;
- институционалних извора (статистичких извештаја, докумената из архива државних институција, евиденције невладиних организација, извештаја осталих релевантних институција);
- евиденције државних и међународних тела задужених за праћење тероризма и криминалитета у земљама у транзицији, јер ови извори и облици угрожавања безбедности могу изазвати кризе великих размера и угрозити критичне инфраструктуре, и
- међународних докумената, конвенција, протокола, међународних уговора и других аката, који су директно или индиректно везани за проблем заштите инфраструктура у земљама у транзицији.

Током истраживања ће, пре свега путем метода анализе садржаја различитих облика комуникација, бити стварана и искуствена грађа релевантна за извођење закључака о испитиваним појавама (процена стања угрожености критичних инфраструктура у земљама у транзицији, могућности унапређења њихове заштите, преглед стања на пољу кризног менаџмента у земљама у транзицији, међузависност ефикасног управљања кризама и заштите критичних инфраструктура).

У циљу постизања што већег степена поузданости и обухватности, испитивање наведених појава ће обухватити како анализу различитих извора података, тако и комплементарно коришћење различитих истраживачких метода:

1. преглед научне и стручне литературе;

2. анализа правних докумената;
3. метод секундарне анализе;
4. метод анализе садржаја;
5. принцип триангулације.

Преглед научне и стручне литературе биће главна метода која ће се користити за теоријско заснивање проблема истраживања. За потребе конципирања овог истраживања углавном ће бити коришћена и анализирана иностранa литература и истраживачка искуства из области наука безбедности, менаџмента, социологије, информационих, војних, правних, криминалистичких и криминолошких наука.

Анализа правних докумената ће у овом истраживању обухватити примену правно-догматског и нормативног метода. Применом ових метода анализираћемо нормативно правне оквире Републике Србије, појединих земаља у транзицији, затим нормативу технолошки развијених земаља, и упоредно, међународне позитивно правне прописе на пољу заштите критичних инфраструктура

Многи документи, створени у различите сврхе послужиће нам као извори сазнања о посматраној појави. Подаци из статистичких извештаја и аналитичких база података биће препознати коришћењем *методе секундарне анализе* са циљем квалитативног описа суштинских карактеристика концепта кризног менаџмента у земљама у транзицији, политике заштите критичних инфраструктура у овим земљама и улоге кризног менаџмента у ефикасној заштити виталних инфраструктурних објеката у транзиционим друштвима.

Методом анализе садржаја прикупиће се грађа неопходна за научну дескрипцију улоге кризног менаџмента у заштити критичних инфраструктура у одабраним земљама у транзицији. Ово је заправо једини начин за сагледавање стања у области управљања кризама и заштите критичних инфраструктура у овим земљама, с обзиром на то да би организовање сопственог емпиријског истраживања било повезано са низом економских, социјалних, политичких и других препрека. Ради тога неопходно је остварити увид у постојећу литературу, изворе статистичких података и остале расположиве информације.

Основни истраживачки принцип којим ће се руководити ово истраживање биће принцип комплементарности, односно *триангулације*. У циљу свеобухватног сагледавања феномена кризног менаџмента и заштите критичних инфраструктура у земљама у транзицији биће примењене различите методе истраживања, а подаци добијени коришћењем сваке од њих омогућиће анализу различитих аспеката везаних за проблем

унапређења заштите критичних инфраструктура посредством кризног менаџмента у овим земљама.

1.6. Научна и друштвена оправданост истраживања

Научна оправданост истраживања институционалних решења и стварног стања на пољу заштите критичних инфраструктура у земљама у транзицији и улоге кризног менаџмента у њиховој заштити огледа се, пре свега, у чињеници да овај проблем није до сада детаљније истраживан у домаћој литератури. Његовим теоријским постављањем, наглашавањем значаја и могућих решења, учинио би се значајан помак у промишљању и заснивању почетног корпуса сопственог теоријског сазнања о кризном менаџменту и заштити критичних инфраструктура. Дескрипција и објашњење класификације критичних инфраструктура, која до сада није постојала у домаћој литератури, такође указују на научну оправданост овог истраживања.

Чињеница да Република Србија у великој мери заостаје у односу на успешније земље у транзицији, при чему је свакодневно суочена са низом најразличитијих криза, праћена је непостојањем одговарајућег институционалног оквира и компаративног увида у најбољу праксу. Из наведених разлога, успостављање институционалног и нормативног оквира на пољима заштите критичних инфраструктура и управљања кризама је од круцијалног значаја за функционисање локалних заједница, државе и нормалан живот друштва. Позитивна (као и негативна) искуства појединих земаља у транзицији, уз неопходно прилагођавање условима и специфичностима Републике Србије, значајно би утицало на убрзање закаснелих транзиционих процеса, што је и више него довољан разлог за друштвену оправданост овог истраживања.

Реално је претпоставити да ће резултат овог истраживања представљати подстрек истраживачима да свестраније истражују корелативност између ефикасног управљања кризама и ризицима и заштите критичних инфраструктура, чиме ће предмет истраживања бити још свеобухватније сагледан у теорији и пракси.

2. ТЕОРИЈСКЕ ОСНОВЕ КРИЗНОГ МЕНАЏМЕНТА И НАУКЕ О БЕЗБЕДНОСТИ

2.1. Концептуални оквир и циљеви кризног менаџмента

2.1.1. Појмовно одређење кризног менаџмента

Кризни менаџмент као научно-теоријска дисциплина и рационално осмишљен концепт прагматичног деловања ступа на историјску сцену у другој половини 20. века. Порекло овог термина налази се у политичкој сфери. Заправо, сматра се да је амерички председник Џ. Ф. Кенеди први употребио термин кризни менаџмент за време Кубанске ракетне кризе 1962. године, када је хладноратовска напетост дошла до кулминације инсталирањем совјетских ракета са нуклеарним главама на Куби. Таквом формулацијом Кенеди је описао управљање једном озбиљном, ванредном ситуацијом која је могла довести до избијања Трећег светског рата.[25]

Потребно је истаћи да су делатности кризног менаџмента старије од самог термина. Тако је на пример Влада САД испуњавањем својих формалних одговорности, услед активности на пољу сузбијања растуће претње од пожара у великим градовима у 19. веку, заправо примењивала концепт управљања у ванредним ситуацијама. Нешто касније, кризни менаџмент се појављује и у облику организације, односно долази до формирања посебних органа, тела и агенција које се баве управљањем кризама.[26] Међу ауторима који се баве овом тематиком углавном постоји сагласност да модерна фаза у развоју кризног менаџмента почиње од 1982. године. Ову фазу је покренуло решавање кризе изазване тровањем пацијената леком *Tylenol* (најпознатији аналгетик у САД) фирме *Johnson&Johnson*.[27] Догађај из 1982. године направио је прекретницу и поставио стандарде у овој области.[28]

Сходно проширивању сазнања, данас се кризни менаџмент може применити у скоро свакој области људске делатности, али се обично најчешће повезује са међународним односима, политичким наукама и пословном сфером. Велике компаније, као и бројне непрофитне организације, препознале су значај и улогу кризног менаџмента у функционисању једног система. То је навело велики број установа, попут

[25] Kešetović, Ž., Toth, I., (2012), *Problemi kriznog menadžmenta*, Veleučilište Velika Gorica, Velika Gorica, str. 53
[26] Кешетовић, Ж., (2008), *Кризни менаџмент*, Факултет безбедности, Службени гласник, Београд, стр. 74
[27] Услед последица тровања леком умрло је седморо људи.
[28] Mitroff, I., *Managing Crises before they happen: What every executive and manager should know about crisis management*, AMACOM, New York, 2000. From: Kešetović, Ž., Toth, I., (2012), *Problemi kriznog menadžmenta*, Veleučilište Velika Gorica, Velika Gorica, str. 53

научно-образовних институција, да сачине приручнике и упутства за понашање у кризним ситуацијама (пожари, непожељни посетиоци, најаве о подметнутим бомбама, насиље и слично). Једном речју, усвојена је свест да неспремност и неадекватно реаговање у кризним ситуацијама могу довести до озбиљних последица.[29]

С обзиром на то да кризни менаџмент представља пре врсту апликативног (примењеног) менаџмента, неголи егзактну науку, постоје бројне дефиниције које покушавају да објасне суштину овог концепта. Све оне настоје да укажу да је реч о концепту који можемо посматрати као неку врсту праксе руковођену теоријом. Тако, на пример, Ћиљоти и Роналд кризни менаџмент одређују као способност организације да поступа брзо, ефикасно и ефективно у могућим операцијама које имају за циљ смањивање претњи људском здрављу и безбедности, умањење штете на јавној или корпорацијској имовини и смањење негативног утицаја на наставак нормалног пословања или других операција.[30]

Кризни менаџмент се често дефинише парцијално, у односу на област или врсту потенцијалних кризних ситуација за које је формулисан. Међу општим дефиницијама кризног менаџмента могу се издвојити Пирсонова и Клерова: "Кризни менаџмент је систематски напор да се избегне организациона криза или да се управља таквим кризним догађајима пре него што се догоде".[31]

Према Ж. Кешетовићу кризни менаџмент се може одредити и као скуп функција или процеса који имају циљ да идентификују, изуче и предвиде могуће кризне ситуације и успоставе посебне начине који ће организацији омогућити да спречи кризу или да се с њом избори и да је превазиђе уз минимизирање њених последица и што бржи повратак у првобитно стање. Кризни менаџмент објашњава као стенографски назив за све врсте активности усмерене на поступање са системом који се налази у стању поремећаја: превенцију, припрему, ублажавање и опоравак. Заправо, реч је о обликовању поступака, договора и одлука које утичу на ток кризе. Ж. Кешетовић указује да кризни менаџмент обухвата читав корпус активности, попут организовања, припрема, разних мера и распоређивања ресурса за савладавање кризе. Наглашава да се

[29] Кешетовић, Ж., (2008), *Кризни менаџмент*, Факултет безбедности, Службени гласник, Београд, стр. 74
[30] Милашиновић, С., Кешетовић, Ж., (2009), *Кризни менаџмент*, Криминалистичко-полицијска академија, Београд, стр. 223
[31] Pearson, C., Clair, J., (1998), "Reframing Crisis Management", *Academy of Management Review*. Vol. 23, No 1, pp. 59-76

он обично одвија у условима организационог хаоса, под притиском бројних медија у стресним ситуацијама и недостатку прецизних информација.[32]

У области јавне комуникације Вилијамс и Оланиран кризни менаџмент дефинишу као "коришћење односа са јавношћу да се умањи штета организацији у ванредним околностима која може да проузрокује непоправљиво оштећење".[33] Значајност правовремене реакције за минимизирање штете проузроковане кризном ситуацијом најбоље илуструје пример лошег реаговања авио-компаније TWA приликом рушења њиховог авиона (авион компаније TWA на лету 800 из Њујорка за Париз, срушио се у Атлантски океан, при чему је животе изгубило 230 људи).[34]

С безбедносног аспекта концепт кризног менаџмента има кључну улогу у спречавању и сузбијању криза, што је навело велики број међувладиних организација да израде сопствене концепте и дефиниције овог појма. Тако је, на пример, Европска унија у области своје безбедносне стратегије дефинисала питања цивилног кризног менаџмента као помоћ у обнови цивилне владе након кризе.[35] У једној независној студији Касперсен и Сендинг су анализирали активности Уједињених нација у решавању криза широм света развијајући при томе посебно област цивилног кризног менаџмента.[36]

Обавештајна заједница Сједињених Америчких Држава пажњу усмерава превасходно на безбедносни концепт и дефинише кризни менаџмент као: "способност једне организације да се припреми за опажене катастрофичне догађаје – као што је тероризам – и да употреби одговарајуће снаге и специјализовану оспособљеност у циљу минимизирања штете која може бити нанета националним интересима САД. На унутрашњем плану, кризни менаџмент употребљава сваки ресурс са којим располаже федерална, државна или локална влада".[37]

---

[32] Кешетовић, Ж., (2008), *Кризни менаџмент*, Факултет безбедности, Службени гласник, Београд, стр. 75

[33] Williams, D. E.& Olaniran, B. A., (1998), *Expanding the Crisis Planning Function: Introducing Elements of Risk Communication to Crisis Communication Practice*, Public Relation Review, 24 (3), pp. 387-400

[34] Кључне грешке које су том приликом начињене су: неодговарање на позиве медија што је аутоматски изазвало панику у јавности, авио компанији је било потребно 16 сати да потврди листу путника и почне да обавештава рођаке страдалих, председник авио компаније TWA је дао изјаву за штампу и појавио се у јавности тек дан након несреће.
Видети на интернет страници: http://sr.scribd.com/doc/99579355/6025-Odnosi-s-Javnoscu-u-Kriznim-Situacijama

[35] Опширније погледати у: EU: *A Secure Europe in a Better World – The European Security Strategy*, 12. December 2003.

[36] Опширније погледати у: Kaspersen, A. T., and Sending, O. J., (2005), *The United nations and Civilian Crisis Management*, Norwegian Institute of international Affairs, May.

[37] *Intelligence Warning Terminology*, Joint Military Intelligence College, Washington DC, October 2001. p. 11

Важно је истаћи да кризни менаџмент не представља јединствену професију, већ је реч о теоријском концепту који у научно-истраживачком смислу обухвата групу догађаја са заједничким законитостима, али и разликама, што значи да експерти из једне области не могу бити подједнако успешни у управљању кризама из неке друге области за коју нису довољно специјализовани.[38] То свакако не представља баријеру за међусобну размену искустава. Дакле, израз кризни менаџмент није синоним за заштиту и спасавање, као ни за обезбеђење од природних и других несрећа, већ је то један појам који обухвата много ширу друштвену реалност која постоји као теоријски концепт у науци и истраживању.[39]

Научни и практични значај кризног менаџмента и одлучивања у кризним ситуацијама је неоспоран. Сам концепт је данас предмет изучавања на бројним факултетима и научним институтима у великом броју земаља широм света. У оквиру међународне сарадње, организују се бројне конференције, округли столови и симпозијуми посвећени овој теми. Такође, у оквиру међународне сарадње постоје и мреже научно-истраживачких организација које се баве изучавањем криза и концептом кризног менаџмента.[40]

2.1.2. Модели процеса и основни задаци кризног менаџмента

Већину криза можемо посматрати као догађаје иницијаторе одређених процеса који угрожавају и нарушавају стабилност и одрживост једног система. Оне обично имају порекло у прошлости и идентификовање њихових првобитних извора може бити од велике помоћи у разумевању и управљању одређеном кризом. Кризе се појављују у различитим облицима и моделима, у виду пораза у међународном оружаном сукобу, револуције, изненадног слома нестабилних демократских режима, економске пропасти, имплозије, губитка стране подршке који може довести до пада зависних режима, температурних промена.[41]

Управљање кризама подразумева ангажовање великог броја учесника који на различите начине учествују у њиховом превазилажењу. Ови учесници морају бити

[38] На пример, различите професије баве се монетарним кризама, војним тензијама, тероризмом, природним несрећама итд.
[39] Kešetović, Ž., Toth, I., (2012), *Problemi kriznog menadžmenta*, Veleučilište Velika Gorica, Velika Gorica, str. 55
[40] Милановић, Г., (2010), *Кризни менаџмент у земљама у транзицији*, Докторска дисертација, Факултет безбедности, Београд, стр. 68
[41] Dogan, M., Higley, J., (1996), *Crises, elite change, and regime change*, International Conference on Regime Change and Elite Change in El Paular, Spain, May 30–June 1, p. 9. From: Farazmand, A., (2001), *Handbook of Crisis and Emergency Management*, Marcel Dekker, Inc, New York, p. 4

оспособљени да међусобно комуницирају и сарађују, као и да контролишу ток кризе. Наведене активности воде ка суочавању са целим низом комплексних проблема који могу да искрсну из различитих извора. У циљу обезбеђивања успешног одговора на све ове изазове, неопходно је да учесници у процесу кризног менаџмента имају усаглашен појмовно категоријални апарат и модел, као и прописане процедуре на основу којих се ангажују. Оваква архитектура управљања кризом заснована је на моделима командовања и контроле, као и на анализи потенцијалних кризних ситуација.[42]

Ефикасан кризни менаџмент подразумева исправно тумачење и развијену свест о томе на који начин се може управљати кризом пре него што до ње дође. С тим у вези, Гонзалес-Хереро и Прат су креирали четворостепени модел процеса кризног менаџмента. Њихов модел процеса управљања кризама укључује:

- *issues* менаџмент;
- планирање - превенцију;
- кризу;
- пост-кризну фазу.[43]

Кековић З. и Кешетовић Ж. наводе модел немачког аутора Д. Глазера који препознаје следеће фазе кризног менаџмента:

- Мере предострожности за кризну ситуацију која укључује припрему за потенцијалну кризу;
- Превентивни кризни менаџмент, који треба да антиципира и предвиди будућу кризу, активни кризни менаџмент, који омогућава брзу идентификацију догађаја, и реактивни кризни менаџмент, који се тиче акутне анализе;
- Антиципативна форма кризног менаџмента треба да ојача способности за реакцију кроз формације прогнозе или сценарија и имплементацију алтернативних планова. Превентивни кризни менаџмент обухвата планирање, имплементацију и контролу превентивне стратегије и мера за помоћ система раног упозорења. Репулзивни кризни менаџмент усмерен је на одржање бизниса у ситуацији настале кризе. Ликвидациона форма кризног

[42] Милановић, Г., (2010), *Кризни менаџмент у земљама у транзицији*, Докторска дисертација, Факултет безбедности, Београд, стр. 68
[43] Gonzalez-Herrero, A., & Pratt, C. B., (1995), *How to manage a crisis before or whenever - it hits*, Public Relations Quarterly, 40(1), pp. 25-29

менаџмента обухвата планирање ликвидације компаније уколико нема изгледа за њено прежив-љавање.

- Стратешки кризни менаџмент концентрисан је на заштиту фактора успеха компаније. Осигурање успеха као форма кризног менаџмента треба да омогући избегавање финансијских и других мањкова који прете факторима успеха као што су профитабилност и флуктуација. Заштита солвентности као форма кризног менаџмента има као циљ одолевање опасности од несолвентности и неоснованог неповерења према компанији.
- Управљање кризом обухвата активности избегавања и суочавања са истом. Стратешки кризни менаџмент означава активности избегавања криза. Оперативни кризни менаџмент подразумева оперативне активности у суочавању са кризом.[44]

Ова значења исти аутори синтетизују кроз две активности обухваћене кризним менаџментом: превенцију и суочавање са кризом. За разлику од суочавања, које је у основи дисконтинуирано и нелинеарно, превенција кризе представља континуирану активност. Ова стратешка активност подразумева:

- политику управљања ризиком и
- припрему оперативног кризног плана.

За разлику од њих, британски истраживачки центар *Thales Researchand Technology*, који се бави кризним менаџментом, ванредним околностима и планирањем опоравка од катастрофа описује два модела кризног менаџмента:[45]

1) први се односи на временску димензију кризе са активностима дефинисаним у свакој фази, а
2) други је заснован на технолошкој оспособљености потребној за успешно суочавање са кризом.

А. Фаразманд истиче да се главни задаци кризног менаџмента своде на тачну и правовремену дијагностификацију критичности проблема и динамике догађаја који следе. То захтева знања, вештине, храбро руководство и мере предострожности. Успешан кризни менаџмент такође захтева мотивисаност, осећај за хитно реаговање, посвећеност и креативни начин размишљања који укључује дугорочну стратешку визију. Према његовом мишљењу, највеће препреке у управљању кризом представљају

[44] Кековић, З., Кешетовић, Ж., (2006), *Кризни менаџмент 1, Превенција кризе*, Факултет безбедности, Београд, стр. 449-450

[45] Опширније погледати у: Craddock, R. J., (2006), *Crisis Management Models and Timelines*, Thales Research and Technology (UK), White Paper, 22.06

установљене организацио-не норме, култура једне организације, правила и процедуре. Администратори и бирократе теже да заштите сопствене интересе скривајући се иза организационих и правних норми. Заправо, то представља највећу институционалну препреку у управљању кризама.

А. Фаразманд апострофира да успешно управљање кризама захтева следеће:[46]

- осећај да је реч о ситуацији која захтева хитну реакцију;
- креативно и стратешко размишљање у циљу решавања кризе;
- предузимање смелих активности и храбро наступање;
- иступање из самозаштитне организационе културе преузимањем ризика и спровођењем акција које могу створити оптималне могућности за проналажење решења где нико неће бити на губитку, и
- одржавање континуираног присуства у сваком моменту управљања кризом.[47]

Кризни менаџмент захтева стратешко размишљање у кризним ситуацијама. Кризе такође стварају прилике, а оне морају бити истражене кроз мобилизацију свих средстава и снага које нам стоје на располагању. Осећај хитности позива на непосредну пажњу, акцију и реакцију. Примарна функција сваке владе јесте заштита живота и власништва грађана. Кризе и ванредне ситуације, у ствари, тестирају способност влада. Кроз историју развоја људске цивилизације, доносиоци политичких одлука су настојали да предвиде неочекивано у циљу смањивања ризика по људски живот и њихову безбедност. А. Фаразманд истиче да "овај приступ треба капитализовати као племенит стратешки и политички избор колективне акције". Нажалост, не размишљају сви на овај начин када се нађу у некој кризној ситуацији. Историја је пуна случајева у којима опортунисти користе предности хаоса и нереда да би стекли личну добит.[48]

Из претходно наведеног можемо извући општи закључак у вези са основним задацима кризног менаџмента који се своде на идентификовање, изучавање и предвиђање могућих кризних ситуација. Такође, један од главних задатака кризног менаџмента јесте развијање посебних модела који ће организацији омогућити правовремено реаговање и превазилажење кризе у циљу минимизирања њених последица и што бржег повратка у нормално стање. Дакле, све активности усмерене на поступање са одређеном организацијом у стању поремећаја, а зарад превенције,

[46] Farazmand, A., (2001), *Handbook of Crises and Emergency Management*, Marcel Dekker, Inc, New York, p. 4
[47] Ibid
[48] Ibid, p. 5

припреме, ублажавања и опоравка, представљају основне задатке концепта кризног менаџмента.[49]

2.2. Доктрине и концепти безбедности

2.2.1. Глобална безбедност

Убрзано развијање друштвених односа на нивоу читаве планете, услед интензивирања процеса глобализације, поставило је изучавање глобалних интереса и концепта глобалне безбедности у жижу интересовања научних кругова из ове области. Замисао глобалне безбедности превазилази концептуална и стварна ограничења међународне безбедности, јер представља феномен који обухвата један шири спектар друштвених збивања.

Концепт глобалне безбедности третира истоветно економску, политичку, културну и материјалну димензију. Једна од главних карактеристика овог концепта јесте подједнако уважавање невладиних и државних актера, односно идентификовање невладиног сектора као веома значајног у укупним светским пословима.[50]

Поменути концепт даје посебну улогу међувладиним организацијама, идентификујући их центром заједничког деловања у циљу постизања мира и безбедности у свету. Међувладине организације се посматрају као нека врста глобалног центра за усмеравање свих активности и подстицање сарадње и развијање поверења међу државама.

За разлику од концепта националног интереса, замисао глобалних интереса ставља нагласак на потребе човечанства као целине, односно пропагира усклађивање супротстављених националних, међународних и поднационалних интереса. Овај концепт је глобалан, јер просторно обухвата интересе целокупног човечанства и односи се на питања од општег значаја.[51]

---

[49] Каровић, С., Комазец, Н., Ђурић, Н., *Подручје одбрамбене делатности као предмет истраживања кризног менаџмента*, стр. 289
http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2011-leto/25.%20Podrucje%20odbrambene%20delatnosti%20kao%20predmet%20istrazivanja%20kriznog%20menadzmenta;%20Samed%20Karovic,%20Nenad%20Komazec%20i%20Nenad%20Djuric.pdf 11.11. 2012

[50] Симић, Д., (2002), *Наука о безбедности – савремени приступи безбедности,* "Службени лист" СРЈ, Београд, стр. 49

[51] Потребно је нагласити да концепт глобалних интереса и глобалне безбедности не потискује замисао националних интереса и националне безбедности, већ је реч о измењеним околностима глобализоване светске политике, где глобално у неким случајевима има примат у односу на национално. Долази до преструктурисања светске политике услед покретања бројних интегративних трендова. Државе се приближавају у погледу комуникације, идеја и трговине. С друге стране, дезинтегративне тенденције потресају свет (ширење конвенцијалног и неконвенцијалног наоружања, глобално погоршање услова

Један од првих редоследа глобалних интереса представио је С. Браун. На првом месту његове листе налази се глобални интерес опстанка људске врсте, као интерес који представља предуслов остварења свих других интереса и вредности. На друго место поставио је интерес смањивања убијања и елиминисања других крајње бруталних начина поступања према људима. Као главни механизам за редуковање наведених претњи наводи потребу демократизације недемократских режима. Наредни глобални интерес је постојање услова за здрав живот свих људи, указујући на потребу предузимања здружених активности на глобалном плану. Затим следи заштита грађанских права, као предуслов демократског уређења. На петом месту Браунове листе интереса налази се поштовање права етничких заједница на различитост. Следећи представљени интерес је интерес заштите животне средине, где се скреће посебна пажња на неодговоран однос према природној средини. Последњи интерес, али не и најмање важан, јесте ширење урачунљивог понашања, интерес који претходи и у великој мери условљава поштовање свих раније поменутих глобалних интереса.[52]

Главна дирекција за питања глобалне безбедности у оквиру Лоренс Ливмор националне лабараторије[53] наводи кључне области које се морају имати у виду приликом суочавања са глобалним безбедносним изазовима:[54]

- био-безбедност,
- противтерористичко деловање,
- одбрана,
- енергија,
- обавештајни рад и
- непролиферација.

Бројни догађаји и дешавања у свету током протеклих година издигли су концепт глобалне безбедности на највиши ниво и указали на неопходност заједничког деловања држава у циљу супротстављања савременим безбедносним изазовима,

---

животне средине, етнички сукоби и слично). Супротстављене силе интеграције и дезинтеграције указују на трансформацију светске политике, прелазак са националног на глобални ниво. Према: Кегли, Ч., Виткоф, Ј., (2004), *Светска политика – тренд и трансформација,* Факултет политичких наука, Београд, стр. 45-46

[52] Симић, Д., (2002), *Наука о безбедности – савремени приступи безбедности,* "Службени лист" СРЈ, Београд, стр. 50-54

[53] Дирекција се бави питањима глобалне безбедности, настојећи да применом мултидисциплинарног научног приступа и најновијих технолошких достигнућа предвиди, иновира и пронађе одговарајућа решења за глобалне безбедносне изазове

[54] Global security, https://www-gs.llnl.gov/ 12.11.2012

ризицима и претњама.[55] Суштински измењена природа претњи безбедности и благостању људи условила је развој и примену нових процедура и механизама како би се достигао жељени ниво безбедности.[56] Такође, идентификована је повезаност концепта националне и глобалне безбедности, односно путем јачања националних система безбедности и сарадње на међународном плану, аутоматски ће се повећати и степен глобалне безбедности.

Дакле, реч је о једном свеобухватном концепту који обухвата безбедносну динамику која се одвија на нивоу читаве планете и представља највиши ниво анализе безбедносних појава. Из те анализе не могу се увек јасно сагледати безбедносни изазови, ризици и претње на нивоу појединца, друштва или државе, али се зато могу уочити макропојаве значајне за свет у целини. Каква ће пак безбедносна динамика бити идентификована на глобалном нивоу анализе у великој мери зависи од одабира аналитичког приступа. Уколико се определимо за државоцентрични приступ, пажња ће бити усмерена на безбедносну динамику која се одвија унутар међудржавног система. С друге стране, ако се определимо за друштвеноцентрични приступ, фокус ће бити усмерен на безбедносну динамику која је резултат процеса савремених глобализованих односа. Потребно је нагласити и то да концепт међународног система пружа добар оквир за статичну анализу глобалне безбедности, док концепт глобализације ствара оквир за динамичку анализу глобалне безбедности.[57]

2.2.2. Регионална безбедност

Реч регион, према М. Фукоу, представља пре свега фискални, административни и војни појам.[58] У најширем смислу те речи, регион представља географски појам који означава територију средње величине. Поред наведеног, постоје и бројни други критеријуми на основу којих је могуће дефинисати регионе. На пример, унутар науке о међународним односима могуће је разликовати три различита приступа у поимању региона. Први приступ је усмерен изнутра-ка-споља и усредсређен је на унутрашња обележја попут климе, културе, језика, економске интеграције и међузависнсти. Други приступ усмерен је споља-ка-унутра и дефинише регион на основу спољашњих

[55] Глобални тероризам; глобално загревање; демографска експлозија; катастрофе које могу проузроковати кризе глобалних размера
[56] Стајић, Љ., (2008), *Основи система безбедности*, Правни факултет, Нови Сад, стр. 157
[57] Ејдус, Ф., (2012), *Међународна безбедност: теорије, сектори и нивои*, Службени гласник, Београдски центар за безбедносну политику, Београд, стр. 261
[58] Crampton, J., Elden, S., (2007), *Space, Knowledge and Power: Foucault and Geography*, Ashgate, Hampshire, p. 173

обележја као што су улога великих сила, интеракција са међународним системом, природне геополитичке границе и слично. Трећи приступ пажњу поклања процесима дискурзивне изградње региона, посматрајући регион као неку врсту друштвене конструкције, а не политички неутралне категорије.[59]

Већ током Хладног рата у студијама безбедности јављају се први гласови који указују на потребу усмеравања веће пажње на регионе као нивое анализе. Један од првих који је предложио да се у науку о међународним односима убаци регионални ниво анализе био је Роналд Јалем. Као главни разлог за увођење овог нивоа анализе Јалем је истакао све већу комплексност светске политике, док је Бери Базан током осамдесетих година 20. века у својој књизи "Људи, државе и страх" дао прво теоријско утемељење за свеобухватно изучавање регионалне безбедности.[60] Овај аутор је идентификовао одређене обрасце регионалне безбедности, назвавши их регионалним безбедносним комплексима.[61]

Крај Хладног рата додатно је подстакао интересовање за изучавање регионалне безбедности. Његовим завршетком створени су нови регионални сукоби који су постали предмет интересовања светске јавности. Распад Совјетског Савеза и нестанак СФРЈ иницирали су потпуно нове регионалне безбедносне динамике. Окончање идеолошког рата доводи до идентификовања етнорелигијског фактора као веома значајног, као и до вишег нивоа аутономије регионалне безбедносне динамике.[62]

Овај период карактерише и развој међувладиних организација. Долази до настанка нових организација, услед реакције на новонастало међународно политичко, економско и безбедносно окружење.[63] С друге стране, долази и до трансформације постојећих међународних организација.[64] Такође, неке хладноратовске организације

---

[59] Ејдус, Ф., (2012), *Међународна безбедност: теорије, сектори и нивои*, "Службени гласник", Београдски центар за безбедносну политику, Београд, стр. 250-251

[60] Регионалну безбедност можемо дефинисати као део међународне безбедности која се фокусира на један регион – пример регион Југоистичне Европе, чији је Србија саставни део. Према: Гаћиновић, Р., (2007), *Класификација безбедности*, Зборник радова НБП, Криминалистичко-полицијска академија, Београд, стр. 16. Интернет страница: http://www.kpa.edu.rs/data/akademija/nbp/nbp_2007_2.pdf 14.11.2012

[61] Бузан је регионалне безбедносне комплексе дефинисао као групу држава чије су примарне безбедносне бриге довољно међусобно повезане да се њихови концепти националних безбедности не могу објективно посматрати одвојено. Buzan, B., (1983), *People, States and Fear: The National Security Problem in International Relations*, Wheatsheaf, Birghton, p. 106. Према: Ејдус, Ф., (2012), *Међународна безбедност: теорије, сектори и нивои*, Службени гласник, Београдски центар за безбедносну политику, Београд, стр. 253

[62] Ibid, p. 253-254

[63] Створене су нове међународне организације: Заједница независних држава (1991), Шангајска организација за сарадњу (1995), Северноамерички споразум за слободну трговину (1994)

[64] Трансформисане су следеће организације: КЕБС у ОЕБС (1995), Европска заједница у Европску унију (1992) итд.

проширују поље свог деловања и укључују бројне државе у разне програме сарадње. Тако је, на пример, НАТО покренуо програм *Партнерство за мир* (1994), а АСЕАН свој Регионални форум (1994).[65]

Због сложеног карактера безбедносних изазова, ризика и претњи, неопходно је да државе широм света заједничким напорима сузбију негативне процесе који угрожавају њихову безбедност. У постојећим условима, међународне регионалне организације као што су ОЕБС, ЕУ и НАТО представљају кључне елементе европске и светске безбедносне архитектуре. Од способности њиховог прилагођавања новим изазовима, ризицима и претњама, као и у зависности од карактера односа које ће те асоцијације успостављати са осталим актерима савремене међународне заједнице, највише зависи безбедност евроатланског простора и света у целини.[66]

2.2.3. Национална безбедност

Концепт националне безбедности[67] заузима централно место у оквиру науке о безбедности. Иако је реч о једном политички веома моћном концепту, не постоји општа сагласност о самом значењу овог појма. Највише несугласица има у погледу набрајања вредности које се штите, односно обезбеђују. Тако на пример, Џорџ Кенан националну безбедност описује као покушај очувања физичке нетакнутости националног живота.[68] Према Антону Гризолду национална безбедност представља безбедност политичког народа и њен садржај обухвата: безбедност националне територије, заштиту живота људи и њиховог власништва, очување и одржање националне суверености и остваривање основних функција друштва. Војин Димитријевић истиче четири универзалне групе вредности у вези са националном безбедношћу. У те вредности спадају: опстанак, територијални интегритет, политичка

[65] Ibid, p. 256

[66] Гаћиновић, Р., (2007), *Класификација безбедности*, Зборник радова НБП, Криминалистичко-полицијска академија, Београд, стр. 17. Видети на: http://www.kpa.edu.rs/data/akademija/nbp/nbp_2007_2.pdf 14.11.2012

[67] Појам национална безбедност у употреби је од 1943. године, када је први пут употребио Валтер Липман у свом делу "*U.S. Foreign Policy*". После Другог светског рата овај појам је нашао широку примену у политичком речнику савремених држава. У том контексту он је употребљаван да означи унутрашњу и спољну безбедност државе, односно безбедност државе у односу на спољне и унутрашње изворе угрожавања. Ради се, дакле, о националној безбедности једне државе, која обезбеђује опстанак и нормално функционисање државе са свим елементима њене независности, територијалне целовитости и уставног поретка. Према: Јовановић, Б., (1997), *Полиција и сигурност*, Ревија, бр. 1-2, Загреб, стр. 6

[68] Kennan, G., (1966), *Realities of American Foreign Policy*, Norton, New York, p. 11. Према: Димитријевић, В., (1973), *Појам безбедности у међународним односима*, Савез удружења правника Југославије, Београд, стр. 20

самосталност и квалитет живота.[69] Одлуку о томе да ли су ове четири основне вредности угрожене доносе политичке елите на основу своје субјективне перцепције и сопствених интереса. Због тога се често каже да је концепт националне безбедности суштински споран.[70]

Најчешће коришћена и најшире прихваћена дефиниција концепта националне безбедности овај појам описује као одсуство страха да ће кључне вредности једне државе бити угрожене. Док с једне стране идентификовање кључних вредности може бити субјективно, широко је прихваћена чињеница да суштина ове дефиниције укључује питања која се тичу суверенитета и територијалног интегритета.[71]

Парадигме и институционални модели националне безбедности су се мењали кроз историју. Дуги низ година национална безбедност је нераздвојно била повезана са државом и њеним безбедносним сектором. Међутим, временом национална безбедност почиње постепено да захвата све сфере људског друштва. Иако главни задатак националне безбедности и даље представља одбрана од спољног напада, пракса недвосмислено потврђује да безбедност државе може бити нарушена унутрашњим потресима, економским и друштвеним поремећајима, као и другим кризним ситуацијама које могу паралисати читав безбедносни систем једне државе.[72]

Отуда Љ. Стајић сматра да је приликом научног разматрања овог појма неопходно правити разлику између појма безбедности државе и појма безбедности друштва, наглашавајући да основни критеријум безбедности државе представља њен суверенитет, а безбедности друштва идентитет, тј. свест о припадности заједници. Оно што се налази у основи ова два термина јесте егзистенција или преживљавање државе и друштва. Држава која изгуби суверенитет престаје да буде држава, а друштво које изгуби идентитет престаје да постоји као суверена јединка.[73]

Раздвајање појма државне од појма друштвене безбедности указује нам да је реч о два нормативна појма који се обједињавају у један интегрални појам означен термином национална безбедност. Суштина је у томе да се и код једног и код другог

---

[69] Димитријевић, В., (1973), *Појам безбедности у међународним односима*, Савез удружења правника Југославије, Београд.
[70] Baldwin, D., (1997), *The Concept of Security,* Review of International Studies Vol.23, No.1, pp. 10-12. Према: Ејдус, Ф., (2012), *Међународна безбедност: теорије, сектори и нивои*, Службени гласник, Београдски центар за безбедносну политику, Београд, стр. 231
[71] Roehrs, P., (2005), *Weak States and Imlications for Regional Security: A case study of Georgian instability and Caspian regional insecurity*, Research paper No. 97, Research Institute for European and American studies, p. 5
[72] Аврамов, С., (2001), *Безбедност у 21. веку*, Зборник радова СИМВОН, Београд, стр. 423
[73] Стајић, Љ., (2004), *Основи безбедности*, Полицијска академија, Београд, стр. 25

појма држава налази у средишту безбедносне дилеме, пружајући легитимитет и заштиту фундамен-талних друштвених вредности.[74]

Концепт националне безбедности производ је дуготрајних историјских процеса стварања првенствено суверене државе, нешто касније и националне државе. Од стварања Венецијанске лиге 1494. године, када долази до успостављања првог модерног система равнотеже снага у Европи, преко Вестфалског уговора из 1648. године и зачетка развоја појма суверености, па све до промене система у Француској крајем 18. века и успона национализма, текао је процес паралелне генезе националне државе и европског система држава.[75] Нешто касније, путем колонизације и деколонизације, европски систем државног уређења проширио се на остатак света. У другој половини 20. века, европски модел суверене државе увелико постаје доминантан у целом свету. Све до завршетка идеолошког сукоба између Истока и Запада, концепт националне безбедности представљао је доминантну тему теорије и праксе међународне политике.[76]

У Србији термин национална безбедност уведен је током периода између два светска рата.[77] Након завршетка Другог светског рата овај термин нестаје из званичног дискурса. Реорганизацијом Одељења за заштиту народа (ОЗНА) 1946. године настаје Управа државне безбедности (УДБ), која је 1966. године преименована у Службу државне безбедности (СДБ). Поред СДБ која је деловала на савезном нивоу, постојао је и Ресор државне безбедности (РДБ) на републичком нивоу, који је био у склопу Министарства унутрашњих послова.[78]

Након демократских промена нова власт је избацила из употребе термин државна безбедност због извесних асоцијација на разне злоупотребе које су биле присутне током постојања комунистичке Југославије, као и током деведесетих година двадесетог века. Усвојен је нови термин који се користи на енглеском говорном подручју, термин национална безбедност. РДБ је 2002. године издвојен из Министарства унутрашњих послова и створена је засебна установа која је преименована у Безбедносно-информативну агенцију (БИА). Термин национална

[74] Гаћиновић, Р., (2007), *Класификација безбедности*, Зборник радова НБП, Криминалистичко-полицијска академија, Београд, стр. 9. Видети на: http://www.kpa.edu.rs/data/akademija/nbp/nbp_2007_2.pdf 17.11.2012

[75] Опширније видети у: Wight, M., (1977), *System of States*, Leicester University Press, Leicester.

[76] Ејдус, Ф., (2012), *Међународна безбедност: теорије, сектори и нивои*, Службени гласник, Београдски центар за безбедносну политику, Београд, стр. 232

[77] У том периоду унутар Министарства унутрашњих послова Краљевине Југославије формирана је Дирекција националне безбедности.

[78] Ibid

безбедност добио је и свој институционални израз 2007. године када је на основу Закона о основама уређења служби безбедности Републике Србије (2007) предвиђено оснивање Савета за националну безбедност. Две године касније, по први пут од демократских промена јасно и изричито су дефинисани национални интереси кроз усвајање Стратегије националне безбедности Републике Србије.[79]

Употребом термина национална безбедност избегнута је политичка конфузија, али је створена нова, семантичка конфузија. За разлику од енглеског језика у коме се термин *nation* односи на државу, у српском језику овај термин се пре свега односи да етничку групу. Тако да често долази до забуне, односно недоумице шта представља референтни објекат националне безбедности (Република Србија или српски народ). Ова конфузија види се и у поменутој Стратегији националне безбедности, где је на први поглед референтни објекат заштите Република Србија, односно држава, док се у позадини назире етнички дефинисана нација. Ова семантичка забуна свакако не олакшава разрешење политичких конфузија које је демократска Србија наследила од претходног режима, а које се тичу дефинисања граница и природе политичке заједнице у којој живе грађани Србије.[80]

2.2.3.1. Национални интерес

Појам *националног интереса*[81] можемо одредити као неку врсту аналитичког апарата за описивање и прописивање онога што јесу или треба да буду виталне потребе неке политичке заједнице. Појам је почео да се развија крајем 16. века, заједно са настанком модерних европских држава. У то време није се употребљавао термин национални интерес, већ термини као што су државни разлог, династијски интереси и воља владара.[82] Са настанком националне државе крајем 18. и почетком 19. века, термин национална безбедност почео је да потискује све ове термине који су се у принципу користили за означавање сличне ствари.[83] У временском периоду између два светска рата, појам националног интереса обично се везивао за економске интересе држава. Тако је 1936. године Вилијем Елиот национални интерес представио као прорачунату анализу, углавном ограничену на стање економског биланса националне

[79] Ibid
[80] Ibid, 233-234
[81] Потребно је истаћи да је појам националног интереса уско повезан са појмом националне безбедности.
[82] Ibid, 234
[83] Beard, C., (1934), *The Idea of National Interest*, Blue Ribbon Books, New York, p. 31. Према: Ејдус, Ф., (2012), *Међународна безбедност: теорије, сектори и нивои*, Службени гласник, Београдски центар за безбедносну политику, Београд, стр. 234

користи, која се може извући из одређене политике.[84] У другој половини 20. века појам националних интереса је доспео у сам центар науке о међународним односима и то највише захваљујући делима Ханса Моргентауа. Према његовом мишљењу суштина сваке политике своди се на интерес, а међународну политику карактерише борба за националне интересе. Стицање, увећање и употребу моћи види као главни национални интерес сваке државе.[85]

Све до завршетка Хладног рата, национални интерес је имао централно место у проматрању међународних односа. Након завршетка идеолошког сукоба, који је трајао готово пола века, долази до великих заокрета у светској политици и у први план науке о међународним односима доспева социјални конструктивизам. Постојећој групи националних интереса (моћ, аутономија, благостање) конструктивисти додају још један интерес, колективно поштовање. У прилог томе, Александар Вент сматра да, као и појединци, и државе теже не само да изграде позитивну слику о себи, већ и да ту слику прихвате и признају и друге државе.[86]

Професор Андреја Милетић закључује да национални интерес мора бити конкретан. Према његовом мишљењу, узалудно је тражити неки општи појам националног интереса који је одређен ван конкретног времена и простора.[87] Иако је национални интерес тешко употребљив као делотворно средство политичке анализе, не сме се занемарити његов значај као политичке чињенице. У том смислу је концепт националног интереса незаобилазан у разматрању концепта националне безбедности.[88]

2.2.4. Људска безбедност

Често се поставља питање због чега је људска безбедност добила тако истакнуто место у бројним расправама и међу бројним групама. Изгледа да енергија извире из раскорака између безбедносних претњи (које су се драматично промениле након завршетка Хладног рата) и одговора држава и међународне заједнице на њих. Иако је

[84] Опширније видети у : Elliot, W., (1935), *The Idea of National Interes*, Harvard Law Review Vol. 48, No. 4, pp. 698-699. Према: Ејдус, Ф., (2012), *Међународна безбедност: теорије, сектори и нивои*, Службени гласник, Београдски центар за безбедносну политику, Београд, стр. 234

[85] Опширније погледати у: Morgenthau, H., (1975), *Politics among Nations*, 5th edition, Knopf, New York

[86] Wendt, A., (1999), *Social Theory of International Politics*, Cambridge University Press, Cambridge, pp. 326-327

[87] Милетић, А., (1977), *Национални интерес у америчкој теорији међународних односа*, Докторска дисертација, Факултет политичких наука, Београд, стр. 614

[88] Симић, Д., (2002), *Наука о безбедности – савремени приступи безбедности,* "Службени лист" СРЈ, Београд, стр. 32-33

неспорно да су неке претње нарасле након Хладног рата, исто је тако извесно да је порасла наша способност да им се супротставимо.

Термин људска безбедност потиче однедавно и све се више употребљава. Појам је произашао из либералне теорије, према којој је човек главни објекат безбедности, за разлику од реализма који у први план ставља државу као главни објекат безбедности. Заговорници либерализма сматрају да људе треба посматрати као циљ, а не као средство, што је начело и људске безбедности. Концепт се почео развијати почетком деведесетих година 20. века, са завршетком Хладног рата који је био обележен заштитом државних интереса и умножавањем војне моћи. За разлику од државне безбедности, коју можемо дефинисати као психолошко одсуство страха од спољне агресије и која у први план ставља државу као главни објекат безбедности, људска безбедност у први план ставља човека.

Сам појам људска безбедност најчешће се доводи у везу са Извештајем о људском развоју (*HDR*) Програма за развој Уједињених нација (*UNDP*) из 1994. године, где се први пут појављује. Намена људске безбедности била је да направи мост између слободе од страха и слободе од ускраћености – самих слобода које су у срцу Уједињених нација.[89] Још 1945. године кад је државни секретар САД поднео извештај својој влади о резултатима Конференције у Сан Франциску рекао је следеће:[90]

"*Битка за мир се мора водити на два фронта. Прва се односи на безбедносни фронт, где победа значи извојевати слободу од страха. Друга се односи на економски и друштвени фронт, где победа значи слободу од ускраћености. Само победа на оба фронта може да обезбеди свету трајни мир. ... Нема те одредбе која би се додала Повељи и тиме омогућила Савету безбедности да створи безбедан свет, уколико мушкарци и жене немају безбедност у својим домовима и на радним местима*".

Према поменутом извештају, чији је аутор иначе пакистански економиста Махбуб ул Хак, људска безбедност обухвата два аспекта. Прво, она подразумева безбедност од хроничних претњи, попут глади, болести и репресије. Друго, људска безбедност обухвата заштиту од изненадних и болних поремећаја у обрасцима свакодневног живота, без обзира на то да ли је реч о кући и послу, или о заједници.[91]

[89] Дулић, Д., (Ур.), (2006), *Људска безбедност 1*, Фонд за отворено друштво, Београд, стр. 106
[90] Ibid
[91] UNDP, Human Development Report 1994, Oxford University Press, New York, 1994. Видети на интернет страници: http://hdr.undp.org/en/media/hdr_1994_en_contents.pdf 17.11.2012

Овако дефинисана људска безбедност обухватала је следећих седам димензија:[92]

- економска сигурност,
- безбедност у погледу здравља,
- безбедност у погледу исхране,
- безбедност животне средине,
- појединачна безбедност,
- безбедност заједнице и
- политичка безбедност.

Извештај о људском развоју из 1994. године није људску безбедност искључиво везивао за заштиту појединца од насиља, већ се односио и на његов свеобухватни развој.

2.3. Однос кризног менаџмента и безбедносних парадигми

Када би се људи, институције и државе у потпуности рационално понашали, безбедносна политика, а са њом и кризни менаџмент мењали би се у складу са променом претњи по друштво и по државу. Велике кризе, велике несреће, терористички напади и слични догађаји (кубанска криза, теористички напади у САД-у, Лондону, Мадриду, Русији, Француској) доказ су да се државе не прилагођавају тако ефикасно новим безбедносним претњама и да се нове безбедносне парадигме и нови приступи у кризном менаџменту не развијају тако лако. Бројне студије указују на то да се нове безбедносне парадигме појављују тек након великих катастрофа.[93] Тако на пример, свих седам безбедносних политика САД-а објављених након Другог светског рата инициране су великим катастрофама које САД нису очекивале или нису биле припремљене за њих. Оно што важи за промене безбедносних парадигми у САД-у, такође важи и за буџет САД-а намењен одбрани државе, јер се ни буџет није мењао (тј. новац се није прераспоређивао) у складу са новим перципираним претњама.[94] Ово правило да се прилагођавање новим безбедносим претњама и стварање нових безбедносних парадигми дешава тек након што држава претрпи неку велику

[92] Ејдус, Ф., (2012), *Међународна безбедност: теорије, сектори и нивои*, "Службени гласник", Београдски центар за безбедносну политику, Београд, стр. 219

[93] Johnson, D. P., and Madin, M. P., (2006), *Paradigm Shifts in Security Strategy*, *Why Does It Take Disasters to Trigger Change*, p. 232

[94] True, J. L., (2002), The changing focus of national security policy. In Baumgartner, F.R. and Bryan, D, J. (Eds), (2002), *Policy Dynamics*, Chicago: University of Chicago Press, p.156

катастрофу, посебно важи у случају демократских, моћних, модерних држава, и то када претрпе катастрофе које су драматичне, које изазивају велике материјалне штете и велики број жртава а које се при том раније нису дешавале. У периодима током којих се не дешавају кризе, мењање безбедносних парадигми је отежано из више разлога – због могућности да претње остану само теоретске, па да се тиме у ситуацији кад дође до неке сличне кризе изазове погрешна (контрапродуктивна) реакција, затим због психолошких склоности особа које доносе безбедносну политику да се одржи *статус кво* кад је у питању промена безбедносних парадигми, због идиосинкратских политичких склоности људи који утврђују безбедносну политику (посебно ако су у питању доминантни лидери држава), као и због организационих склоности и бирократских процеса који настоје да се одупру променама. Теорија о изненадним катастрофама које прекидају периоде *стагнације* у развоју безбедносних парадигми и кризног менаџмента појавила се још 1970. године када је то правило приметио Томас Кун (Thomas Kuhn),[95] да би се затим на то поново осврнули Френк Баумгартнер[96] (Frank Baumgartner, 1993. године) и Брајан Џоунс (Bryan Jones, 2002. године) када су објашњавали динамику развоја америчке безбедносне политике.

Чак и кад адаптација на нове претње настаје пре саме катастрофе, дешава се да безбедносне парадигме буду кратког века. У таквим ситуацијама брзо до изражаја дођу недостаци нових парадигми, било да су настали из психолошких, организационих или политичких разлога. Људски мозак често настоји да перципира прошле догађаје у претерано позитивном светлу.[97] Чак и након Првог светског рата који је до тада био крвопролиће без преседана, Џон Стосингер[98] је приметио "да се старији људи са којима је разговарао о рату, сећају почетка рата као величанственог периода. Дистанца са које они посматрају овај догађај романтизовала је њихово сећање, пригушила је бол и осећање ужаса".[99] Свака држава и друштво настоје да ублаже своје неуспехе и изграде нове митове којима би реинтерпретирали историју. Тако је на пример немачко друштво након Првог светског рата пригрлило мит којим су им политичари сервирали да је

[95] Kuhn, S.T., (1970), *The Structure of Scientific Revolutions*, Chicago University Press, Chicago.
[96] Baumgartner, F. R., and B. D. Jones, (1993), *Agendas and instability in American politics*, University of Chicago Press, Chicago; Schacter, D. L., ed., (1995), *Memory distortion: How minds, brains, and societies recontruct the past*, Harvard University Press, Cambridge.
[97] Greenwald, A. G., (1980), *The totalitarian ego: Fabrication and revision of personal history*, American Psychologist 35: 603–618
[98] Stoessinger, J. G., (1998), Why nations go to war, St. Martin's Press, New York.
[99] Van Evera, S., (1998), *Hypotheses on nationalism and war*, International Security 18, pp. 5–39; Schivelbusch, W., (2004), *The culture of defeat: On national trauma, mourning, and recovery*, Picador Press, Newyork; Johnson, D. D. P., and D. R. Tierney., (2006), *Failing to win: Perceptions of victory and defeat in international politics*, Harvard University Press, Cambridge.

аустроугарска војска остала непоражена на бојном пољу. У међувремену, политичка елита пролази кроз промене, и формира привид промене, без икакве намере да сносе одговорност. За падање неке велике кризе у заборав, а самим тим и за неозбиљније схватање постојећих безбедносних претњи и настанак пропуста у спровођењу безбедносне политике и кризног менаџмента данас није неопходно да прође претерано много времена. Практичан пример је терористички напад у САД-у 2001. године. Наиме, напад се релативно скоро догодио, али изгледа као да су последице напада помало заборављене, с обзиром на то да многе планиране реформе (које је предложила комисија основана непосредно након напада и која је требало да се бави новим безбедносним решењима) још увек нису спроведене.[100] Слично се догодило и након бомбашког напада у лондонском метроу. У листу *Економист* је 2006. написано: "Злочин почињен 7. јула 2005. године у Лондону заправо је био нека врста аларма, који је најпре довео до неумерене војне реакције, а затим до колективног падања друштва у сан". Приметно је да су се политичка и медијска пажња као и пажња јавности врло брзо преусмериле са тероризма и борбе против теоризма на нову катастрофу о којој су сви говорили – рату у Ираку.

Срећна околност је у томе да велике катастрофе (у овом случају терористички напади) обично оставе довољно последица да се и након што тај иницијални занос и намера да се оформе нове безбедносне парадигме и мере кризног менаџмента избледе, настави (додуше много спорије) са увођењем нових безбедносних мера (нпр. спровођење мера обезбеђивања аеродрома и оснивање британског секретаријата за ванредне ситуације).[101] Ипак, иако људи (државе, друштва) не успевају да избегну катастрофе, треба бар да науче како да реагују на њих на начин који би довео до квалитетних промена безбедносне политике, безбедносних парадигми и начела кризног менаџмента.

Демократске моћне модерне државе можда имају најбоље могућности да избегну безбедносне катастрофе. Било да држава има или нема добре шансе да избегне безбедносне катастрофе, постоје бројне препоруке (у виду промена безбедносне политике) које би могле да унапреде ефикасно адаптирање новим безбедносним претњама. Постоји низ модела на основу којих се мењају безбедносне парадигме на нивоу једне државе.

---

[100] 9/11 Public Discourse Project, final report on 9/11, Commission recommendation, 2005, извештај је доступан на интернет адреси: www.9-11pdp.org 17.11.2012

[101] www.ukresilience.info 17.11.2012

Иако постоји могућност да се унапреди безбедносна политика било које државе, као што постоји и могућност да се установе нове безбедносне парадигме и нова правила кризног менаџмента, историјска искуства указују на то да су државама и друштву потребне катастрофе (кризе) како би се *пробудили* и почели да раде на променама безбедносних парадигми.

3. ПОЈМОВНО ОДРЕЂЕЊЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ И КЛАСИФИКАЦИЈА КРИТИЧНИХ СЕКТОРА

3.1. Појам инфраструктуре

Инфраструктура представља основ опстанка и развоја цивилизације. Такву улогу имала је од оног тренутка од када је човек свесно оформио прво станиште и култивисао прве житарице. Поред станишта он је морао да изгради и прве примитивне инфраструктурне објекте као што су бунари и спремишта за производе које је узгајао. О овим, као и свим другим инфраструктурним објектима који су потом следили, тадашњи човек морао је да научи да је поред њихове изградње веома важна и ефикасна експлоатација и квалитетно одржавање и заштита. До данас то је био и остао услов и једини начин да ти објекти буду од помоћи људима како са економског, тако и са друштвеног, културног и политичког аспекта.

Термин *инфраструктура* први пут се појавио у Француској, где је коришћен за означавање постељице – материјала испод пруге. Сама реч *инфраструктура* настала је комбиновањем латинског префикса *инфра*, што значи *доле*, *испод* и *структура*. Касније се овај термин појављује најпре у војсци у Сједињеним Америчким Државама након формирања НАТО-а 1949. године, а затим је у модерном цивилном смислу усвојен и од стране урбаниста 1970. године.[102] Термин се у Сједињеним Америчким Државама интензивније користи од 1980. године, након објављивања књиге *Америка у рушевинама*,[103] која је покренула низ јавно-политичких расправа о *кризи националне инфраструктуре*, узроковане вишедеценијским неадекватним улагањем и лошим одржавањем. Захваљујући овим расправама у многоме је унапређен менаџмент инфраструктуре, као и одржавање инфраструктуре у САД - у.

[102] Online Etymology Dictionary, Douglas Harper, Historian*, The Etymology of Infrastructure:* http://dictionary.reference.com/browse/infrastructure 17.11.2012

[103] Choate, P., and Walter, S., (1981), *America in Ruins: The Decaying Infrastructure*, Duke Press Policy Studies, New York.

Расправа о политици управљања инфраструктуром је у то време била додатно отежана због недостатка прецизне дефиниције инфраструктуре.

Дефиницију инфраструктуре у томе периоду даје између осталих Амерички савет државних агенција за планирање, који је објашњава као појам који обухвата јавне услуге и производна постројења која даље обухватају "широк опсег јавних постројења и опреме која је потребна за пружање друштвених услуга и подршке привредним активностима приватног сектора". Према овој дефиницији, инфраструктура обично обухвата *путеве, мостове, водене и канализационе системе, аеродроме, луке и јавне објекте*, док може да обухвати *школе, здравствене установе, затворе, рекреационе објекте, производњу електричне енергије, противпожарне службе, депоније отпада и телекомуникације*.[104]

У извештају Конгреса из 1983. године о политици која се односи на стање националне инфраструктуре Конгресна канцеларија за буџет (ЦВО) анализира седам категорија инфраструктуре: ауто-путеве, системе јавног саобраћаја, постројења за прераду отпадних вода, водне изворе, контролу авио-саобраћаја, аеродроме и општинске водне системе. Ови системи, према поменутој канцеларији "имају заједничке карактеристике капиталног интензитета и високог јавног улагања на свим нивоима власти. Они су директно критични по активности националне привреде". Конгресна канцеларија за буџет наглашава да "концепт инфраструктуре може да има широку примену и да обухвати друштвене објекте као што су школе, болнице и затвори, а често обухвата и индустријске капацитете".[105]

Амерички национални истраживачки савет је покушао 1987. године да превазиђе забуну око дефиниције инфраструктуре усвајањем термина *инфраструктура јавних радова*, који се с једне стране односи на специфичне функционалне модалитете − ауто-путеве, улице, путеве и мостове; градски транспорт, аеродроме и ваздушне путеве; водоводе и водне ресурсе, управљање отпадним водама, менаџмент отпадних вода, производњу и дистрибуцију електричне енергије; телекомуникације и менаџмент опасних материја и отпада, и комбиноване системе ових поменутих елемената, а с друге стране обухвата оперативне процедуре,

[104] Vaughan, R., and Pollard, R., (1984), Rebuilding America VOL1, Planning and Managing Public Works in the 1980s., Council of State Planning Agencies, Washington D.C. pp. 1-2
[105] U. S. Congressional Budget Office. Public Works Infrastructure: Policy Considerations for the 1980s, April 1983. p.1

менаџмент поменутих инфраструктура и формирање развојних политика које су у складу са друштвеним потребама.[106]

У извештају из 1988. године Конгресна канцеларија за буџет даје допуњену категоризацију инфраструктуре (ауто-путеви, авио-саобраћај, јавни превоз, прерада отпадних вода и водни транспорт) на основу дефиниције по којој та постројења: "пружају основу или основни оквир за националну привреду, у којој федерална политика игра значајну улогу…". Ова дефиниција искључује неке објекте који се често сматрају за инфраструктуру – као што су јавни смештај, државне зграде, приватне железничке услуге и школе – и неке објекте који су везани за животну средину (попут отпада опасних и токсичних материјала), где примарни терет одговорности пада на приватна лица.[107]

Конгрес је у много случајева уводио законе који су се односили на једну или више категорија инфраструктуре, као што су копнени транспорт или водни ресурси, али је ретко то радио свеобухватно. Током расправа 80-их година о пропадању јавних система, Конгрес је донео закон којим се успоставља Национални савет за унапређење система јавних услуга чији је задатак био да анализира и извештава Конгрес и председника о стању јавних инфраструктурних система. Према секцији 2 тог закона председник је дужан да пружи одређене информације о буџетским средствима која се издвајају за јавне цивилне и војне капиталне инвестиционе програме у годишњем извештају о буџету. Према закону, инфраструктура је у том тренутку обухватала "сваки физички објекат који се користи за пружање услуга или пружа друге користи на дужи временски период", а такође је обухватала, али није била ограничена на "путеве или мостове; аеродроме или ваздухопловне објекте; системе јавног превоза; прераду отпадних вода или слична постројења; пројекте за водне ресурсе; болнице; постројења за обнављање ресурса; јавне установе; просторне или комуникационе објекте; железничке путеве и федералне зграде".

Национални савет за унапређење система јавних услуга пружио је другу дефиницију инфраструктура и обухватио девет категорија система у својим анализама: ауто-путеве, улице, путеве и мостове; аеродроме и писте; јавни превоз; интермодални транспорт; снабдевање водом; прераду отпадних вода; водне изворе; чврсти отпад; и отпаде опасних материја. Ове категорије, према Савету, имају јаке везе са привредним развојем и генерално имају традицију повезаности са јавним сектором. Постројења и

[106] *Infrastructure for the 21st Century*, National Academy Press, Washington, D.C, 1987
[107] U. S. Congressional Budget Office. *New Directions for the Nation's Public Works*, September 1988

објекти имају високе трошкове и дуг економски живот. Према Савету, услуге које пружају инфраструктуре су јако битне за "националну одбрану, јаку привреду и здравље и сигурност грађана".[108]

Од 1980-их година, пажња политичара знатно је померена са разматрања проблема инфраструктура свеобухватно и на начин на који је то рађено у то време. Законски предлози генерално су били окренути потребама појединачних сектора и уз дефинисање улоге федералне власти, посебно кад су у питању финансије.

Имајући у виду важност инфраструктуре једне државе, њену употребну вредност и значај за развој и унапређење сваке заједнице, као приоритетан задатак сваког друштва се намеће рационално и ефикасно управљање овим јавним добрима. То се може постићи само доследним поштовањем и спровођењем дугорочне државне стратегије развоја, унапређења и заштите инфраструктурних система.

Нека општа подела данашњих инфраструктура може се извршити на *тврде* и на *меке* инфраструктуре. Термин *тврде* односи се на физичке системе неопходне за функционисање модерног индустријског друштва, док се термин *меке* инфраструктуре односи на институције које су неопходне за очување економских, здравствених, културних и друштвених стандарда (финансијски систем, образовни систем, систем здравствене неге, систем државне управе, спровођење закона, службе за ванредне ситуације).[109]

У оквиру *тврде* (физичке) инфраструктуре разликују се следећи сектори:[110]

- **Саобраћајна инфраструктура**
  - Друмски саобраћај − мрежа друмских саобраћајница, мостова, тунела, одводних канала, систем сигнала и ознака, електрични системи (улично осветљење и семафори), ивичњаци, тротоари и специјализовани објекти, као што су складишта за одржавање путева и одморишта,
  - Системи масовног транспорта − шински системи, подвожњаци, трамвајски, тролејбуси, и аутобуски превоз, железнички саобраћај – железнице,

[108] National Council on Public Works Improvement, Fragile Foundations: A Report on America's Public Works, Final Report to the President and Congress, Washington D.C., February 1988, p. 33

[109] Niskanen, A. W., (2011), The soft infrastructure of a Market, CATO Journal, pp. 233-238; Gotbaum, R., (2011), The Difference Between Soft And Hard Infrastructure, And Why It Matters, State Impact Magazine, New Hampshire, 26. October

[110] Grübler, A., (1990), The Rise and Fall of Infrastructures: Dynamics of Evolution and Technological Change in Transport Heidelberg and New York, Physica –Verlag.

терминална опрема (железничке станице), прелази, сигнализација и комуникациони системи,

- Канали и пловни путеви који захтевају континуирано одржавање (багеровање, итд.),
- Луке и светионици,
- Аеродроми, ваздушни навигациони системи,
- Бициклистичке стазе и пешачке стазе, пешачки мостови, подвожњаци, пешачке и друге специјализоване конструкције за бициклисте и пешаке,
- Трајекти.

- **Енергетска инфраструктура**:

  - Електроенергетска мрежа, укључујући и производна постројења, електричну мрежу, трафо-станице, као и локалну дистрибуцију.
  - Гасоводи, терминали за складиштење и дистрибуцију гаса, као и локалне дистрибутивне мреже. Неке дефиниције могу да укључе и налазишта гаса, као и флоту бродова и камиона којима се превози течни гас,
  - Нафтни цевоводи, терминали за складиштење и дистрибуцију нафте. Неке дефиниције могу да подразумевају и нафтне бушотине, рафинерије, као и флоте бродова танкера и теретних возила за транспорт нафте,
  - Специјализована постројења за обраду угља, за прање, складиштење и транспорт угља. Неке дефиниције могу да укључе и руднике угља.
  - дистрибутивне мреже система даљинског грејања,
  - Мреже станица (терминала) за пуњење електричних возила.

Рудници угља, налазишта нафте и гаса могу се класификовати као део рударског и индустријског сектора економије, а не као део инфраструктуре.[111]

- **Инфраструктура менаџмента вода**:

  - Снабдевање водом за пиће, укључујући и систем цеви, акумулацију воде, пумпе, вентиле, системе за филтрирање и пречишћавање, затим зграде и објекти за смештај опреме која се користе за прикупљање, пречишћавање и дистри-буцију воде за пиће,
  - Канализација и одлагање отпадних вода,
  - Дренажни системи (кишне канализације, канали, итд),

[111] Economic Infrastructure CRS Codes, OECD: http://www.oecd.org/dataoecd/12/25/43860714.pdf 17.11.2012

- Велики системи за наводњавање (резервоари, канали за наводњавање),
- Велика системи за одбрану од поплава (насипи, контролни системи, главне црпне станице и бране),
- Системи за уклањање снега – флота возила која се бави уклањањем снега, плугови, чистачи снега, дампер камиони, тротоарски плугови, снежне бране, топљачи снега,
- Приморски менаџмент − валобрани, молови, бране стабилизација пешчаних дина и заштита шума мангрове приобалних мочвара.

- **Комуникациона инфраструктура**:
  - Поштанске службе, укључујући и објекте за сортирање пошиљки,
  - Телефонске мреже (фиксна телефонија) укључујући и систем телефонских централа,
  - Физичка инфраструктура мобилне телефоније,
  - Станице за пренос ТВ и радио емисија, укључујући прописе и стандарде који регулишу емитовање,
  - Физичка мрежа кабловске телевизије укључујући станице и дистрибутивне мреже кабловског сигнала (не укључује провајдере садржаја или тв мреже, када се термин користи у смислу специјализованих канала као што су CNN и MTV),
  - Интернет − основни рутери, сервери, локални интернет провајдери, протоколи и основни софтвер неопходан за функционисање система (не укључује конкретне сајтове, мада може да подразумева неке често коришћене веб-услуге, и често коришћене друштвене мреже и веб-претраживаче),
  - Комуникациони сателити,
  - Подморски каблови,
  - Главне приватне, државне или наменске телекомуникационе мреже, као што су оне које се користе за интерну комуникацију и праћење од стране великих инфраструктурних предузећа, од стране влада, војски или хитних служби, као и националне истраживачке и образовне мреже,
  - Мрежа за дистрибуцију поште путем пнеуматских цеви.

- **Управљање чврстим отпадом**:

- Општинске депоније и прикупљање отпада за рециклирање,
- Депоније чврстог отпада,
- Постројења за спаљивање чврстог отпада,
- Објекти за одлагање опасног отпада,
- Објекти за рециклирање отпада.

- **Мрежа за праћење и надзор Земље**:

  - Метеоролошка мрежа,
  - Мреже за гравитациони мониторинг,
  - Сеизмометарска мрежа,
  - Сателити за посматрања Земље,
  - Геодетске референтне тачке,
  - Глобални систем за позиционирање (GPS),
  - Инфраструктура просторних података.

За разлику од тврде инфраструктуре, суштина меке инфраструктуре је да се односи на пружање специјализованих услуга људима. Пружање услуга које се сматрају *меком* инфраструктуром зависи од високо развијених система и великих специјализованих институција које деле доста карактеристика са *тврдом* инфраструктуром.

Следећи сектори спадају у *меку* инфраструктуру:

- **Инфраструктура државне управе**,

  - Систем државне управе и спровођење закона, укључујући политичке, законодавне, правне и казнене системе, специјализоване објекте (владине канцеларије, судови, затвори, итд), као и специјализоване системе за прикупљање, чување и дистрибуцију података, закона и прописа,
  - Хитне службе − полиција, противпожарна заштита, хитна помоћ, укључујући и специјализована возила, зграде, комуникационе и диспечерске системе,
  - Војна инфраструктура − војне базе, складишта оружја, постројења за обуку, командни центри, комуникациони објекти, велики оружани системи, утврђења, специјализована постројења за производњу оружја, стратешке резерве.

- **Економска инфраструктура**:
  - Финансијски систем, укључујући банкарски систем, финансијске институције, платни промет, производњу новца, финансијске прописе, и рачуноводствене стандарде и прописе,
  - Главна пословна постројења и системи за логистику, укључујући и складишта, као и системе за управљање складиштењем и шпедицијом,
  - Производња инфраструктуре, укључујући и индустријске паркове и специјалне економске зоне, руднике и постројења за прераду сировина, специјализоване енергетске, транспортне и инфраструктуре вода се користи у индустрији, зонирање еколошких закона и прописа којима се регулише и ограничав аиндустријска активност, организације за стандардизацију,
  - Пољопривредна, шумска и рибарска инфраструктура, укључујући и специјали-зована складишта и транспорт хране, товилишта великих пољопривредних система подршке (укључујући и пољопривредно осигурање), пољопривредно-здравствене стандарде и здравствене инспекције хране, експерименталне фарме и пољопривредне истраживачке центре и школе, системе за издавање дозвола, спровођење система против криволова, шумских чувари и ватрогасне службе.

- **Социјална инфраструктура**:
  - Систем здравствене заштите, укључујући болнице, финансирање здравствене заштите, здравствено осигурање, системе за регулисање и испитивање лекова и медицинских процедура, системе за обуку, системе за инспекцију, системе за испитивање професионалне дисциплине лекара и других здравствених радника, системе за праћење јавног здравља. Такође, систем здравства обухвата и координационе мере предузете у јавним здравственим институцијама у ванредним ситуацијама и у случају епидемија,
  - Образовни и истраживачки системи, укључујући и основне и средње школе, универзитете, специјализоване факултете, научне установе, системе за финансирање и акредитацију образовних институција,
  - Социјална заштита у виду материјалне помоћи сиромашнима, како од стране владе тако и од стране приватног сектора, као и пружање социјалне заштите људима у невољи или жртвама злостављања.

- **Културна, спортска и рекреациона инфраструктура**
  - Спортска и рекреативна инфраструктура, као што су паркови, спортски објекти, систем спортских лига и удружења,
  - Културна инфраструктура − концертне дворане, музеји, библиотеке, позоришта, студији, и специјализовани објекти за обуку,
  - Пословна путовања и туристичка инфраструктура, укључујући и вештачке и природне атракције, конгресне центре, хотеле, ресторане и остале услуге које су намењене углавном туристима и пословним људима, као и системе за информи-сање и привлачење туриста и осигурања.

3.2. Заштита инфраструктуре као транснационални интерес

Безбедност инфраструктуре подразумева пре свега заштиту оних инфраструктура које се сматрају критичним (о чему ће бити више речи у следећим поглављима, али се у контексту заштите, а затим и у контексту транснационалног карактера већ сад морају поменути) као што су: аеродроми, ауто-путеви, болнице, мостови, транспортна чворишта, мрежне комуникације, медији, мрежа снабдевања електричном енергијом, бране, нуклеарне електране, луке, рафинерије нафте, водни системи итд. Главни циљ заштите критичне инфраструктуре је ограничење рањивости те инфраструктуре, спречавање саботажа, тероризма и контаминације и на крају спречавање ширења негативних ефеката на неко веће подручје и већи број сектора, уколико се догоди нешто што би прекинуло нормално функционисање инфраструктуре.[112]

Критичне инфраструктуре у свом развоју све више користе информационе технологије, с обзиром на то да оне постају доступне све широј јавности. Као резултат интензивнијег коришћења информационих технологија од стране разних сектора дошло је до стварања огромне зависности између различитих инфраструктурних сектора. У овом контексту посебно је приметна и значајна зависност скоро свих инфраструктурних сектора од информационих технологија (које су и саме прерасле у један критични, вероватно и најкритичнији инфраструктурни сектор). Данас је постојање велике међу-повезаности инфраструктура један од већих проблема у управљању тим инфра-структурама.[113]

[112] Детаљније видети на интернет адреси: http://www.tsa.gov/who_we_are/index.shtm 17.11.2012
[113] Li, H., et al, (2005), Strategic Power Infrastructure Defense, Proceedings of the IEEE.

Критичне инфраструктуре од виталног су значаја за нормално функционисање друштва и држава. Инциденти, несреће или намерно ометање нормалног функционисања инфраструктура може да остави озбиљне последице по економију и да спречи на дужи или краћи период рад инфраструктуре, што се може одразити на велики број људских делатности. Бројни су разлози због којих инфраструктура мора бити добро обезбеђена и заштићена. Неки од разлога су ***терористички напади*** (ситуације кад једна особа или група људи намерно напада инфраструктуру из политичких или идеолошки разлога – напади на Светски трговински центар у САД-у 2001. године, бомбашки напади у лондонском метроу (2005. године) и у Мадриду (2004. године), бомбашки напад на аеродрому Домодедово у Русији (2011. године), бомбашки напади на главној железничкој станици у Мумбаију 2008. године), ***саботаже*** (ситуације када једна особа или организована група (нпр. бивши запослени на некој инфраструктури, политички противници Владе или групе за заштиту животне средине предузимају напад током ког преузимају контролу над функционисањем кртичне инфраструктуре), ***информационо ратовање*** (приватни корисници – хакери или пак читаве државе могу из различитих разлога да нападају информационе системе у разним земљама и да доведу до великих проблема не само у функционисању информационе инфраструктуре већ и многих других сектора, с обзиром на то да се многи ослањају на информационе системе – такви су били сајбер-напади током 2008. године, тј. током рата у јужној Осетији), ***природне катастрофе*** (урагани и природни догађаји оштећују инфраструктуру попут цевовода, мрежа снабдевања водом и храном и сл. - такви су били ураган Ике или пак ураган Катрина).

Један од основних инфраструктурних сектора за опстанак човека дефинитивно је и сектор производње и снабдевање становништва електричном енергијом. Намерно узурпирање функционисања мреже снабдевања електричном енергијом може да има јако негативан утицај на националну безбедност, националну економију и на живот сваког човека понаособ. Пошто је мрежа дистрибуције електричне енергија врло разграната, велики изазов представља очување нормалног функционисања те инфраструктуре.[114] Саботаже попут сајбер-напада могу у великој мери да оштете сектор производње и дистрибуције електричне енергије и да спрече успут и нормалну комуникацију и рад информационих система и то не само на националном већ и на транснационалном нивоу.

[114] Massoud, A., (2002), "Security Challenges for the Electricity Infrastructure (Supplement to Computer Magazine)". *Computer* (IEEE computer society), 2002-04

Напади слични овом везани за сектор производње и дистрибуције електричне енергије могући су и у великом броју других сектора, при чему последице могу да превазилазе границе земље у којој се десио инцидент. Ова тенденција да се последице прекида нормалног функционисања инфраструктуре у једној земљи осете и ван те земље, довела је до увођење новог термина – **транснационалне инфраструктуре**. Јохан Шот у свом раду о транснационалним инфраструктурама у модерној Европи 2003. године каже да су то оне инфраструктуре које повезују државе.[115]

Данас се може говорити о све већем броју инфраструктурних сектора који постају транснационални – сектор информационих и комуникационих технологија је одавно превазишао националне границе држава (а из дана у дан постаје све утицајнији), а такви су и сектори саобраћаја (друмски, железнички, ваздушни, водни), затим телекомуника-ција, хемијске индустрија, као и нуклеарне индустрије. Посебно значајан је и финансијски сектор, који је дефинитивно у огромној мери транснационални, за шта постоје врло очигледни докази. Наиме, светска економска криза која је започела крајем 2007. године у САД-у врло брзо се са националног пренела на међународни ниво, довела до глобалне рецесије, уздрмала темеље националних тржишних привреда и довела у питање до тада неприкосновену ефикасност слободног тржишта.[116] Увид у све релевантне и на међународном нивоу значајне транснационалне инфраструктуре у Европи остварен је формирањем списка критичних инфраструктура Европске уније. Наиме, један од предуслова да нека инфраструктура буде критична на нивоу ЕУ јесте да је транс-национална, односно да се последице њеног отказивања не осете само у земљи у којој је дошло до прекида функционисања, већ бар у још једној земљи. Слична регулатива и правила постоје на нивоу свих организација које имају транснационални карактер, а баве се између осталог и питањима што ефикаснијег коришћења и заштите инфраструктуре.

Из постојећег транснационалног карктера и значаја већег броја инфраструктурних сектора јасно произилази да и заштита тих инфраструктурних сектора последично има велики значај не само за државу којој припада конкретна инфраструктура већ и за све остале државе на које евентуални прекид нормалног функционисања може имати утицај. Заштита транснационалних инфраструктура дакле логично представља и транснационални интерес и захтева висок ниво сарадње свих

[115] Schot, J., (2003), Transnational Infrastructures and the Rise of Contemporary Europe, working Doc No.1, January

[116] *Global Economic Crisis*, A Publication of Yale Center for the Study of Globalization, Yale Global Online, доступно на сајту: http://yaleglobal.yale.edu/content/global-economic-crisis 17.11.2012

битних актера у процесу заштите и свих држава за које је одређени инфраструктурни сектор битан.

3.3. Критична инфраструктура

3.3.1. Појмовно одређење критичне инфраструктуре

Појава концепта критичне инфраструктуре у политичком лексикону Запада може се објаснити променама које су најпре настале у перцепцији претњи и све већом међуповезаношћу разних инфраструктурних елемената, што заједно чини друштво изузетно рањивим на разне врсте напада и отказивања критичних инфраструктурних система. Током последњих година променио се начин на који се посматра концепт критичне инфраструктуре и рањивост критичне инфраструктуре. Рањивост критичне инфраструктуре и читавог друштва раније се везивала за проблеме у функционисању високоризичних технологија, да би се данас на критичну инфраструктуру и претње по критичну инфраструктуру гледало као на питање од највећег значаја за националну безбедност.

У књизи Чарлса Пероа (Charles Perrow) из 1984. године помиње се концепт *нормалних несрећа*, који се односи на системску рањивост високоризичних технолошких система као што су на пример авиони, нуклеарне електране и генетски инжењеринг. Чарлс Пероу је изнео и аргументовао претпоставку да се менаџмент комплексним технолошким системима може унапредити тиме што би се приликом доношења одлука у обзир узимали безбедносни ризици људског и технолошког порекла, али да се и поред свих напора, несреће и велике катастрофе тешко могу избећи баш због огромне комплексности задатака постављених пред менаџмент. Писана у време Хладног рата, књига указује на то "да високоризичне технологије представљају творевину друштвених и државних система, а не дело појединаца или продукт неке идеологије".[117] Пероу доводи у питање производњу нуклеарне енергије, ДНК инжењеринг и системе контроле ваздушног саобраћаја, јер по његовим речима "ови системи настају и опстају захваљујући спрези политичких погодби, приватизација и немарног односа према трошковима које сноси друштво".[118]

Немачки социолог Улрих Бек спровео је 1986. године истраживање везано за импликације које високоризичне технологије имају на друштвену и политичку

[117] Perrow, C., (1999), *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton, p. 351
[118] Ibid, p. 351

динамику. Бек разматра у истраживању свакодневне ризике са којима се друштво суочава и парадигматске карактеристике будућих ризика. Он даље разматра разлоге настајања катастрофа у будућности; скреће пажњу на праксе које постоје и технике које се већ примењују приликом предвиђања глобалних ризика. Нешто касније ове праксе и технике процене ризика постају саставни део државних безбедносних политика.

Концепт колонизације ризика појављује се нешто касније како би објаснио процес у коме "људи више не управљају ризицима, већ се човечанство налази у ситуацији где ризици управљају људским поступцима". Управљање ризицима, по речима Хенрија Ротштајна, не може бити потпуно, јер одређени елементи којима је немогуће управљати и неочекиване последице стварају институционалне ризике који могу да угрозе легитимност организација које се баве управљањем ризиком. Даље, Ротштајн указује на то да "појава ризика није толико повезана са стварним или измишљеним променама објективних претњи по друштво, колико са начином на који системи за управљање ризицима перципирају претње по друштво".[119]

Након више од 30 година тумачења која је изнео Пероу о системској рањивости критичне инфраструктуре и Бековo истраживање ризичног друштва актуелнији су више него икад. Пероу је у издању своје књиге из 1999. године изнео став да су несреће попут Чернобиља, Бопала, Челенџера, које су посредно и непосредно погодиле читав свет, само потврда тога да се није много ствари променило у индустријском свету од 1984. године. Пероу даље констатује да се није направио неки значајан напредак у превенцији несрећа, али да је направљен велики напредак у интерпретирању несрећа.[120] Данас постоји одомаћени став да су несреће и велике катастрофе последица већег броја међусобно повезаних разлога. Неке катастрофе могу се предвидети или чак спречити, док друге несреће везане за отказивање комплексних система само чекају да се догоде, баш како је то објаснио Пероу још 1984. године. Оно што се од тад променило су системски оквири у којима се посматрају несреће и катастрофе. До ових промена парадигми у издвајању одређених инфраструктурних система као *критичнијих* у односу на друге дошло је услед нове интерпретације ризика и рањивости и њихове повезаности са националном безбедношћу.

[119] Beck, U., (2006), *World at Risk*, Polity Press, Cambridge, 2009, p. 3; H Rothstein, "*The Institutional Origins of Risk: A New Agenda for Risk Research*", Health, Risk & Society, vol. 8, no. 3, pp. 216–217

[120] Perrow, C., (1999), *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton, p. 353

Године 1997. америчка председничка комисија издала је један од првих извештаја о критичној инфраструктури у којем је идентификовано осам инфраструктура као *виталних*, тј. *критичних*. **Те инфраструктуре су**: 1) телекомуникације, 2) енергетски системи за производњу и експлоатацију електричне енергије, 3) енергетски системи за производњу и експлоатацију природног гаса и нафте, 4) банкарство и финансије, 5) саобраћај и транспорт, 6) системи снабдевања водом, 7) државне службе и 8) службе за помоћ у ванредним ситуацијама.[121] У извештају је закључено да је САД у тој мери зависна од ових инфраструктура да је Влада САД-а морала да их посматра у оквиру концепта националне безбедности, па су на основу тога ове инфраструктуре и сврстане у критичне.[122] Од 1997. године дефиниција критичне инфраструктуре се проширила те листа критичних инфраструктура и са њима повезаних кључних ресурса тренутно укључује 18 сектора.[123] Дефиниција критичне инфраструктуре коју је дала Организација за економску сарадњу и развој (OECD) 2008. године под критичном инфраструктуром подразумева скуп инфраструктура и служби које "представљају основу економског и социјалног благостања, јавне безбедности и функционисања владиних органа".[124] У оквиру Европске уније под термином критичне инфраструктуре подразумевају се постројења, системи или одређене компоненте тих система, који су лоцирани у земљама чланицама и који су есенцијални за обављање основних функција држава и Уније, затим који су неопходни за функционисање здравства, за безбедност чланица и за економско и социјално благостање грађана, а чије би отказивање или ометање функционисања имало знатан негативан утицај на земље чланице, а посредно и на читаву Европску унију.[125]

Мириам Дан Кевелти (Myriam Dunn Cavelty), начелница јединице за нове ризике у склопу Центра за безбедносне студије у Цириху, сматра да је концепт критичних инфраструктура као битног фактора националне безбедности само један од

[121] Pursiainen, C., (2009), "The Challenges for European Critical Infrastructure Protection", *European Integration*, vol. 31, no. 6, p. 723
[122] Brunner, E. M., Elgin, M., and Sutter, M., (2009), *International CIIP Handbook 2008/2009*, An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, Centerfor Security Studies, eth Zurich, p. 37
[123] Pursiainen, C., (2009), "The Challenges for European Critical Infrastructure Protection", *European Integration*, vol. 31, no. 6, p. 723
[124] Gordon, K., and Dion, M., (2008), "*Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security*", OECD, May, p. 3
[125] Council Directive 2008/114/EC, On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, Official Journal of the European Union, 23 December 2008, L 345/75-L 345/82

аспеката ширих промена у безбедносном дискурсу. Наиме, раније су претњу по безбедност представљале "агресивне намере одређених (конкретних) држава" које су данас замењене "ширим спектром ризика и непријатељима које је много теже идентификовати". Како тврди Дан Кавелти, за промену безбедносног дискурса одговорна је војска САД-а и то се десило из два разлога − најпре због експанзије спектра претњи по безбедност након Хладног рата, а затим последично и због промене у перцепцији могућих мета, јер се више не сматрају метама само војни циљеви, већ и неке друге *рањиве тачке*.[126] Ипак, могуће је повући паралелу између парадигми Хладног рата где се безбедност заснива на *заједнички осигураном уништењу* и заштите критичне инфраструктуре данас која се сматра наставком претходних парадигми у новом облику.

Током година Хладног рата нуклеарно застрашивање функционисало је под претпоставком *заједничког осигураног уништења*. Шездесетих година 20. века америчка стратешка ваздухопловна команда имала је 25 војних мета на свом радару, а такође се метом сматрао 151 урбани и индустријски центар у Совјетском Савезу, укључујући фабрике цемента и челика, нуклеарна постројења, радио станице, нафтне рафинерије, карго превоз и чворишта путничког саобраћаја. Иако могућност ненамерног напада услед квара нуклеарног оружја или система повезаних са функционисањем неуклеараног оружја није у потпуности искључена, основна претпоставка је да је концепт *заједнички осигураног уништења* у потпуности контролисан од стране држава. Како тврди Кевелти, перцепција претњи драстично се променила, док су критичне тачке остале исте.

Нове перцепције претњи по критичну инфраструктуру доста су повезане са традиционалним перцепцијама. У првом издању Међународног журнала о заштити критичне инфраструктуре из 2008. године (*International Journal of Critical Infrastructure Protection*) указује се на ту повезаност кроз причу о догађајима који су довели до уништења Рима. Наиме 537. године пре нове ере Готи су отпочели опсаду Рима и уништили главне аквадукте, који су представљали основну компоненту критичне инфраструктуре у граду. Може се рећи да улогу коју су тада у Риму имали аквадукти данас имају интернет и телекомуникациони системи, па се стога догађаји везани за опсаду Рима од стране Гота могу схватити као упозорење да је могуће да злонамерни ентитети из различитих делова света нападну интернет и телекомуникационе системе и

[126] Cavelty, M., (2007), *Critical Information Infrastructure: Vulnerabilities, Threats and Responses*, UNIDIR Disarmament Forum, no. 3, pp. 15–22

да тиме у истој мери угрозе функционисање друштва као што је угрожен био опстанак Рима након уништења аквадукта. Оно што представља додатну разлику у односу на тај период, како је напоменуто у журналу, јесте и чињеница да "данашњи варвари не морају да путују до капија града да би извршили опсаду града или уништили град".[127] Терористички напади на САД из септембра 2001. године главни су разлог што је заштита критичне инфраструктуре постала један од најважнијих елемената безбедносне политике САД-а, а затим и свих европских земаља и Европске уније.[128] Ти терористички напади представљају тренутак од ког почиње припрема америчке националне стратегије за физичку заштиту критичне инфраструктуре и кључних ресурса, која је објављена у фебруару 2003. године. Стратегијом се ствара основа за заштиту САД-.а од терористичких напада и за обезбеђивање *америчког начина живота*.[129]

Начин на који је критична инфраструктура представљена као основа западњачког начина живота привукла је пажњу многих стручњака који се баве критичним инфраструктурама и питањима безбедности. Стручњаци истичу да критичне инфраструктуре играју виталну улогу у данашњем друштву и представљају основ оног што се данас сматра квалитетним животом. Како Мајкл Дилон (Michael Dillon) и Џулијан Рид (Julian Reid) кажу: "одбрана критичне инфраструктуре није везана за свакодневну заштиту људи и људских живота од директних напада других људи, већ је везана за један свеобухватнији приступ комбинованој заштити физичке и технолошке инфраструктуре коју модерни либерални режими виде као неопходну за функционисање друштва и за очување безбедности".

Терористички напади на САД утицали су директно на промену безбедносне политике и промену приоритета у тој политици, па су од тог тренутка питања везана за еколошку заштиту (спречавање наглих климатских промена и сл.), која су до тада била најважнија, делимично скрајнута.[130] Појачани осећај рањивости и перцепција претње коју представља тероризам, резултовали су квантитативним ширењем безбедносног дискурса и довели су до стварања све веће дистинкције између цивилног и војног,

[127] Shenoi, S., (2008), "*Editorial*", International Journal of Critical Infrastructure protection, vol. 1 no. 1–2, p. 1
[128] Pursiainen, C., (2009), "The Challenges for European Critical Infrastructure Protection", *European Integration*, vol. 31, no. 6, p. 725
[129] The National Strategy for Physical Protection of Critical Infrastructures and Key Assets, The White House, February 2003. Доступно на сајту: http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf 17.11.2012
[130] Grove, K., (2010), Insuring Our Common Future, Dangerous Climate Change and the Biopolitics of Environmental Security, Geopolitics vol. 15, no. 3, p. 537

легалног и илегалног, домаћег и међународног, приватног и јавног и изнад свега између интерног и екстерног.

Фокусирање на критичну инфраструктуру и заштиту критичне инфраструктуре спречава оно што се у либерним демократским друштвима сматра "способношћу одржавања људи, служби и добара у покрету". Трауматични догађаји попут криза, ванредних ситуација, катастрофа представљају сметње који прекидају уобичајени ток живота. Баш такви трауматични догађаји брзо постају нека врста парадигматског сочива кроз које се посматра, разумева и конципира савремена безбедносна политика.[131] Проблем истраживања заштите критичне инфраструктуре данас се посматра у оквирима вежби решавања проблема, док се питања везана за новонастале односе снага ретко постављају.

Оно што се наглашава у скорашњим истраживањима заштите критичне инфраструктуре је схватање концепта заштите као скупа ствари које обухватају како људске тако и све остале компоненте. За функционисање лука, железница или пак електричне мреже најпре је неопходан комплексан систем физичких објеката, затим су неопходни подаци за покретање и функционисање система и, коначно, потребне су норме и правила која морају да поштују људи који оперишу том инфраструктуром. Исто тако сајбер-простор састоји се од опипљивих ствари у физичком простору укључујући широкопојасне оптичке линије, операционе центре, центре за подршку који контролишу проток финансијских информација, итд. У глобалу, политике заштите критичне инфраструктуре настоје да представе овакве комплексне системе као "затворене тоталитарне и обавезно успешне биополитичке системе". Уместо оваквог погледа на критичну инфраструктуру Лундборг и Вон-Вилиамс предлажу да ове комплексне инфраструктурне системе треба посматрати онакве какви су заиста – отворени, рањиви и неретко апсурдни системи са доста мана и унутрашњих проблема.[132]

Данас стручњаци у области заштите критичне инфраструктуре више практикују ову друго схватање критичне инфраструктуре и с обзиром на то да се заштита критичне инфраструктуре не посматра само као заштита од спољних напада, већ се под тим концептом подразумева и планирање опоравка, тако да је битан показатељ успешне политике заштите критичне инфраструктуре чињеница да систем може да

[131] Brasset, J., Vaughan-Williams, N., Governing Traumatic Events, Alternatives: Global, Local, Political, vol. 37, no. 3, p. 183

[132] Lundborg, T., and Vaughan-Williams, N., Resilience, Critical Infrastructure and Molecular Security: the Excess of Life in Biopolitics, *International Journal Political Sociology*, vol. 5, no. 4, p. 369

функционише у свим условима и да може брзо да се опорави уколико дође до оштећења неког сегмента критичне инфраструктуре.

Критичне инфраструктуре су раније доживљаване као нешто стабилно и конкретно, било да се ради о физичким или информационим и комуникационим системима, али је данас актуелан холистички доживљај критичне инфраструктуре као скупа мрежа или система који су витални за друштво у целини.[133]

Истраживање које је спровела Организација за економску сарадњу и развој (ОЕЦД) из 2008. године закључује да су дефиниције оног што улази у састав критичних инфраструктура углавном врло широке и да укључују и физичку инфраструктуру и неопипљиве елементе. Оно што је такође карактеристично је да су програми влада већег броја земаља засновани на *сверизичном приступу*, што значи да се приликом планирања политике заштите разматрају претње по критичну инфраструктуру везане за природне катастрофе, несреће и намерне нападе. Разлике у концептуализацији и дефинисању критичне инфраструктуре у различитим земљама последица су различите перцепције претњи и безбедносних ризика и разлика у географским и историјским предусловима и социополитичким факторима.

3.3.2. Различити приступи у класификацији критичних инфраструктура

Критична инфраструктура обухвата широк спектар виталних сектора, као што су саобраћај, транспорт, производња и дистрибуција енергије, информациони и комуни-кациони системи, здравствене службе, системи за снабдевање водом и храном, финансијске службе, државна инфраструктура (агенције и организације влада, административни сектор) итд. Делимично или потпуно отказивање ових инфраструктура може да угрози друштво, националну безбедност и да доведе до најразличитијих криза. Развијене земље, а последњих година и оне мање развијене, настоје да идентификују и анализирају критичне секторе, потсекторе, процесе и објекте коришћењем различитих методолошких и политичких приступа. Невероватна комплексност инфраструктурних система је дефинитивно највећи заједнички проблем свих земаља које су се упустиле у анализирање и идентификовање критичне инфраструктуре, као и оних које покушавају да формирају политику заштите критичне инфраструктуре. О овој комплексности инфраструктурних система говоре многи стручњаци из области заштите критичне

[133] Pursiainen, C., (2009), *The Challenges for European Critical Infrastructure Protection*, European Integration, vol. 31, no. 6, p. 723

инфраструктуре. Тако нпр. Рајнерман и Вебер[134] 2003. године закључују да инфраструктурни сектори истовремено обухватају већи број подсектора, грана индустрије, служби, производних области и имају специфичну вертикалну структуру (вишеслојну структуру која обухвата све аспекте инфраструктуре од локалних до глобалних). Други стручњаци посматрају критичну инфраструктуру као комплексни систем блиских међусовно повезаних елемената.[135] Неки стручњаци попут Луиса[136] (2006. године), Мотефа и Парфомака[137] (2004. године), Боина, Лагадека, Мајкл-Керјана и Овердајка[138] (2003. године) или пак Хелстрома[139] (2006. године) указују на опасност идентификовања свих инфраструктура као критичних услед нејасних граница између критичне и *некритичне* инфраструктуре. Ле Гранди Спрингисфелд[140] (2003.), Перебум[141] (2001. године), Боин, Лагадек, Мајкл – Керјан и Овердајк[142] (2003.) заједно указују на све јачу међуповезаност критичних инфраструктура (међусекторска повезаност). Све у свему, велики број стручњака[143] је сагласно да бројне ризике, претње и рањивости треба идентификовати пре него што се пређе на идентификовање критичних инфраструктура (КИ).

Општи циљ заштите критичне инфраструктуре (ЗКИ) и формирања политике ЗКИ је спречавање отказивања, несрећа и напада на било који елемент КИ. Политика ЗКИ обухвата концепте, стратегије, методологије, планове и организације које се баве превенцијом и реаговањем у случају постојања ризика, претњи, или рањивости КИ на било ком нивоу (локалном, регионалном, националном, међународном). Поменута сложеност процеса ЗКИ захтева развој мултидисциплинарне и интердисциплинарне

[134] Reinermann, D., and Weber, J., (2003), *Analysis of Critical Infrastructures: The ACIS Methodology*, Federal Office for Information Security, Bonn, Germany, p. 3
[135] Lewis, T.**,** (2006), *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Wiley Interscience, p. 29; Moteff, D. J., and Parfomak, P., (2004), *Critical Infrastructure and Key Assets: Definition and Identification*, Congressional Research Service, Library of Congress.
[136] Lewis, T.**,** (2006), *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Wiley Interscience.
[137] Moteff, D. J., and Parfomak, P., (2004), *Critical Infrastructure and Key Assets: Definition and Identification*, Congressional Research Service, Library of Congress.
[138] Boin, A., Lagadec, P., Michel-Kerjan, E., Overdijk, W., (2003), "Critical Infrastructures under Threat: Learning from the Anthrax Scare", *Journal of Contingencies and Crisis Management,* p. 100
[139] Hellstrom, T., (2007), *Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework*, National Emergency Training Center, p. 5
[140] Le Grand, G., Springinsfeld, F., Riguidel, M., (2003), *Policy Based Management for Critical Infrastructure Protection*. ACIP Project, Founded by the EU Commission, p. 2
[141] Pereboom, J., (2001), *Infrastructure Interdependencies: Overviews of Concepts and Terminology*, Infrastructure Assurance Center, Argonne.
[142] Boin, A., Lagadec, P., Michel-Kerjan, E., Overdijk, W., (2003), "Critical Infrastructures under Threat: Learning from the Anthrax Scare", *Journal of Contingencies and Crisis Management ,* p. 103
[143] Le Grand, G., Springinsfeld, F., Riguidel, M., (2003), *Policy Based Management for Critical Infrastructure Protection*. ACIP Project, Founded by the EU Commission, p. 5; Barry, E. C., *Infrastructure Vulnerability Assessment Model (I-VAM)*, Risk Analysis Vol. 27, No. 3

политике заштите. Комплексни проблеми захтевају свеобухватна решења, како у организационом, тако и у методолошком приступу. Стручњаци су констатовали да секторска анализа помаже у разумевању функционисања појединачних инфраструктурних сектора, процеса који се у њима одвијају и ресурса неопходних за њихово функционисање. Ипак, секторска анализа сама није довољна за холистичко разумевање већих инфраструктурних система у оквиру комплексног друштвеног контекста. Стога је неопходно развити смислену (одговарајућу) анализу, која се не би везивала за само један сектор.[144] У складу са тим ставом, неки стручњаци продложили су формирање свеобухватног система који би чиниле политике ЗКИ, интегралне стратегије и међуповезана спремност за реаговање у случају криза, а који би имао форму мреже, уз асиметричан приступ решавању проблема заштите ЗКИ,[145] или приступ код кога би се КИ посматрала као *систем састављен од низа других система*[146] или пак међусекторски приступ.[147]

Главни методолошки проблем овог последњег (који је касније прихваћен као најбољи метод за идентификовање критичне инфраструктуре) јесте како остварити међусекторски приступ у претежно дисциплинарно оријентисаном и секторски организованом друштву. Секторски приступ и приступ *од дна ка врху* се у заштити критичне инфраструктуре сматрају фундаменталним и најчешће се примењивао услед великих разлика у функцијама, структури, обиму и природи сваког инфраструктурног сектора. Ипак, модерна политика ЗКИ све више тражи усвајање хоризонталног приступа и тзв. приступа *од врха ка дну*, како би се превазишао мултиорганизациони и фрагментисани секторски приступ и како би се сви инфраструктурни сектори посматрали као целина са свим својим међузависностима. У области критичне инфраструктуре ово је изузетно значај заокрет у приступу јер постоји много међуповезаности између критичних инфраструктура (како позитивних, тако и негативних). Ипак, проблем примене овог приступа у условима велике сложености мреже критичних инфраструктура остаје актуелан.

---

[144] Dunn, M., (2004), Analysis of Methods and Models for CII Assessment in Myriam Dunn and Isabelle Weigert, International CIIP Handbook an Inventory and Analysis of Protection in 14 Countries, ETH – Swiss Federal Institute of Technology, Zurich, p. 227

[145] Michel-Kerjan, E., (2003), New Challenges in CI: A US Perspective, Journal of Contingencies and Crisis Management, Vol.11, No.3, p. 134; Auerswald, P., Branscomb, L., La Porte, T., and Michel-Kerjan E., (2005), The Challenges of Protecting CI, Issues in Science and Technology.

[146] Pereboom, J., (2001), *Infrastructure Interdependencies: Overviews of Concepts and Terminology*, Infrastructure Assurance Center, Argonne; Le Grand, G., Springinsfeld, F., Riguidel, M., (2003), *Policy Based Management for Critical Infrastructure Protection*. ACIP Project, Founded by the EU Commission, p. 3

[147] Hellstrom, T., (2007), *Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework*, National Emergency Training Center, p. 7

Литература везана за проблеме заштите критичних инфраструктура нуди неколико решења за примену поменутог свеобухватног приступа за анализу и идентификовање критичне инфраструктуре. Према устаљеном правилу, приликом утврђивања критичних инфраструктура најпре је неопходно обавити детаљно испитивање свих виталних националних сектора и са њима повезаних подсектора, уз тестирање свих тих сектора и подсектора на основу претходно утврђених критеријума.

Циљ интегралног међусекторског испитивања и међусекторског приступа је стварање увида у границе инфраструктурних сектора и формирање списка критичних инфраструктурних сектора и повезаних подсектора, на основу одређених критеријума.

Међусекторски приступ заснован је на претпоставци да се идентификовање виталних инфраструктурних сектора може постићи испитивањем одређеног броја кључних критеријума који се постављају пред сваки сектор, као што су:

1. Перцепција претњи, рањивости и ризика од стране одговорних менаџера, власника и оператера инфраструктуре,
2. Предвиђена штета по друштво коју би изазвало отказивање инфраструктурног сектора,
3. Временски период који протекне од тренутка кад дође до престанка функционисања инфраструктуре до тренутка избијања кризе,
4. Прекограничне последице престанка функционисања инфраструктуре,
5. Међузависност инфраструктурних сектора,
6. Критични објекти и географска област у којој су концетрисани,
7. Одговорност менаџера, власника и оператера инфраструктуре,
8. Власништво над инфраструктуром,
9. Законске основе,
10. Спроведене и планиране безбедносне мере.

Ови критеријуми су заправо најважније карактеристике критичних инфраструктура које треба анализирати. Подаци о овим критеријумима представљају за сваку државу кључне улазне податке на основу којих се формира политика ЗКИ.

Перцепција претњи, рањивости и ризика од стране одговорних менаџера, власника и оператера критичне инфраструктуре. Разумевање претњи, рањивости и ризика по критичну инфраструктуру (КИ) заправо представља разумевање негативних ефеката претњи, ризика и рањивости. Претње, ризици и слабе тачке КИ умањују поузданост инфраструктуре и стога директно и индиректно негативно утичу на друштво. Према једној од дефиниција претње, ризици и рањивости КИ представљају

кварове и престанак нормалног функционисања КИ услед интерних недостатака система и несрећа које се дешавају услед екстерних разлога.[148] Рањивости КИ су структурално усађене у састав КИ и уколико се изврши удар (напад) на те делове КИ, долази до престанка нормалног функционисања КИ и до несрећа.[149] Рањивости критичне инфраструктуре могу се умањити, али се не могу потпуно искоренити. Од екстерних претњи, најозбиљније и најчешће проучаване претње везане су за терористичке претње. Постоји више различитих методолошких приступа за мерење и процену претњи и ризика по критичну инфраструктуру. Међусекторски приступ фокусира се на испитивање перцепције претњи и ризика од стране кључних менаџера, власника и оператера критичне инфраструктуре. Перцепције претњи су од суштинског значаја за припрему и реакцију у случају отказивања КИ, без обзира на методологију. Праћење перцепција претњи из перспективе релевантних менаџера, власника и оператера битна је за проналажење и означавање критичних окидача у оквиру КИ.

Предвиђена штета по друштво коју би изазвало отказивање инфраструктурног сектора. Ефекат на друштво у случају отказивања сектора (прекида рада инфраструктуре) може бити директан и индиректан.[150] Директна штета односи се на моменталне ефекте отказивања инфраструктуре на становништво, економију, јавност и окружење. Процена штете врши се на основу три претпоставке: потпун прекид функционисања инфраструктуре, непостојање противмера, непостојање сценарија. Прва претпоставка је да се инфраструктура суочава са потпуним прекидом функције или са тоталним уништењем. У стварности то је скоро немогуће, али је с друге стране то једини добар начин да се утврди значај конкретне инфраструктуре за друштво. Друга претпоставка је да процена треба да се обави без претходне примене мера заштите. У стварности и то је скоро немогуће и увек постоји одређени скуп мера заштите, које имају задатак да спрече претњу и отказивање инфраструктуре. Ипак, узимање у обзир свих могућих и потенцијалних мера заштите инфраструктуре учинило би процену значаја инфраструктуре по друштво немогућом. Трећа претпоставка је да се процена значаја неке инфраструктуре по друштво треба да се ради без разматрања било каквог сценарија. Процена претњи и рањивости у пракси је углавном заснована на

[148] Le Grand, G., Springinsfeld, F., Riguidel, M., (2003), *Policy Based Management for Critical Infrastructure Protection*. ACIP Project, Founded by the EU Commission, p. 5

[149] Perrow, C., (1999), *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton, p. 4-5

[150] Индиректна штета представља врло широку категорију, која обухвата економске ефекте, симболичке, политичке и друге ефекте. Врло је тешко, ако не и немогуће, проценити индиректне ефекте помоћу тренутне методолошке апаратуре.

процени различитих сценарија. Ипак, у овом конкретном случају се никакав сценарио не узима у обзир и није важан. Важна је чињеница да је инфраструктура у потпуности престала да функционише. Процена негативних ефеката по друштво не укључује директне последице догађаја који су били окидач за престанак рада инфраструктуре, већ само последице нефункционисања инфраструктуре. На основу три наведене претпоставке добија се процена директне штете по друштво у случају престанка рада инфраструктуре, односно процена апсолутног друштвеног значаја одређеног инфраструктурног сектора. Међусекторски приступ идентификовања критичне инфраструктуре резултате ове процене значаја посматра кроз призму безбедности друштва (процењују се могући број настрадалих и број повређених, затим ефекат отказивања инфраструктуре на поверење јавности, затим ефекат отказивања инфраструктуре на јавни ред и мир, број погођених корисника инфраструктуре који су угрожени отказивањем, геополитички ефекат, ефекат на окружење, тј. на животну средину). Директна штета по друштво процењује се за период који није краћи од једног дана и није дужи од месец дана. Недељу дана се сматра најприкладнијим периодом времена за процену директних последица. Последице се потом рангирају на основу усвојених скала и категорија и тиме се коначно утврђује апсолутни друштвени значај инфраструктура. Неке међународне организације попут Европске уније настоје да идентификују своје регионалне критичне инфраструктуре применом врло сличних методолошких оквира. Критеријуми које користи ЕУ приликом процене значаја инфраструктуре укључују процену економских ефеката, евентуалних ефеката на животну средину и ефеката на јавност. Директива ЕУ из 2008. године наглашава да критеријуми који се користе за утврђивање значаја инфраструктурних сектора за друштво треба да рефлектују озбиљност утицаја који има уништавање или узурпирање рада неке инфраструтуре и да их треба одредити посебно за сваки случај (тј. посебно за сваку државу чланицу).

Индекс критичности рачуна се на основу категорија које се установљава приликом утврђивања значаја инфраструктуре за друштво (како је објашњено изнад) и требало би да рефлектује ниво критичности сваког сектора и подсектора. Индекс критичности представља збир процена штете по становништво, по економију, по јавност и по животну средину. Вредност индекса критичности креће се од 0 до 16. Како би се омогућило поређење критичности инфраструктура, рачуна се нормализовани индекс критичности. Овај индекс рефлектује релативну критичност одређеног

инфраструктурног сектора (критичност у односу на друге секторе) и креће се у опсегу од 0 до 100%.

Временски период који протекне од тренутка кад дође до престанка функционисања инфраструктуре до тренутка избијања кризе. Искуства свих држава везана за отказивања инфраструктуре указују на то да је битан фактор време. Наиме, важно је у ком тренутку, којој недељи и сезони се догоди квар и прекид функције неке инфраструктуре, а у ком тренутку то доведе до кризе. Прекид функције неких сектора би скоро моментално довело до озбиљних поремећаја у друштву и до криза, док прекид функционисања других сектора може много спорије да доведе до кризе. Према временском периоду који протекне од тренутка кад дође до престанка функционисања инфраструктуре до тренутка избијања кризе све инфраструктуре се могу поделити на оне чије отказивање доводи до кризе у периоду од 0 до 12 сати, затим у периоду од 12 до 48 сати, након два дана до једне недеље и инфраструктуре чије отказивање доводи до кризе тек након више од недељу дана.

Прекограничне последице престанка функционисања инфраструктуре. Националне КИ једне државе, у данашње доба су у све већој мери повезане са КИ тог истог типа у другим државама. Ефекти великих кварова и отказивања инфраструктура у једној држави могу да се пренесу на друге суседне државе, па чак и даље од тога. Стога, националне КИ представљају део јако комплексне међународне мреже. Баш из тог разлога се Европска унија током последњих 5-10 године озбиљно бави питањима прекограничних ефеката отказивања и кварова КИ. Директива Европске комисије о идентификовању европске критичне инфраструктуре (2008. године) настоји да идентификује КИ у свим државама чланицама, како би обезбедила бољу заштиту од прекограничних ефеката који су последица престанка рада КИ у једној земљи. ЕУ је дала и дефиницију тзв. европске критичне инфраструктуре (ЕКИ), која каже да ЕКИ обухвата ону КИ лоцирану у државама чланицама ЕУ чије узурпирање или уништење може да има значајан утицај на најмање две државе чланице. Међусекторска анализа бави се баш тим секторима.

Међузависност инфраструктурних сектора. Витални друштвени сектори су међусобно повезани и зависе једни од других, што доводи до стварања нових рањивости. Ометање функционисања једног сектора може да утиче и на функционисање других сектора, а такође важи и обрнути случај (међузависност). Истраживања у овој области указују да таква међузависност између сектора из дана у

дан расте,[151] да та међуповезаност постаје хијерархијски структурирана[152] и мултикатегоријска.[153]До увећа-ња међузависности дошло је услед потребе за повећањем ефикасности и услед примене нових технологија, пре свега информационих и телекомуникационих (ИКТ).[154] Хијерархијска природа међузависности везана је за секторску диференцијацију, односно за раслојавање сектора, при чему неки сектори постају *зависнији* од других. Бројна истраживања указују на то да сектор енергетике и сектор информационих и телекомуникационих технологија играју најбитнију улогу међу критичном инфра-структуром и да скоро сва остала КИ зависи од ових сектора. Зимерманова база података из 2004. године[155] о крос-секторским инцидентима у САД-у за период од 1990. године до 2004. године показала је да неке КИ више и чешће утичу на функционисање. других, него што друге КИ утичу на њих.

Могу се разликовати три категорије деструктивних међузависности између инфраструктура. *Каскадни ефекат* приликом отказивања инфраструктура односи се на ситуације кад прекид функционисања једне инфраструктуре изазива прекид функционисања друге инфраструктуре, док се *ескалирајући ефекат* односи на ситуације током којих прекид функционисања једне инфраструктуре додатно погоршава већ отежано функционисање друге инфраструктуре. Трећа категорија међузависности односи се на прекид функционисања више инфраструктура услед заједничког узрока који свој ефекат остварује на све инфраструктуре истовремено (нпр. природне катастрофе).[156]

---

[151] Boin, A., Lagadec, P., Michel-Kerjan, E., Overdijk, W., (2003), "Critical Infrastructures under Threat: Learning from the Anthrax Scare", *Journal of Contingencies and Crisis Management,* p. 100; Pereboom, J., (2001), *Infrastructure Interdependencies: Overviews of Concepts and Terminology*, Infrastructure Assurance Center, Argonne; Zimmerman, R., (2004), *Decision-making and the Vulnerability of Interdependent Critical Infrastructure*, IEEE Control Systems Magazine.

[152] Lewis, T.**,** (2006), *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Wiley Interscience.

[153] Pereboom, J., (2001), *Infrastructure Interdependencies: Overviews of Concepts and Terminology*, Infrastructure Assurance Center, Argonne, p. 20

[154] Кварови на рачунарима и на комуникационим системима били су извор многих отказивања и кварова на другим инфраструктурним системима. Примери за то су рецимо крах немачког Интерсити Експреса у јуну 1998. године, затим нестанак струје у САД-у и Канади у августу 2003. године, прекиди рада на многим аеродромима.

[155] Zimmerman, R., (2004), *Decision-making and the Vulnerability of Interdependent Critical Infrastructure*, IEEE Control Systems Magazine, p. 23

[156] Pereboom, J., (2001), *Infrastructure Interdependencies: Overviews of Concepts and Terminology*, Infrastructure Assurance Center, Argonne; Koubatis, A., and Schonberger, J. Y., (2005), *Risk Management of Complex Planning Framework*, Safety Science, p. 202

Међузависности нису униформна категорија с обзиром на то да се односе на просторне (географско) и функционалне (логичке,[157] сајбер[158] и физичке[159]) међузависности. Просторне међузависности односе се на просторну блискост једне инфраструктуре другој као најзначајнији услов за међузависност, док се функционална међузависност односи на ситуацију где је један тип инфраструктуре неопходан за функционисање друге инфраструктуре. Интензитет међузависности инфраструктура варира од случаја до случаја, мења се у зависности од комплексности односа инфраструктуре и може имати локалне, регионалне, националне и међународне димензије. Ове комплексне међузавис-ности и са њима повезани домино ефекти, упркос бројним научним и истраживачким радовима из ове области, остале су непотпуно разјашњене. Економски, здравствени и ефекти на животну средину нису у потпуности јасни.

Међусекторски приступ у идентификовању инфраструктура, настоји да идентификује мрежу међузависности између релевантних инфраструктура на основу скале:[160]

- 0 – нема међузависности између инфраструктура (0%−1%),
- 1 – постоји мала међузависност између инфраструктура (2%−33%),
- 2 – постоји умерена међузависност између инфраструктура (34%−66%),
- 3 – постоји висок степен међузависности између инфраструктура (67%−98%),
- 4 – постоји потпуна међузависност између инфраструктура, тј у потпуности зависе једне од других (99%−100%).

Стручњаци који су везани за конкретне секторе задужени су за процену степена међузависности подсектора на основу дефинисаних листа. Процена међузависности инфраструктура такође се обавља на основу три претпоставке: прекид рада инфраструктуре је потпун, противмере се не предузимају и не разматрају, непостојање дефинисаних сценарија за реаговање у оваквим ситуацијама. Међузависност инфраструктура која се на овакав начин утврди може се сматрати *чистом зависности*. На основу ових процена даље се могу формирати графикони међузависности. Сектори који су у највећој мери повезани са другима сматрају се и критичнијим.

[157] Појављују се код инфраструктура које су међусобно повезане преко финансијских тржишта.
[158] Појављују се код инфраструктура које користе електронске информационе и контролне системе.
[159] Јављају се кад једна инфраструктура користи материјална добра (производе и слично) других инфраструктурних сектора.
[160] Проценти се користе само као оријентир за одређивање степена међузависности.

Географске области у којима су концетрисани критични објекти. Критични сектори нису и не морају бити критични као целина. Неки објекти и службе критичних инфраструктура критичнији су од других. Након идентификовања таквих сектора треба их сагледати са географског аспекта. Теоретски гледано, критични објекти асиметрично су распоређени у простору. Најчешће су ови сектори концентрисани у урбанијим срединама. Процена је да је неких 80% ресурса концетрисано на 20% националне територије.[161] Прецизност ових процената мање је битна него само постојање асиметричног принципа. Међусекторски приступ покушава да изнађе такав критични (згуснути) распоред кри-тичних инфраструктура. Након идентификовања области у којима су инфраструктурни сектори скупљени, могућ је и заједнички приказ националне критичне инфраструктуре.

На основу објашњених критеријума међусекторске анализе може се формирати упитник о критичним инфраструктурама за било коју конкретну државу. Након формирања упитника у даљем раду везаном за идентификовање критичних инфраструктура апсолутно је неопходна сарадња свих актера у будућој заштити КИ: представника компанија, менаџера, оператера и власника инфраструктура, као и свих државих органа и администрације.

3.3.3. Класификација критичних инфраструктура

3.3.3.1. Енергетски системи

Енергетска инфраструктура покреће економију XXI века. Без стабилног снабдева-ња енергијом здравље као и економско благостање људи били би изузетно угрожени, а економије држава не би могле да функционишу. У скоро свим развијеним државама које имају своје програме заштите критичне инфраструктуре постоје документи и закони у којима се енергетика, односно енергетска инфраструктура дефинишу као апсолутно критичне. јер омогућавају функционисање свих осталих критичних инфраструктурних сектора. У највећем броју развијених држава запада сектор енергетике је великим делом у приватном власништву. Нормално функционисање сектора енергетике омогућава редовно снабдевање транспортне индустрије горивима, затим снабдевање становништва, послов-них простора и свих

[161] Lewis, T., (2006), *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Wiley Interscience, p. 17

грана индустрије струјом и свим осталим видовима енергије. Стога, енергетика представља есецијални елемент развоја и сваког вида производње.

Енергетика обухвата скуп свих компанија, идустријских организација и агенција које су укључене у процес производње и продаје енергије укључујући и оне које се баве екстракцијом, рафинирањем, дистрибуцијом и складиштењем нафте, затим екстракцијом, дистрибуцијом и складиштењем гаса, производњом, дистрибуцијом и складиштењем електричне енергије, рудном индустријом (само вађење угља), нуклеарном индустријом и обновљивим изворима енергије.

Сектор енергетике обухвата следеће подсекторе:

- Нафтна индустрија – нафтне компаније, нафтне рафинерије, транспорт горива и крајњи корисници,
- Индустрија гаса – екстракција природног гаса, прављење плина, дистрибуција и продаја гаса,
- Индустрија електричне енергије – генерација електричне енергије, њена дистрибуција и продаја,
- Рударска индустрија – рудници угља,
- Индустрија нуклеарне енергије,
- Индустрија обновљиве енергије – обухвата компаније које се баве алтернативним изворима енергије и одрживим изворима енергије, укључујући и компаније које се баве производњом хидроелектричне енергије, генерацијом енергије из ветра и генерацијом соларне енергије, као и компаније које се баве производњом и дистрибуцијом алтернативних горива,
- Традиционална енергетска индустрија заснована на сакупљању и дистрибуцији дрва за огрев (још увек присутан и чак врло заступљен подсектор енергетике, нарочито у сиромашним државама).

Постоје различите поделе критичне енергетске инфраструктуре у подсекторе, али се најчешће прихвата амерички модел по коме је она подељена на три међусобно повезана сектора: производња и пренос струје, производња и транспорт течних горива, производња и пренос природног гаса. Притом, подсектор производње струје може се додатно делити према начину на који се струја добија. Струја се може добити сагоревањем угља (како се добија највећи део струје и у Србији), затим из нуклеарне енергије у нуклеарним електранама, сагоревањем природног гаса, као и коришћењем

снаге воде у хидроелектранама, али и коришћењем снаге ветра и других обновљивих извора енергије (што није увек и свуда могућ начин добијања струје). У многим земљама је производња струје коришћењем угља најзаступљенији начин, при чему се угаљ транспортује од копова до постројења углавном железницом, што указује на значајну зависност производње струје од транспорта. Такође, у неким државама се сагоревање природног гаса користи за добијање електричне енергије, а гас се транспортује цевоводима, који су такође део транспортних система, што још једном указује на повезаност струје и транспорта.

Подсектор нафте и течних горива обухвата процесе истраживања, производње, складиштења, транспорта и рафинисања сирове нафте. Сирова нафта се рафинише у нафтни производ који се потом складиште и дистрибуирају кључним економским секторима широм државе. Најбитнији нафтни деривати су бензин, млазно гориво (керозин), мазут и течни нафтни гасови. Мали број држава успева да задовољи своје потребе за нафтом и нафтним дериватима, па их стога увозе (што се претежно обавља бродовима, где опет наилазимо на зависност енергетике од транспортног сектора).

Сектор природног гаса обухвата процесе производње, транспорта цевоводима, складиштења и дистрибуирања (а врло често и увоза).

Коришћење енергије било је кључно за развој људског друштва и у многоме је помогло друштву у контроли и прилагођавању животној средини. Менаџмент коришћења енергије неопходан је за нормално функционисање друштва. У новом индустрија-лизованом друштву енергетски ресурси постали су есенцијални за нормално функционисање пољопривреде, саобраћаја и транспорта, прикупљања отпада, као и за функционисање информационих технологија и комуникација, које су предуслов функционисања модерног друштва. Интензивније коришћење енергије, почев од индустријске револуције, донело је са собом и бројне озбиљне проблеме, као што је глобално загревање (које би у будућности могло у великој мери да угрози друштво).

Бројни геолози тврде да се резерве нафте и гаса полако исцрпљују и да ће доћи тренутак када ресурса више неће бити. То би могло да доведе до дестабилизовања светске економије, па и до ратова који би заменили трговину и постали једини начин за народе да обезбеде довољне количине воде, хране и енергије за себе. Такође, предвиђа се да ће се у скорије време, баш због проблема са нафтом и са гасом, вишеструко повећати тражња за угљем. Нуклеарној енергији се још увек поклања доста пажње као евентуалном одрживом извору енергије. На међународном нивоу

константно траје трка за енергетским ресурсима. Русија је виртуелно национализовала заједнички вентил за гас у Сахалинској области који би требало да контролише заједно са холандском компанијом Шел и већ је једном пре неколико година завртнула тај вентил и спречила доток гаса и нафте европским земљама.[162] Кина настоји да од западних играча на пољу енергетике преузме што више енергетских извора не би ли могла самостално да производи неопходне количине енергената и да се у том контексту осамостали. Овакво *такмичење* све мање мари за нуклеарне споразуме, уговоре о људским правима, хуманитарни развој и мирна решења.[163]

Приступ јефтиној енергији постао је изузетно битна ствар за функционисање модерних економија. Неравномерна дистрибуција енергије довела би до значајних проблема, а врло вероватно би се појавиле и прве претње по енергетску безбедност. Претње по енергетску безбедност могла би да представља политичка нестабилност неколико земаља које производе енергију, манипулисање енергетским залихама, такмичење око енергетских извора, напади на инфраструктуру ланаца снабдевања, као и несреће, природне катастрофе, финансирање страних диктатора и терориста, као и доминантно ослањање земље на стране резерве нафте.[164] Због оваквог огромног значаја неопходно је и квалитетно дефинисање и спровођење мера безбедности у области енергетике.

Ослањање свих грана индустрије на електричну струју и горива указује на зависност свих сектора критичне инфраструктуре од сектора енергетике. Зато је енергетски сектор и додатно рањив, па је неопходно подизање нивоа свести о ризицима у оквиру овог сектора, можда чак и на доста виши ниво у односу на неке друге секторе. Ово је скоро по правилу прихваћена идеја у свим земљама са развијеним програмима заштите КИ и стога све интензивно и континуирано раде на планирању заштите и побољшању готовости за реаговање у ванредним ситуацијама. Сарадња свих грана индустрије, размена информација и искустава и учествовање приватног и јавног сектора у заштити енергетске инфраструктуре од есенцијалног су значаја за успешно очување овог сектора. Последњих година све више пажње поклања се сајбер-безбедности, јер се сајбер-напади све чешће дешавају и могу да имају жестоке последице.

---

[162] Maitland, H., (2007), "*Critical Information Infrastructures Resilience and Protection*", Spronger, UK, Springer Science

[163] Tadjibayev, A. F., Sattarova, Y. F., (2009), *Categorization of Critical Infrastructures and Critical Information Infrastructures*, International Journal of Advanced Science and Technology, Volume 8, July, p. 20

[164] Power plays: Energy and Australia's security, October 2007.

Производња струје је у великој мери (у развијеним државама посебно) аутоматизована, па оператери у контроли процеса производње струје користе софистициране компјутерске системе, као и софистициране методе надзора и системе за прикупљање података, због чега у великој мери зависе од информационе инфраструктуре.

Централни орган држава који се бави заштитом КИ у сектору енергетике обично су министарства енергетике која су задужена за координацију свих активности које су везане за заштиту енергетске инфраструктуре. Такође, ова министарства контролишу и коорди-нирају процес размене информација и искустава између партнера из приватног и јавног сектора и баве се одређивањем ефективних мера заштите. Министарства енергетике, као и сви елементи енергетске инфраструктуре, нарочито у државама са развијеним системом ЗКИ сарађују са свим организацијама и секторима који су директно или индиректно повезани са енергетиком. У свету постоје различите организације које се упоредо са министарствима енергетике баве појединим сегментима процеса ЗКИ. Тако постоје разне регулаторне комисије за енергетику које доносе прописе о обавезама оператера и свих осталих који имају контакт са енергетском инфраструктуром, затим постоје организациије (асоцијације) које се баве проценама ризика у енергетском сектору, централни органи који се баве заштитом свих критичних инфраструктура, као и разне агенције држава на које би могло да има утицај отказивање енергетских система у конкретној држави и које понекад и зависе од тих система. Све ове организације морају да функционишу складно и координисано и у томе лежи најтежи задатак министарстава енергетике у било којој држави, када се ради о заштите енергетске инфраструктуре.

Пракса је у развијеним државама да сваки подсектор сектора енергетике има и посебна тела која су задужена само за заштиту тих сектора, а сва та тела наравно налазе се у склопу министарстава енергетике. Тако нпр. у САД-у постоји Савет за координацију активности у подсектору електричне енергије, у чији састав улазе власници и оператери КИ и који редовно одржава састанке на којима се разматрају проблеми координације активности у оквиру подсектора и иницијативе које би требало да унапреде отпорност КИ (како физичке, тако и сајбер-инфраструктуре, тј. информационе инфраструктуре) у оквиру подсектора. У оквиру подсектора нафте и природног гаса, у САД-у постоји Савет за координацију активности у овим подсекторима, а слични органи постоји и у другим западним земљама. Овај Савет оформиле су трговачке асоцијације за нафту и природни гас, у намери да помогну

координацију иницијатива и активности, да унапреде партнерства и сарадњу свих власника и оператера као и сарадњу приватног и јавног сектора.[165]

На нивоу влада држава, сем министарстава енергетике и централних тела за заштиту свих КИ, у области заштите енергетске инфраструктуре могу да постоје и координациона тела влада за енергетски сектор, која уско сарађују са министарствима.

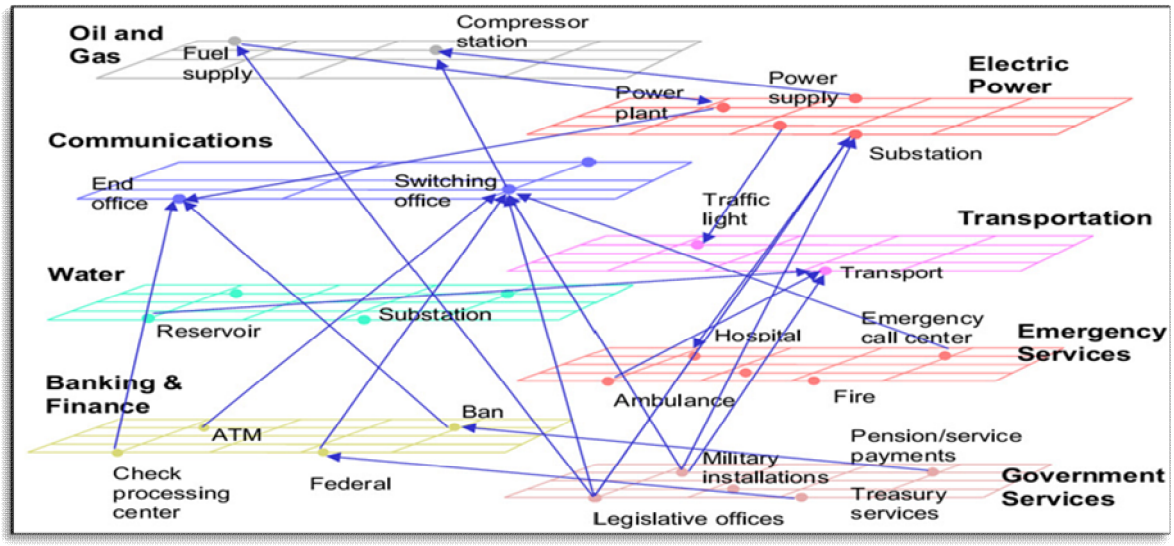
Ова координациона тела могу да заказују састанке (форуме) са представницима приватног сектора ради размене информација, дискутовања тренутних иницијатива и договарања нових. Скоро идентичан систем ових савета који постоји у САД-у постоји и у Немачкој и у Великој Британији. Разлика је само у томе што у САД-у централно тело за заштиту свих КИ у свим секторима представља *Department of Homeland Security*, док у Немачкој централну улогу у заштити КИ игра Министарство унутрашњих послова. Одређивањем ових централних тела за заштиту свих КИ омогућено је обједињавање рада свих поменутих већа, која сем што обављају активности у оквиру својих подсектора, сада могу да под окриљем централних тела за заштиту КИ у земљи, изнесу и упореде своје резултате и проблеме и да квалитетније размењују информације и искуства.[166]

3.3.3.2. Телекомуникације

Телекомуникационе мреже се на свим нивоима сматрају неодвојивим делом друштвене интеракције. Треба посебно нагласити да комплетна електронска комуникациона инфраструктура која се састоји од *комуникационих мрежа*, *дистрибуираних рачунарских система*, *софтвера* и *апликација* игра кључну улогу у унапређењу укупног знања и технологије. Захваљујући њеној могућности да окупи *критичну масу* људи, идеја и инвестиција, она на различите начине доприноси напретку на свим нивоима друштвеног и економског живота. Из тог разлога, телекомуникациона инфраструктура представља веома важну имовину и средство које мора бити заштићено и неопходно је да се препозна као део националне критичне инфраструктуре. Заштита ових мрежа од напада и природних непогода, које могу довести до недоступности мрежних сервиса, веома је битан аспект који се не сме занемарити.

[165] Видети шире на интернет адреси: http://www.dhs.gov/energy-sector 17.11.2012

[166] Department of Homeland Security in Cooperation with Department of Energy, National Infrastructure Protection Plan – Energy Sector, 2010



Слика бр. 3.1. – Приказ међузависности критичних инфраструктурних сектора[167]

Дефинисање телекомуникационе инфраструктуре као и критичне телекомуникационе инфраструктуре већина европских држава базира на искуствима и донетој регулативи Европске Уније, САД-а и земаља у региону. Као битан елемент у дефинисању КИ као и критичности појединачних сектора (у овом конкретном случају критичност сектора телекомуникација) треба нагласити постојеће зависности између критичних инфраструктура различитих сектора (слика бр. 3.1.). Кроз разматрање процене ризика од различитих напада усмерених ка телекомуникационој инфраструктури (малициозних, природних катастрофа и сл.), може се уочити неопходност регулисања и заштите сектора телекомуникација и корака које треба предузети.

Телекомуникациона инфраструктура једне земље је *комплексан скуп система* који укључују *велики број технологија и сервиса*, а које се налазе у власништву више ентитета (државе, приватних компанија). Инфраструктура обухвата *жичне, бежичне, кабловске и технологије за емитовање, језгрене мреже базиране на интернет протоколу као и интерне информационе системе.*[168] Многе телекомуникационе компаније/оператори које поседују и управљају телекомуникационом инфраструктуром су током времена имплементирале мере заштите од природних катастрофа и незгода у оквиру својих архитектура уводећи редундантне чворове и системе, бизнис планове и стратегије за санацију након напада или природних

[167] Извор: Lane, B., "Federal Communications Commission". http://transition.fcc.gov/pshs/techtopics/techtopics19.html 17.11.2012

[168] Gospic, N., Muric, G., and Bogojevic, D., (2012), "Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia," in International Conference on Applied Internet and Information Technologies, Zrenjanin, October.

непогода. То указује да и поред данашњег веома конкурентног пословног окружења због повезаности и међузависности мрежа различитих оператора/сервис провајдера, сви чиниоци телеком сектора једне земље треба да сарађују, јер проблеми у функционисању мреже једног учесника на тржишту често могу да утичу на мрежу која је у власништву неког другог.

Како је највећи део телекомуникационе инфраструктуре у власништву приватног сектора, битно је установити заједнички стратешки оквир којим ће се осигурати заштита телекомуникационе инфраструктуре једне земље и осигурати њена безбедност.

Вођени општом трансформацијом и конвергенцијом технологија почетком двадесет првог века сектор телекомуникација и ИТ-а су постали практично нераздвојиви. Телекомуникациони сектор не укључује само физичке елементе као што су жичне, бежичне, кабловске и сл. технологије, већ и сервисе као што су интернет саобраћај и рутирање, информационе сервисе и мреже кабловске телевизије. Самим тим, компоненте комуникационе инфраструктуре које су у власништву државе и приватних компанија су нераскидиво повезане у оквиру ових физичко-логичких структура.

У дефинисању телекомуникационе инфраструктуре, уобичајено је да се за основу узима оно што је Међународна унија за телекомуникације (*International Telecomunication Union* – ITU) дефинисала. Међутим, у оквиру фамилије ITU није дефинисана критична телекомуникациона инфраструктура, иако многи документи које издаје Унија за телекомуникације помињу потребу заштите критичне телекомуникационе инфраструктуре (PP-10 Rec. 130, PP-10 Rec. 174, ITUCS/Art.38, ITUCS/Art. 34, ITUCS/Art. 35). Хармонизација која је урађена у оквиру ITU-T сектора серијама препорука E.408-409 и X.805 и X.1051 дефинише захтеве за безбедност, оквире и смернице за идентификацију претњи, смањивање ризика, организацију у случају инцидента и архитектуру сигурности за системе који пружају *крај-крај* (*end-to-end*) комуникацију. И друге стандардизационе организације као што су Међународна стандардизациона организација (*International Standardization Organization* – ISO), ZGPP и ZGPP 2 (*Group for Partnership for Third Generation*) такође не дају дефиниције критичне телекомуникационе инфраструктуре већ само оквире за сигурност система мобилних комуникација и управљачких система.

Начин дефинисања критичне телекомуникационе инфраструктуре у многоме зависи од контекста у ком се посматра не само критична телекомуникациона

инфраструктура већ и друге КИ у некој земљи. Да би се дефинисала КТИ, као основа се могу користити опште дефиниције КИ. У том смислу КТИ се може дефинисати као јавна или приватна мрежа која преноси информације релевантне за националну безбедност или информације велике материјалне вредности. У физичком смислу КТИ може бити дефинисана као целокупна мрежа или део мреже преко које се преносе информације од велике важности.

3.3.3.3. Саобраћај

Транспорт представља кретање људи, животиња и добара са једне локације на другу. Постоје следећи модови транспорта: ваздушни, железнички, друмски, водни, путем цевода и *свемирски*. Читава област коју покрива саобраћај може се поделити на три посебне целине: 1) инфраструктура, 2) возила и 3) операције. Транспорт је за сваку државу током историје, као и данас, изузетно битан сектор. Он представља предуслов за развој трговине, а она опет предуслов за формирање цивилација.

Саобраћајну и транспортну инфраструктуру чине: фиксне инсталације, неопходне за функционисање саобраћаја и транспорта – путеви, пруге, ваздушне и пловне руте, канали, цевоводи и свемир. Сем тога, у транспортну инфраструктуру спадају и терминали попут аеродрома, аутобуских станица, железничких станица, складишта, затим бензинске пумпе и луке. Терминали се могу користити за размену путника, размену карга, или пак ради одржавања возила. У путничком транспорту, терминали су тачке интегри-сања различитих видова саобраћаја (нпр. железница или метро који може да пролази испод аеродрома служи за повезивање аеродрома са центром града). Терминали за аутомобиле су паркинг места, а аутобуси имају своје обележене станице. За теретни саобраћај и транспорт терминали су тзв. *тачке претовара*, мада се данас практикује да се превоз карга транспортује *point-to-point* системом. Финансирање инфраструктуре може да буде јавно или приватно. За функционисање друмског, железничког, кабловског и транспорта путем цевовода, неопходно је претходно изградити инфраструктуру. За ваздушни и водни саобраћај није потребно изградити *путеве*, али је неопходно имати одређену фиксну инфраструктуру и терминале. Путеви, а у неким земљама и пруге и аеродроми, граде се и путем опорезивања. Извођење нових инфраструктурних пројеката скоро по правилу се врши кроз узимање кредита. Баш због тога, многи власници инфраструктуре уводе корисничке таксе (аеродромске таксе, таксе на наплатним рампама на путевима). Путнички транспорт може бити јавни (где оператер пружа одређене претходно

договорене услуге) и приватни. Теретни транспорт у свету углавном се фокусирао на превожење контејнера. Транспорт је битан сегмент сваког друштва који поред економског значаја има и негативне аспекте будући да узрокује велико загађење ваздуха и заузима велики део површине читаве планете, које онда не могу да се користе ни за коју другу активност. Циљеви планирања саобраћаја данас су успостављање ефикасног саобраћајног протока и заустављање процеса ширења градова. У контексту заштите критичне саобраћајне инфраструктуре, сем физичке инфраструктуре, критичним се у сегменту саобраћаја и транспорта могу сматрати и операције везане за обављање и планирање јавног транспорта.

Према америчком закону о критичној инфраструктури, критични сектор саобраћаја и транспорта чини седам подсектора (односно модалитета), што је врло често прихваћена подела критичних инфраструктура у области критичног сектора саобраћаја и транспорта и у другим државама на западу:[169]

1. Ваздухопловна инфраструктура, која укључује авионе, системе за контролу лета, аеродроме, хелипортове и полетно-слетне стазе. У критичну инфраструктуру авијације такође се у САД-у убрајају и војни аеродроми, хелипортови, кратке полетно слетне стазе и ваздухопловне базе.
2. Путна инфраструктура друмског саобраћаја, коју чине коловози, мостови, тунели, возила (аутомобили, мотори, камиони и друга комерцијална превозна средства).
3. Инфраструктура водног саобраћаја, коју чине обала, луке, водни путеви, екслузивне економске зоне и интермодалне конекције са друмским саобраћајем, као и сви типови бродова који се користе за пловидбу.
4. Инфраструктура масовног транспорта и путничке железнице, које чине аутобуси, путнички возови, систем метроа, лаке пруге, тролејбуси и трамваји, дуге пруге, као и сама мрежа пруга.
5. Систем цевовода, који чини огромна мрежа цеви које се простиру дуж читаве државе преносећи скоро целокупну количину природног гаса која прође кроз државу, као и већи део опасних течности и разних хемикалија.
6. Инфраструктура теретне железница, коју чине систем пруга, теретни вагони, превозници терета, локомотиве и

[169] Видети на: https://www.dhs.gov/transportation-systems-sector 17.11.2012

7. Инфраструктура поштанских служби и служби за доставу пакета. Служба за доставу пакета се посебно наводи заједно са поштанским службама, а не у склопу превозника терета – карго превозника (теретне железнице и сл.) јер своје операције фокусира углавном на доставу поштанских пошиљки, публикација и малих и средњих пакета.

Међународна експанзија система друмског, водног и вадушног саобраћаја последица је политичке стабилности и економских трговинских споразума. Постојање и заштита националних транспортних система једне државе добар су показатељ снаге и организованости читаве државе. На националном нивоу, стање у ком се налази транспортни систем може бити врло добар показатељ стања у ком се држава налази. Јаке државе по правилу имају добре транспортне системе и ефикасне алтернативе функционисања система у случају да дође до отказивања система. Приватизација железничких и друмских саобраћајница није тако редак случај у свету. Истина, тиме се у многоме мења начин функционисања транспорта. Основу живота и рада људи (појединаца) у данашњем друштву између осталог представља и ефикасан транспортни систем.

Такође треба нагласити да је добар део терористичких напада (а посебно оних највећих размера) у последњих 15-ак година, био усмерен на различите елементе транспорта. Од терористичких напада у САД-у 2001. године, преко напада у Лондону и Мадриду, до напада на аеродром Домодедово у Русији, различити модели транспорта врло су атрактивна мета за терористе. Сви ови напади указали су на велики број недостатака у обезбеђивању транспорта. Такође, треба рећи и да је окидач за формирање читаве једне области у истраживању безбедности, која се бави заштитом критичне инфраструктуре, био терористички напад на САД из 2001. године, током ког је отето четири авиона. Зато је и заштита КИ у САД-у отпочела увођењем много ригорознијих мера провере на аеродромима и у авионима.

3.3.3.4. Вода

Цивилизације су током историје скоро по правилу ницале око река и великих водних путева.[170] Тако је на пример Месопотамија, тзв. колевка цивилизације, била ситуирана између две велике реке Тигра и Еуфрата, док је Стари Египат у потпуности зависио од Нила. Велике метрополе попут Ротердама, Лондона, Монтреала, Париза,

[170] Gleick, P. H., ed., (1993), Water in Crisis: A Guide to the World's Freshwater Resources, Oxford University Press, p. 13, Table 2.1. "Water reserves on the earth".

Њујорка, Буенос Ајреса, Шангаја, Токија, Чикага, и Хонгконга дугују свој развој рекама и воденим површинама крај којих се налазе, које су им и омогућиле да постану трговински центри. Острва са безбедним лукама, попут Сингапура, доживела су процват такође захваљујући трговини која се обављала водним путевима. У областима света као што су Северна Африка и Средњи исток, где су залихе воде оскудне и недовољне, успостављање приступа води и нормализација снабдевања чистом водом за пиће представља главни приоритет у плановима развоја ових подручја.

Вода је природни ресурс који у неким деловима света постаје дефицитиран, па стога доступност и снабдевање чистом водом за пиће постају главни социјални и економски проблеми. Тренутно око милијарду људи на планети свакодневно пије воду која није здрава за пиће. На самиту групе Г8 2003. године (Евиан самит) већина земаља прихватила је циљ да се до 2015. године број људи којима чиста вода за пиће и за купање није доступна преполови.[171] Лош квалитет воде и лоша санитарна ситуација су смртоносни. Око пет милиона људи умре сваке године због конзумирања загађене воде. Светска здравствена организација процењује да би постојање довољних количина безбедне воде могло да спречи да 1,4 милиона деце умре сваке године.[172] Вода се још увек не може сматрати ресурсом кога има у ограниченим количинама с обзиром на то да је има свуда и да ¾ површине планете чини вода, али начини на које би се вода пречишћавала као и начини снабдевања водом морају у будућности бити доста побољшани. На свету постоје релативно мале количине воде за пиће у виду резерви, што је необновљиви ресурс, и може се рећи да је пре дистрибуција воде за пиће и наводњавање проблем, него што је проблем сама количина воде на планети.

У неразвијеним деловима света 90% свих отпадних вода одлази без икаквог третирања и пречишћавања у реке и потоке.[173] Око 50 земаља, у којима живи трећина светске популације, такође имају мање или веће проблеме са снабдевањем водом, а 17 земаља троше више воде годишње него што је произведу у својим водоводима.[174] Све ово има негативан утицај како на површинске воде (реке, језера) тако и на подземне воде.

---

[171] G8 Action plan decided upon at the 2003 Evian Summit: http://www.g8.fr/evian/english/navigation/2003_g8_summit/summit_documents/water_-_a_g8_action_plan.html 17.11.2012

[172] World Health Organization, Safe Water and Global Health: http://www.who.int/features/qa/70/en 17.11.2012

[173] UNEP International Environment, Environmentally Sound Technology for Wastewater and Stormwater Management: An International Source Book, 2002.

[174] Nijavali, H. R., Sathaye, A. J., (2002), *Climate Change and Developing Countries*, Springer.

Пре 50 година постојало је схватање да је вода непресушни ресурс. У то време на свету је живело мање од половине данашњег броја људи. Истраживањем је утврђено да преко 1,2 милијарде светског становништва живи у зонама у којима постоји физичка несташица воде, односно где нема довољно воде за задовољење свих потреба. Даље је утврђено да 1,6 милијарди људи живи у областима у којима постоји економска несташица воде, односно где нема довољно инвестиција у воду или где не постоји довољно људских капацитета, што чини немогућим задовољење потреба за водом. Истраживањем је утврђено да ће бити могуће производити потребне количине хране у будућности, али да ће наставак данашњег темпа производње хране заједно са утицајима околине довести до криза у многим деловима света. Како би се избегла глобална криза у снабдевању водом, фармери ће морати да повећају продуктивност како би задовољили растуће потребе за храном, док ће индустрија и градови морати да нађу ефикасније начине коришћења воде.[175]

Између воде и безбедности појединаца, заједнице, нација и читавог света постоји комплексна веза. Витална улога воде у свакодневном животу и економским активностима додатно наглашава важност воде за безбедност и стабилност у свету. Водни ресурси и снабдевање водом блиско су повезени са политичким одлукама и екстремним типовима конфликата који могу да ескалирају у насиље, тероризам или рат.

П. Глајк даје хронолошки преглед конфликата везаних за воду кроз историју, уз категоризовање конфликата зависно од разлога и умешаних учесника. Према овој категоризацији постоје следећи типови конфликата:[176]

- Сукоби државних и недржавних органа око контроле снабдевања водом или приступа водним ресурсима (конфликти око контроле водних ресурса),
- Државе користе водне ресурсе и водне системе као оружје током војних акција (конфликти у којима се вода користи као средство ратовања),
- Државни и недржавни органи користе водне ресурсе и водне системе за остваривање политичких циљева (конфликти у којима се вода користи као средство за остваривање политичких циљева),
- Недржавни чиниоци користе водне ресурсе или водне системе као мету или средство за насиље или средство принуде,

[175] Chartres, C., and Varma, S., (2010), Out of water - From Abundance to Scarcity and How to Solve the World's Water Problems FT Press (USA)
[176] Gleick, P., (2000), "Water Conflict Chronology (September 2000 Version)", Pacific Institute http://www.worldwater.org/conflict.htm 17.11.2012

- Државе користе водне системе као мете за војне акције (конфликти у којима се вода користи као војна мета),
- Државни и недржавни органи расправљају о води и водним ресурсима у контексту економског развоја (конфликти у којима је вода предмет расправе о развоју).

И у историји после Другог светског рата постоје примери да су се водни ресурси користили као стратешки циљеви током војних конфликата:[177]

- САД су бомбардовале системе за наводњавање у северном Вијетнаму током шездесетих година прошлог века и уништиле 661 насип,
- Израел је у два напада уништио новоизграђени канал Источни Гор у Јордану због сумњи да је Јордан преусмерио ток реке Јармук (1969. година),
- Ирак је претио бомбардовањем сиријске бране ал-Таврa, наводећи као разлог да је изградњом бране редукован проток воде реке Еуфрат у Ираку (1974. године),
- НАТО је прекинуо снабдевање водом у Београду током бомбардовања СР Југославије 1999. године.

Критични сектор вода у већини развијених држава са развијеном критичнином инфраструктуром и системом одбране инфраструктуре чине два посебна система: водовод (систем снабдевања чистом пијаћом водом) и канализација (систем отпадних вода). Критични сектор вода подложан је различитим нападима и ризицима, укључујући контаминацију смртоносним агенсима, физичке нападе на системе водовода и канализа-ције, испуштање токсичних хемикалија у велике колекторе воде, али и сајбер-нападе. Уколико се овакви сценарији остваре, може доћи до великих епидемија разних болести, до смрти већег броја људи, или пак до дужег престанка функционисања читавог критичног сектора (што такође може да представља огроман проблем, како по здравље људи, тако и по економију државе чији је сектор вода угрожен). Други критични сектори и критичне службе попут ватрогасних и служби хитне помоћи и медицинске неге, као и сектори енергетике, хране (односно хране и пољопривреде, који у већини развијених држава заједно чине критични сектор хране), транспортни системи (односно саобраћај у целини као критични сектор) и други, услед велике међузависности од сектора вода би претрпели велике штете уколико би дошло

[177] Friedman, T. L., (2002), Longitudes and Attitudes: Exploring the World After September 11. New York: Farrar Straus & Giroux.

до било каквог напада на критични сектор вода или прекида нормалног функционисања овог сектора.[178]

Безбедност пијаће воде и правилан и одговоран третман отпадних вода апсолутно су неопходни за нормално функционисање модерног друштва. Постојање безбедне пијаће воде предуслов је за све људске активности (физичке, економске и културне). Правилан треман отпадних вода важан је ради превенције болести и заштите околине. Стога је са становишта јавног здравља и економских утицаја неопходна потпуна заштита система за прераду и снабдевање пијаћом водом, као и система отпадних вода, као и инфраструктуре коју ови системи користе, а која се без икакве сумње мора сматрати критичном и која једним називом чини критични инфраструктурни сектор вода.

У развијеним земљама обично постоји огроман број система за снабдевање пијаћом водом, као и система отпадних вода, при чему је највећи део становништва (проценат опет зависи од развијености државе, доступних средстава за спровођење система до крајњих корисних и других фактора) прикључен и потпуно зависан од нормалног функционисања ових система.[179]

Критични сектор вода најчешће чине и приватни и јавни системи за снабдевање пијаћом водом и системи за третман отпадних вода. Овај сектор, без обзира на то што се многи други критични сектори налазе потпуно у приватном власништву, још увек је у доста земаља контролисан у доброј мери од стране државе. Такође, државе учествују кроз разна своја тела у контроли функционисања и заштити система вода. То су углавном разне службе, агенције и други типови организација за еколошку заштиту околине, које функционишу под окриљем државе. Пример такве организација је америчка Агенција за заштиту животне средине (*Environmental Protection Agency* - EPA). У Србији не постоји тело које се директно бави критичним сектором вода, већ су задужења подељена између неколико организација и министарстава (Министарство пољопривреде, шумарства и водо-привреде, Србија воде, Војводина воде, Министарство здравља, некадашње Министарство за заштиту животне средине, водоводи и канализациони системи градова у Србији итд). Ово систем контроле и заштите сектора вода у Србији чини тежим него у другим државама. Главни задатак

[178] Видети на: https://www.dhs.gov/water-and-wastewater-systems-sector 17.11.2012

[179] Примера ради – у САД-у постоји 160.000 јавних система за снабдевање пијаћом водом који заједно чине огромну водоводну мрежу, као и преко 16.000 система за третирање отпадних вода. Више од 84% људи у САД-у прикључено је на водоводни систем, док је око 75% америчке популације повезано на канализациону мрежу.

тела задужених за критични сектор вода је развијање, промовисање и имплементација безбедносних програма, којима би се унапредила способност читавог сектора да делује превентивно против разних ризика, затим способност да детектује, одговори и опорави се од било ког типа напада, природне непогоде или било ког другог типа опструкције нормалног фукционисања.[180]

План заштите сектора вода и оквирни план управљања ризицима по сектор вода спроводи у свакој земљи централно тело које се бави заштитом КИ (у Немачкој, као и многим другим државама Европе је то Министарство унутрашњих послова, у САД је Министарство унутрашње безбедности (DHS – *Department of Homeland Security*), земље Азије опет имају своја специјализована тела која су задужена за заштиту КИ) и организације (тела) која су задужена за конкретне секторе (у овом случају организације задужене за управљање ризицима и заштиту сектора вода).

Процес формирања и спровођења плана заштите КИ има неколико стандард-них корака, који су заједнички за све критичне инфраструктуре:[181]

1. Постављање безбедносних циљева који се желе постићи,
2. Идентификовање постројења, мрежа и система критичне инфраструктуре које треба заштитити,
3. Процена ризика по критичну инфраструктуру, која се обавља на основу три фактора:
   - анализе последица, што је обично одговорност специјализованих тела за сваки конкретан сектор, уз надзор централног тела за заштиту КИ,
   - процена рањивости, што је такође у надлежности специјализованих тела за сваки конкретни сектор,
   - анализа претњи, коју обављају централна тела за заштиту КИ у сарадњи са другим органима државе (полицијом, обавештајним агенцијама и другим),
4. Постављање приоритета у оквиру сектора критичне инфраструктуре (што је основа за алокацију ресурса),
5. Имплементација програма заштите КИ,
6. Утврђивање ефективности мера заштите КИ.

Као део програма заштите конкретне КИ, свака специјализована организација за свој сектор формира план заштите КИ у складу са претходно наведеним корацима, при

[180] Видети на: http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/water.htm 17.11.2012
[181] Ibid

чему се стално обавља мониторинг мера заштите и континуирано шаље повратна информација (*feedback*) о успешности спроведених мера не би ли се унапређивале мере које не постижу жељене резултате.

У складу са наведеним корацима у оквиру сектора вода специјализоване организације постављају безбедносне циљеве као што су очување и заштита јавног здравља и животне средине, препознавање и редуковање ризика, одржавање одговарајућег степена отпорности инфраструктуре у оквиру сектора вода, унапређење комуникације и повећање поверења јавности. Тако, на пример, у оквиру америчког система заштите КИ, и конкретно, у оквиру критичног сектора вода дефинисани циљ (визија) је: "безбедна и отпорна инфраструктура у оквиру система вода, која осигурава довољну количину чисте воде за пиће, која је критични елемент неопходан за опстанак друштва. Такође циљ је осигурање економске виталности и јавног поверења у националне системе пијаће воде и отпадних вода кроз вишеслојну одбрану и унапређење готовости за реаговање у било којој ванредној ситуацији у којој би инфраструктура у оквиру сектора вода била угрожена".[182]

Слика бр. 3.2. Континуирани процес унапређења заштите критичне инфраструктуре[183]

[182] http://cfpub.epa.gov/safewater/watersecurity/legislation.cfm 17.11.2012
[183] Department of Homeland Security in Cooperation with Environmental Protection Agency, Water – Critical Infrastructure and Key Resources, Sector-specific plan as Input to the National Infrastructure Protection Plan-Executive Summary, May 2007, p. 2

Процес идентификовања постројења, мрежа и система критичне инфраструктуре обављају специјализована тела за критичне инфраструктуре у оквиру сектора вода у сарадњи са централним телом за заштиту КИ у држави, као и у сарадњи са свим релевантним приватним и државним операторима и власницима критичне инфраструктуре. Кроз ову сарадњу утврђују се релевантни елементи сектора вода који се морају заштити, при чему се пролази кроз неколико фаза:[184]

1. Дефинисање критичне инфраструктуре и елемената критичне инфраструктуре у водном сектору, које обавља специјализовано тело задужено за заштиту КИ у оквирну сектора вода.
2. Прикупљање података – податке о критичној инфраструктури и рањивим тачкама у оквиру инфраструктуре сакупљају власници/оператери КИ (делова водовода и канализације), а затим те податке шаљу специјализованим телима за заштиту КИ у оквиру сектора вода.
3. Верификовање података – након пријема података о критичној инфраструктури, специјализована тела би требало да још једном обаве проверу тих података да би се тек након тога означили одређени елементи инфраструктуре као критични.
4. Задатак специјализованих тела је и да редовно прикупљају податке о новим инфраструктурама у оквиру водног сектора и да редовно ажурирају базу података о критичним инфраструктурама.

Након идентификовања КИ врши се процена ризика у три корака: кроз процену претњи, рањивости и последица отказивања критичне инфраструктуре из било ког разлога. Приликом процена евентуалних последица отказивања критичне инфраструктуре која је везана за снабдевање водом или за третирање отпадних вода, треба најпре обратити пажњу на низ међузависности које постоје између те и других критичних инфраструктурних сектора. Наиме, огроман број критичних инфраструктурних сектора директно или индиректно зависи од вода, што је прва ствар која указује на последице које може да има отказивање КИ у оквиру сектора вода. Приликом процене последица такође се узимају у обзир димензије последица до којих долази услед отказивања система, број оболелих или преминулих услед проблема са КИ, утицај који све то има на поверење јавности, економски ефекат догађаја, као и

[184] Department of Homeland Security in Cooperation with Environmental Protection Agency, Water – Critical Infrastructure and Key Resources, Sector-specific plan as Input to the National Infrastructure Protection Plan-Executive Summary, May 2007. p. 6-8

разни други индикатори, у зависности од разлога, озбиљности и природе догађаја. Приликом процене рањивости указује се на карактеристике постројења, локације, положаја, процеса и операција које се одвијају у оквиру сектора вода, а које критичну инфраструктуру чине подложном разарањима, онеспособљавању, нападима, отказивањима и сл. Процена претњи захтева квалитетну координацију и сарадњу централног тела за ЗКИ са полицијом и обавештајном службама (кад је реч о процењивању вероватноће терористичких напада), као и са разним другим службама (метеоролошким, осигуравајућим и др). Сектор вода врло је изложен различитим типовима претњи, могућности терористичких напада увек постоје, као и могућност природних непогода, а такође опасност представљају и људске грешке.

Након процене ризика одређују се приоритетни елементи критичне инфраструктуре. Овај процес обављају централна тела која се баве заштитом КИ, при чему значајну улогу играју и сви елементи у ланцу заштите КИ, јер најпре власници/оператери КИ морају да на одговарајући начин пошаљу информације о свим елементима критичне инфраструктуре, како би централно тело могло да изврши поређење свих тих елемената и одреди оне који представљају приоритете кад је у питању ЗКИ.

После одређивања приоритета у оквиру сектора вода развијају се и примењују програми заштите критичне инфраструктуре у оквиру сектора. Током овог процеса, пажња се поклања и идентификовању, процени, одабиру и имплементацији програма заштите, а улога специјализованих тела за заштиту КИ у оквиру сектора вода је у највећој мери да координишу имплементацију. Програм заштите је заправо план координисаних акција, којима се врши превенција, детекција и спречавање било какве опструкције критичне инфраструктуре, али и опоравак и обнова критичне инфраструктуре, уколико се проблем ипак догоди и последице терористичког напада, природне катастрофе или пак људских грешака, не спрече. Програмима заштите предлажу се оператерима и власницима КИ најефективније стратегије за заштиту постројења, укључујући критичне компоненте. У оквиру сектора вода праве се посебни програми заштите за различите терористичке нападе (био тероризам, терористички напади на постројења итд.), програми за реаговање у случају природних катастрофа, програми за реаговање у случају људских ненамерних и намерних грешака (саботажа). У оквиру описа сваког програма заштите, одговорна тела издају и објашњења начина на који ће конкретни програм заштите променити перформансе читавог сектора, као и начина на који би програм требало да делује на остварење постављених циљева.

Примену програма заштите КИ прати мониторинг успешности примењених мера, и то од стране свих учесника, почев од оператера/власника КИ, преко специјализованих тела за заштиту КИ у оквиру сектора вода, па све до централног тела за ЗКИ на нивоу државе, при чему се сарадња ових елемената ни у једном тренутку не прекида. Циљ праћења ефективности мера је њихово стално прилагођавање и унапређивање, уколико се покаже да такве какве су тренутно не дају одговарајуће (жељене) резултате.

Такође, на крају овог разматрања треба се осврнути и на раније помињане међузависности сектора вода са другим критичним инфраструктурним секторима. Вода је од есенцијалног значаја за опстанак људи, за људске здравље, за опстанак економије, као и за функционисање многих јавних служби, које се у многим државама такође сматрају критичним инфраструктурним сектором. Било која штета која се нанесе инфраструктури у оквиру сектора вода стога утиче на све критичне секторе, који зависе од воде, а такође оваква узрочно-последична веза може да постоји и у супротном смеру. У свим земљама са развијеним програмима ЗКИ вода проглашена је критичном инфраструктуром, а њена заштита представља један од најбитнијих државних приоритета.

3.3.3.5. Храна

Храна је после воде најбитнија људска потреба, па је самим тим нормално и апсолутно логично означити производњу хране као критични сектор.

У великом броју држава храна (целокупан процес производње хране) и пољопривреда спојени су у један критични сектор. Овај сектор се скоро по правилу налази у приватном власништву и чине га пољопривредна имања, ресторани и постројења за производњу, прераду и складиштење хране и прехрамбених производа. Економска стабилност скоро свих држава у свету зависи од стабилности овог сектора, јер он њега долази добар део укупних државних прихода.

Критични сектор хране има критичне међузависности са многим секторима, али посебно је повезан са следећима:

1) Системи за снабдевање чистом пијаћом водом и за третман отпадних вода (због неоходности наводњавања пољопривредног земљишта чистом водом),
2) Транспорни системи тј. саобраћај и транспорт (јер је неопходно транспортовати производе, стоку, храну и прерађевине на разне дестинације),

3) Енергетски системи, струја и течна горива су неопходни за функционисање пољопривредних машина, као и машина које се користе за прераду и производњу храну,
4) Финансијске службе и
5) Хемијска индустрија (производња разних хемикалија које се користе у пољопривреди за заштиту биља и пољопривредних култура).

Као што је случај са сваком другом КИ, у државама са развијеном заштитом критичне инфраструктуре постоји централно специјализовано тело које се бави заштитом конкретних КИ (у овом случају заштитом хране и пољопривреде) и на крају власници/оператери критичних инфраструктура. Најчешће се овим сектором баве министарства здравља и пољопривреде и организације и агенције које функционишу под њиховим окриљем.[185] Министарства пољопривреде задужена су за снабдевање становништва храном, као и за заштиту и промовисање пољопривредне производње и здраве хране. Такође, министарства пољопривреде задужена су углавном и за контролу безбедности пољопривредних производа и за заштиту и промоцију здравог начина живота. Министарства све ове дужности обављају у сарадњи са другим државним органима (најпре са главним органима задуженим за заштиту КИ), са разним локалним агенцијама, академским институцијама, здравственим институцијама, са власницима пољопривредних добара и са потрошачима. Скоро по правилу министарства пољопривреде у сарадњи са министарствима здравља регулишу и проверавају и увоз прехрамбених производа и њихов квалитет. Такође, исправност прехрамбених производа у ресторанима и разним типовима продавница регулишу по свету разне организације, које блиско сарађују или се налазе под окриљем министарстава пољопривреде.

У неким земљама, попут САД-а, формирају се и Савети за координацију активности у оквиру сектора, који се састају неколико пута годишње, организују форуме на којима учествују представници приватника и представници држава, а на

[185] Тако су на пример у САД-у за пољопривреду задужени Одељење, тј. Министарство за пољопривреду (*Department of Agriculture*) и Одељење, тј. Министарство здравља и јавних служби (*Department of Healthand Human Services*), као и Администрација за храну и лекове (*Foodand Drug Administration*), док је у нашој земљи (без обзира на то што Србија нема Закон о КИ као ни дефинисан програм заштите КИ као такве, пољопривреда и производња хране морају на одређени начин бити заштићене) то дужност Министарства пољопривреде, шумарства и водопривреде и Министарства здравља, као што је случај и у Немачкој, с том разликом што у Немачкој постоји и неколико одељења која су задужена само за заштиту КИ у сектору пољопривреде и производње хране. Такође, треба напоменути да се изнад ових министарстава, кад је у питању ЗКИ налазе *Department of Homeland Security* (DHS) у САД-у и Министарство унутрашњих послова у Немачкој.

којима се обавља размена информација и договарају разне акције из области заштите КИ у сектору хране и пољопривреде. Ови савети олакшавају сарадњу приватног и јавног сектора, учествују у доношењу, имплементирању, спровођењу и унапређењу безбедносних програма и процедура, подстичу размену информација и искустава и врше процене безбедности пољопривредне производње и производње хране. Такође на нивоу држава са развијеним системом заштите могу и одвојено од ових савета или упоредо са њима да постоје форуми и платформе, сличне већ поменутим, на којима приватни и јавни сектор обављају највећи део својих договора о заштити КИ.[186]

Државе, као и већ поменути органи држава (министарства, агенције и разне друге организације) формирају дугорочне и средњорочне програме, којима се планира увођење неких новина у област заштите КИ у оквиру сектора хране и пољопривреде. У великом броју држава се због недовољних буџета врши приоритизација између различитих критичних сектора, при чему се, последњих пар година, фаворизује сектор пољопривреде и производње хране као један од најбитнијих. Сектори који се фаворизују добијају веће износе за заштиту КИ и уопштено за развој. Такође, и програми ЗКИ који се праве чешће су посвећени фаворизованим секторима. Тако је у САД-у настао програм за процену критичности одређених елемената у оквиру сектора пољопривредне производње и производње хране. Задаци овог програма су између осталог идентификовање елемената и система у оквиру сектора који су критичнији од осталих, проналажење приоритетних елемената и система у оквиру сектора, формирање база података о уоченим ризицима по КИ у оквиру сектора, формирање предлога будућих активности у области заштите КИ у сектору пољопривредне производње и производње хране.[187] Овај програм настао је 2011. године, и у том тренутку је био једини у свету, мада сада и Велика Британија и Немачка раде на програмима који су јако слични овом. Као део процеса заштите КИ у оквиру сектора пољопривреде и хране, у доста држава спроводе се вежбе у којима учествују сви који су укључени у рад сектора, почев од највиших државних органа, преко разних центара и савета, до индустријских постројења за прераду пољопривредних постројења и производњу хране као и пољопривредних произвођача. Вежбе за циљ имају успостављање одговарајућег система деловања у ванредним ситуацијама као што су контаминација хране или пољопривредних производа или ширење биљних или

[186] Department of Homeland Security, National Infrastructure Protection Plan – food and Agriculture Sector (snapshot), 2010, p. 2
[187] Ibid

животињских болести и штеточина. Овакве вежбе дају увид у могуће начине координисања акција, сарадње и комуникације свих елемената у оквиру сектора пољопривредне производње и производње хране.

У свим до сада помињаним земљама о овој проблематици постоје и документи намењени запосленима, у виду упутстава и приручника, којима се прописује шта све представља индикаторе сумњивих активности у поменутом сектору.

4. БЕЗБЕДНОСНИ РИЗИЦИ И ПРЕТЊЕ КРИТИЧНИМ ИНФРАСТРУКТУРАМА

4.1. Појмовно одређење безбедносних ризика и претњи

Проблем безбедности КИ постепено постаје један од приоритета савременог друштва. Учестали инциденти, као и кривична дела усмерена проотив КИ, алармирали су стручну и ширу јавност и покренули бројна правна, социолошка и безбедносна питања на која до сада није пружен задовољавајући одговор.

Критична инфраструктура у Србији (која још увек није законом дефинисана) представља огледало озбиљне економске и социјалне кризе. Све сложенија безбедносна проблематика везана за критичну инфраструктуру последица је нарушеног стања безбедности друштва. Традиционални методи за очување безбедности инфраструктуре више нису довољни и зато унапређење безбедности КИ мора да буде брига свих субјеката у друштву, који ће у зависности од својих објективних могућности, али и развијености безбедносне културе, тиме дати свој допринос.[188]

У традиционалном дискурсу разматрања проблема безбедности КИ уочени проблеми се повезују са специфичностима функционисања КИ које су погодне за различите типове напада и због којих је критична инфраструктура подложна различитим типовима ризика.

Безбедност КИ подразумева стање заштићености интегритета КИ, као и оператера, власника и свих осталих који су директно или индиректно заслужни за функционисање КИ, а и заштићеност од оштећења или уништења постројења критичне инфраструктуре. Пошто је, због сложености данашњих система, генерално немогуће елиминисати све хазарде, реалан циљ је развој система са прихватљивим ризицима. Овај циљ се може постићи минималним трошковима ако се мере заштите примене што раније, још у фази стварања система. То се постиже идентификовањем потенцијалних

[188] Papa, M., and Shenoi, S., (2008), *Critical Infrastructure Protection II – Emergent Risks in Critical Infrastructures*, International Federation for Information Processing, New York, p. 3-17

опасности, процењивањем ризика и примењивањем корективних радњи како би се елиминисале идентификоване опасности или смањили ризици.

Бројна истраживања везана за безбедност КИ дају само делимичан увид у разне облике угрожавања безбедности КИ. Иако истраживања идентификују неке ризике по КИ, У Србији никад није спроведено истраживање усмерено на идентификовање ризика којима су изложене критичне инфраструктуре. Такође, не постоје ни теоријски нити емпиријски показатељи на основу којих би могли да се идентификују сви безбедносни ризици по КИ и да се систематизују према одређеним критеријумима. У свету се о овим питањима већ доста говори, и постоји велики број различитих размишљања и класификација ризика.

Основни појмови везани за угрожавање безбедности КИ су: претња, ризик, хазард, рањивост (вулнерабилност).

Претња безбедности је све оно што представља извор опасности и има могућност да нанесе озбиљну штету лицима, имовини, друштву или држави.[189] Претња је неко или нешто што има могућност да науди националним интересима једне државе и да оствари нежељени догађај. Када се ова могућност актуелизује, она престаје да буде претња и постаје догађај попут других. У тренутку када је претњу уочена она постаје део ризика, а као таква, и предмет расподеле њиховог времена и расположивих ресурса (људских, техничких, финансијских итд.) ради супротстављања.[190]

Претња представља јасно и непосредно изражену намеру и/или способност да се неко или нешто повреди, уништи, казни итд. [191] Политика националне безбедности увек зависи од перцепције претњи које постоје у односу на националне интересе и представља развијање могућности заштите од истих.[192]

Бројне дефиниције појма ризик у домаћој и страној литератури указују да је ризик (итал. risico) могућа опасност. Ризиковати значи изложити се (излагати се) опасности.[193] Под ризиком се подразумева вероватноћа или могућност опасности, губитка, озледе или неке друге штетне последице.[194] Ризик је и могућност да се

[189] Baldwin, D. A., (1971), "*Thinking about Threats*" Journal of Conflict Resolution, Vol. 15, no. 1, March, 70-78
[190] Путник, Н., (2009), *Сајбер простор и безбедносни изазови*, Београд, Факултет безбедности, стр. 62
[191] Daasse, C., and Kessler, O., "Knowns and Unknowns in the War in Terror: uncertainty and the political contruction of danger".
[192] Milburn, T. W., and Watman, K. H., (1981), *On the Nature of Threat: a Social Psychological Analysis*, New York: Praeger.
[193] Московљевић, М., (2006), *Речник савременог српског књижевног језика с језичким саветником*, Гутенбергова галаксија, Београд, стр. 577
[194] *Consise Oxford Dictionary*, Ninth edition, Claredon Press, Oxford, 1997, p. 866

одређени циљ не оствари у потпуности или да се оствари делимично. Могућност отклањања или смањења ризика зависи од нивоа познавања појаве у којој је садржан одређени ризик.

Појам ризик представља универзалан и специфичан облик опасности по безбедност било ког објекта безбедности, независно од тога да ли је у поседу субјекта безбедности или субјекта опасности. Наиме, извориште заштите (одбране) сваког објекта безбедности је у одлучивању, а доносити одлуке значи излагати се ризику. Таквој опасности излажу се обе стране у конфликту: субјект безбедности доноси одлуку ради оптималне заштите свог објекта безбедности, а субјект опасности доноси одлуку да на најефикаснији начин угрози безбедност, односно изазове промене на дотичном објекту безбедности.[195]

Анализа ризика пружа улазну информацију о оцени ризика и одлукама да ли ризици треба да се решавају и које су то одговарајуће (најприхватљивије) стратегије у третирању ризика. Анализа ризика обухвата разматрање узрока и извора ризика, њихових позитивних и негативних последица, као и вероватноћу појављивања тих последица. Такође, могу се идентификовати и фактори који утичу на појаву последица и вероватноћу њиховог појављивања. Ризик се анализира тако што се одређују последице и вероватноћа њиховог настанка, као и остале особине ризика.[196]

Идентификација и анализа ризика представљају део ширег процеса процене ризика (*risk assessment*), односно управљања ризиком (*risk management*). *Процена ризика* је саставни део процеса управљања ризиком и представља свеобухватни процес идентификовања потенцијалних опасности, анализе и оцене ризика.

Заједнички именитељ наведених дефиниција ризика јесте неизвесност и могућност губитка КИ. Неизвесност постоји онда када се не може са сигурношћу знати исход одређеног догађаја. Када ризик постоји, морају постојати бар два могућа исхода. Најмање један од могућих исхода мора да буде непожељан. То може да буде губитак у смислу да је нешто што је било у саставу КИ инфраструктуре оштећено (изгубљено), затим то може да буде губитак који је већи од пројектованог или пак добитак који је мањи од пројектованог. Уопштено, као битна карактеристика ризика може се навести могућност да се претрпи штета.

[195] Мијалковски М., Ђорђевић И., (2006), *Ризик – Специфичан облик угрожавања безбедности*, Универзитет у Београду, Факултет безбедности.
[196] Кековић, З., Савић, С., Комазец, Н., Милошевић, М., Јовановић, Д., (2011), *Процена ризика у заштити лица, имовине и пословања*, Центар за анализу ризика и управљање кризама, Београд, стр. 108

Хазард се дефинише као могући извор опасности, физичких или операционих услова, са потенцијалом који може да произведе одређену врсту негативних последица.[197] У стручној литератури среће се појам физичких хазарда, који представљају материјалне услове средине који утичу на учесталост и степен губитка имовине, као што су локација, конструкција и инсталације, као и начин коришћења објеката и опреме.[198]

Вулнерабилност је слабост одређене особе, групе или система, односно слабост критичне инфраструктуре или њених елемената услед које они постају изложенији ризику од наступања нежељеног догађаја који може резултовати нарушавање физичког или психичког интегритета појединаца односно стања система.[199]

4.2. Врсте безбедносних ризика и претњи критичним инфраструктурама

Идентификација и процена ризика са којима се суочава КИ је први корак у изградњи успешне стратегије унапређења безбедности и процеса њихове заштите. Разумевање узрока безбедносних проблема и њихово повезивање са манифестацијама угрожавања широког спектра, а не само оних које су кривично или прекршајно санкционисане, може помоћи да се изврши идентификовање безбедносних ризика који утичу на стање безбедности КИ.

Идентификовање ризика подразумева процес проналажења, прописивања и карактерисања елемената ризика релевантних за циљеве управљања, односно процену ризика. Неопходно је идентификовати изворе ризика, догађаје или низ околности, као и њихове потенцијалне последице. Свеобухватна идентификација и регистровање ризика је од суштинске важности јер се ризик, који у овом стадијуму није идентификован, искључује из даље анализе. Идентификација би требало да укључи све ризике без обзира на то да ли су под контролом или нису.[200]

Ипак, иако се безбедносни ризици по КИ могу класификовати на различите начине, несумњиво је да се многи од њих међусобно прожимају или су каузално условљени. Без обзира на критеријум класификације, неке ризике није могуће сврстати

[197] Ibid, 176
[198] Ibid, 28
[199] Bankoff, G., (2006), Maping Vulnerability, Earthscan, London, 2004.; Thywissen, K., *Components of Risk: A Comparative Glossary*, Source 2; Villagran, J. C., (2006), *Vulnerability – A Conceptual and Methodological*, Review, Source 4.
[200] Кековић З., Савић С., Комазец Н., Милошевић М., Јовановић Д., (2011), *Процена ризика у заштити лица, имовине и пословања*, Центар за анализу ризика и управљање кризама, Београд, стр. 107

у само једну категорију, док се поједини често не могу уклопити ни у једну класификациону класу. Стога се сматра да се не могу утврдити универзално важећи и непроменљиви класификациони критеријуми већ да се морају изградити флексибилни оријентациони критеријуми чија ће се садржина мењати у зависности од конкретних варијетета и специфичних просторних, временских и фактора средине.[201]

Безбедносна пракса подразумева и формирање листе ризика који морају бити укључени у сваку класификацију која ће имати употребну вредност и чија се конкретна садржина може допуњавати и мењати у зависности од фактора који доводе до промене постојећих и евентуалне појаве нових ризика, као и у зависности од типа критичне инфраструктуре. Пре приступања класификацији безбедносних ризика треба указати на чињенице које свака листа ризика мора да уважи.

Прво, под ризиком треба подразумевати све чиниоце који могу довести до угрожавања нормалног функционисања КИ и нормалног обављања дужности од стране оператера, као и власника КИ, социјалну климу и интерперсоналне односе између свих људи неопходних за функционисање КИ, као и обезбеђеност објеката, техничких и информационо-комуникационих система и осталих средстава, и правила функционисања самог процеса КИ. Затим, треба водити рачуна о томе да су ризици међусобно условљени и испреплетени и да промене временских, просторних и фактора средине, односно окружења доводе до појаве нових и промене постојећих ризика. Другим речима, ризици су варијабилна категорија, тако да редуковање једне врсте ризика може да доведе до настајања новог или до повећања вероватноће остварења другог ризика, што не би требало занемарити у процесу анализе, идентификације и класификације ризика. Треба напоменути да приступ идентификацији и класификацији ризика мора бити заснован на објективности, систематичности и непристрасности, с тим да је пожељно узети у обзир субјективне доживљаје свих одговорних за нормално функционисање КИ о степену и врсти угрожавања, па је препоручљиво процес идентификације и класификације ризика прилагодити специфичностима једне КИ, њеног окружења и локалне заједнице. У идентификовању и класификовању ризика врло су битне релевантне и ажуриране информације и посебна стручна знања.

Фактори који доводе до ризика морају се хијерархијски градирати, на основу чега се врши њихова приоритизација. Њихови извори могу бити интерни и екстерни, тј.

[201] Ibid

ризици могу да настану услед: више силе, људског фактора (намерно или ненамерно) и техничко-технолошких дисфункција.

Да би се смањио ризик и ограничиле последице природним и људским факторима иазваних катастрофа по критичну инфраструктуру, повећала отпорности друштва и КИ неопходно је најпре детектовати потенцијалне безбедносне ризике и претње. Постоји неколико претњи које се могу сматрати најбитнијим за данашњу критичну инфраструктуру, како на националном, тако и на глобалном нивоу. Међу њима се истичу тероризам[202] (као глобална претња свим државама), сајбер-криминал[203] и све врсте незаконитих ометања информационих и комуникационих инфраструктура али и бројне природне (елементарне) непогоде, које су услед константних климатских промена све чешће у свим деловима света. [204]

Сем наведених постоји и низ других претњи по нормално функционисање критичне инфраструктуре које у мањем броју случајева изазивају последице великих димензија. У такве претње спадају: отказивања система (техничке грешке), дефектан драјвер или грешке у софтверу који се користи у оквиру неког инфаструктурног сектора, лоше планирање активности у оквиру сектора (људски фактор), несмотреност оператера критичном инфраструктуром, неадекватна кооперација или координација активности, разни облици саботаже, криминале актвности.

4.3. Класификација безбедносних ризика

Класификација безбедносних претњи и ризика по критичну инфраструктуру може се извршити на више начина. Тако, на пример, могуће их је на основу порекла поделити у три изоловане категорије:[205]

1. Елементарне непогоде,
2. Грешке унутар система инфраструктуре, које се могу даље према пореклу узрока поделити поделити на:
   - Оне до којих доводи људски фактор − лоше планирање активности у оквиру сектора, несмотреност оператера критичном инфраструктуром, неадекватна кооперација или координација активности, и

[202] Simon, S., Benjamin, D., (2000), *New Terrorism in America*, Taylor & Francis, New York
[203] Clarke, R., Knake, R., (2010), *Cyber War – The next treat to National Security and What to do about it*, Harper Collins e-books, p. 87
[204] Закон о ванредним ситуацијама Републике Србије, Министарство унутршњих послова.
[205] La Porte, T. R., (2007), *Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise*, Volume 15 Number 1, March

- Оне до којих долази из техничких (технолошких) разлога − отказивања машина, дефектан драјвер или грешке у софтверу који се користи у оквиру неког инфаструктурног сектора,

3. Напади на систем критичне инфраструктуре, где би могла да се направи дистинкција између физичких (директни терористички напади, саботаже) и виртуелних (сајбер-напади). Такође у оквиру ове категорије могли би се као претња рачунати и могући ратови.

По општем значају и утицају на организацију, Кајч Д. дели ризике на три категорије.[206] У прву категорију спадају ризици више силе, у које се убрајају све природне катастрофе које имају утицаја на организацију. Последице догађаја које се сврставају у групу ризика више силе (потреси, поплаве, пожари) могу бити у распону од потпуно безначајних до оних погубних. У другу категорију Кајч Д. сврстава политичке и економске ризике, које дефинише као промене у политичком и економском окружењу организације. Трећа категорија састављена је од свих ризика који настају у самој организацији, на које сама организација има највише утицаја. Заједничким именом називају се пословним ризицима, а деле се на организационе ризике, ризике пословања и финансијске ризике.

Сви ризици који утичу на сигурност људи, имовине и пословања, у ширем смислу, представљају безбедносне ризике, без обзира на то да ли су природно или друштвено условљени. Када је извор ризика људски фактор, онда се говори о ризицима који се могу поделити на намерне и ненамерне. Ненамерни се везују за могућност настанка људске грешке, као последица умора, немара, непажње и сличних околности. Намерни ризици су ризици од криминала и они се могу поделити на високофреквентне – некатастрофичне ризике и нискофреквентне – катастрофичне ризике. У високофреквентне ризике се убрајају криминални догађаји или прекршаји, чији се тренд испољава са одређеном дозом статистичке правилности, иако кумулативно могу довести до катастрофалних последица, што је иманентно другој групи – катастрофичних ризика, какви су на пример терористички.

Могућа је и подела безбедносних ризика према изворима настанка, предвидивости и утицају техничког фактора. Према изворима настанка ризици се могу поделити на интерне (крађе од стране запослених, разни облици општег, имовинског, привредног или еколошког криминала) и екстерне (напади на имовину, лица и

[206] Keitsch, D., (2000), *Risiko management*, Schaffer-Poeschel, Stuttgart.

пословање споља). Према предвидивости ризици се могу поделити на непредвидиве или тешко предвидиве (утицај законских прописа из области безбедности и заштите, природне несреће и опасности, политичко-безбедносни ризици) и предвидиве (активности конкуренције, пореска политика). Са аспекта утицаја техничког фактора, ризици се деле на: техничке (повреде на раду, пожари, експлозије и друге опасности) и нетехничке (људске грешке, обуставе рада).

Са становишта безбедности, битна је подела на: чисте и спекулативне ризике. Да би постојао чисти ризик, потребно је да постоји вероватноћа да се неки губитак деси. У области безбедности и заштите многи чисти ризици се односе на удесе настале деловањем техничког фактора и они су најповољнији са аспекта предвиђања, односно прикупљања података од значаја за процене, па и примене одговарајућих стратегија смањења ризика (нпр. осигурања). Спекулативни ризици представљају могућност и добитка и губитка, али и ону тачку пресека где се организације, у већој мери свесне предности него недостатака, усуђују да ризикују.

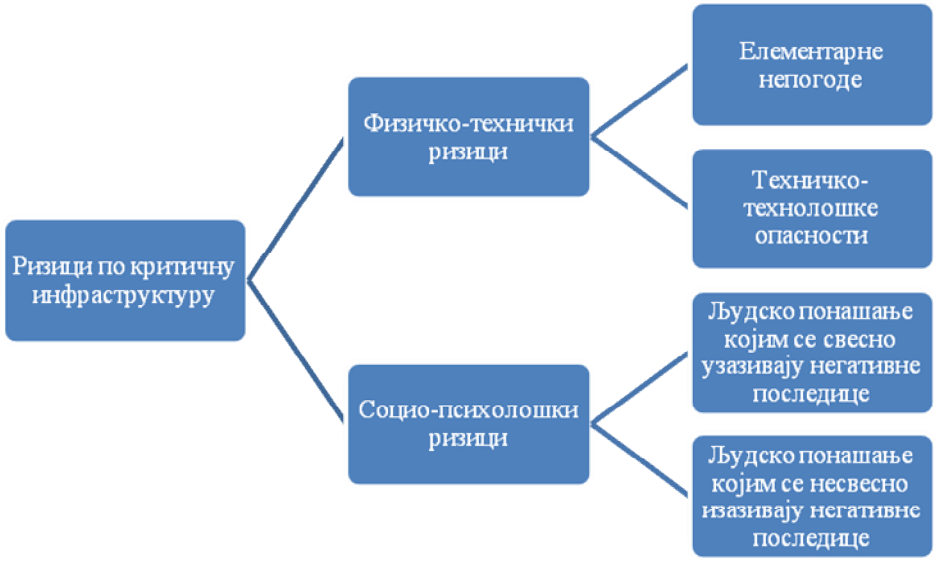
Ипак, категоризација заснована на подели свих безбедносних ризика на две основне класификационе групе - физичко-техничке и социо-психолошке, чини се да је теоријски и практично корисниja и чешће коришћена.

Под безбедносним ризицима физичко-техничке природе подразумевају се могућности угрожавања КИ услед елементарних непогода (земљотреси, поплаве, обилне падавине, ваздушна струјања) или техничко-технолошких опасности (пожари, хемијска контаминација).[207]

Социо-психолошки безбедносни ризици односе се на квалитет социјалне климе која је уско везана са функционисањем КИ. Под ризике социо-психолошке природе сврставају се различите ситуације које могу да наруше позитивну социјалну климу и тиме угрозе функционисање КИ. Идентификација социо-психолошких ризика захтева анализу неколико елемената:[208]

- квалитета интерперсоналних односа свих људи чије су активности директно или индиректно везане за КИ,
- перцепције нивоа безбедности КИ од стране оператера и власника КИ и
- постојања програма превенције и редукције ризика по КИ.

[207] Papa, M., and Shenoi, S., (2008), *Critical Infrastructure Protection II – Emergent Risks in Critical Infrastructures*, International Federation for Information Processing, New York, p. 3-17
[208] Ibid



Слика 4.1. – Класификација безбедносних ризика по критичну инфраструктуру[209]

У оквиру основних класификационих група (физичко-технички и социо-психолошки безбедносни ризици) може се даље вршити гранање на подгрупе. У том смислу, група физичко техничких ризика би обухватила подгрупе *елементарне непогоде* и *техничко-технолошке* опасности, док би група социо-психолошких ризика обухватала подгрупе *људско понашање којим се несвесно изазивају негативне последице* и *људско понашање којим се несвесно изазивају негативне последице*. Основни критеријум овакве поделе ризика је извор ризика. Под безбедносним ризицима физичко-техничке природе сматрају се они ризици који потичу од природних сила (елементарне непогоде) или од техничко-технолошких опасности (пожари, хемијска контаминација). Социо-психолошки безбедносни ризици могу потицати из два извора: људског понашања свесно усмереног ка изазивању одређених негативних последица (криминално деловање, други облици девијантног понашања, интерперсонални конфликти, злоупотреба информационих система) или људских грешака које доводе до негативних последица (грешке у пројектовању, инсталацији и одржавању инфраструктуре, непостојање надзора и контроле, непримењивање процедура, протокола и техничких правила и стандарда, неадекватна организација и насавесно вршење послова).

Једну од тешкоћа приликом сваког покушаја класификације безбедносних ризика представља чињеница да је број претњи које могу угрозити КИ практично

[209] Ibid

неограничен, због чега их је веома тешко све предвидети. Другим речима, свакој класификацији се може замерити одређени степен непотпуности. Зато идентификација претњи захтева наглашену опрезност будући да се претња која није била идентификована често може показати као катастрофална. Из тог разлога се поставља и питање избора адекватног методолошког приступа, посебно зато што у вези са овим проблемом ни на нивоу теорије још не постоји јединствено решење. Са друге стране, неизбежно је разврставање безбедносних претњи у групе које, у извесном смислу, представљају логичке целине јер то омогућава њихову анализу, што је неопходан корак за формулисање сваке политике заштите.

Ипак, сматра се да постоје ризици који се нужно морају укључити у сваку листу ризика која настоји да буде научно заснована, објективна и практично применљива. Постоји схватање да је најбољи приступ онај који не инсистира на строгом разврставању безбедносних ризика у тачно одређене и статичне категорије већ уважава њихову динамичност, испреплетеност и варијабилност. Полазећи од ових премиса, састављена је горња листа која укључује све релевантне безбедносне ризике, при чему остаје флексибилна и широка како би могла да укључи њихове различите модалитете, као и евентуалне нове врсте.

Прегледи релевантних истраживања упућују на закључак да су тзв. информатички ризици (који претежно спадају у категорију социо-психолошких ризика) готово потпуно занемарени, што с обзиром на савремене тенденције развоја и процес информатизације друштва представља озбиљан недостатак досадашњих класификација. Чињеница да истраживачи нису посветили одговарајућу пажњу феномену који задире у све токове друштвеног живота, указује на недовољно разумевање социо-психолошких реперкусија информационог друштва.

5. ПРЕГЛЕД ПОЛИТИКА ЕУ И ТЕХНОЛОШКИ РАЗВИЈЕНИХ ЗЕМАЉА НА ПОЉУ ЗАШТИТЕ КРИТИЧНИХ ИНФРАСТРУКТУРА

5.1. Програм Европске уније за заштиту критичних инфраструктура

Европска унија је један од кључних фактора на међународном нивоу кад је у питању заштита критичне инфраструктуре. Стога је ЕУ покренула низ иницијатива и истраживачких програма како би се проучили различити аспекти заштите и претњи по критичну инфраструктуру, као и утицаји које оштећивање критичних инфраструктура има на образовање, привреду, здравство, комуникације и многе друге сегменте људске делатности.

Терористички напади и проблеми са електромрежом показали су да оштећење или потпуни губитак инфраструктуре у једној од држава ЕУ може да има негативан утицај на већи број земаља, као и на европску економију у целини. Стога је Европски савет затражио од Европске комисије да припреми целокупну стратегију и акциони план за побољшање заштите европске критичне инфраструктуре (ЕКИ). Већ 20.10.2004. године Комисија је усвојила документат под називом "Заштита критичне инфраструктуре у борби против тероризма", који предлаже јасне сугестије како побољшати превенцију, спремност и одговор на терористички напад који погађа критичну инфраструктуру. Савет је усвојио намеру Комисије да предложи Европски програм за заштиту критичне инфраструктуре (ЕПЗКИ/EPCIP) и дао сагласност око аранжмана Комисије за Информациону мрежу за упознавање о критичној инфраструктури (ИМУКИ/CIWIN). Европски програм за заштиту критичне инфраструктуре (EPCIP) се састоји од три главна дела: Директиве за идентификацију и именовање ECI, Финансијског програма и Информационе мреже критичне инфраструктуре (CIWIN). У одлуци Савета за унутрашње послове и правосуђе из децембра 2005. године од Комисије је затражен нацрт Европског програма за заштиту критичне инфраструктуре. Основни циљ европске политике јесте обезбеђење једнаког степена заштите за постројења одабране критичне инфраструктуре, што је изводиво једино на основу заједничког европског оквира за заштиту критичне инфраструктуре. Овакав приступ проистекао је из опасности да би разарање или поремећај одређене критичне инфраструктуре у једној земљи чланици могли непосредно утицати и на друге земље чланице. У овом смислу Европска унија дефинише тзв. Европску критичну инфраструктуру која се састоји од оних физичких ресурса, служби, уређаја,

информационе технологије, економске или социјалне користи: било а) две или више земаља чланица, било б) три или више земаља чланица.

Кад се ради о *Критичним секторима* треба истаћи да извештај Комисије Европске уније о заштити критичне инфраструктуре у борби против тероризма даје дефиницију критичне инфраструктуре, преглед идентификованих критичних инфраструктурних сектора и указује на критеријуме за проглашење одређених инфраструктурних сегмената критичним. У њему се наводи да се критичне инфраструктуре "састоје од оних физичких и информационих технологија, постројења, мрежа и служби, чије би ометање или уништење имало озбиљне негативне ефекте на здравље, безбедност или економско благостање грађана или на ефикасно функционисање влада држава чланица. Критичне инфраструктуре обухватају и велики број економских сектора и кључне службе влада држава чланица".[210]

Након извештаја Комисије ЕУ донет је и Зелени документ о европском програму заштите критичне инфраструктуре (*Green Paperon a European Program for Critical Infrastructure Protection − Green Paperon* EPCIP).[211] У овом документу дата је и дефиниција заштите критичне информационе инфраструктуре, где се наводи: "сви програми и активности власника, оператера, произвођача и корисника инфраструктуре као и регулаторних органа, који за циљ имају обезбеђивање квалитетног функционисања, минимизирање штете и брз опоравак критичне информационе инфраструктуре у случају кварова или напада на критичну информациону инфраструктуру, представљају заједно програм заштите критичне информационе инфраструктуре". Заштита критичне инфор-мационе инфраструктуре би требало да се посматра у контексту међусекторске повезано-сти с обзиром на то да прожима скоро све остале критичне секторе и требало би да се координише са заштитом свих осталих критичних инфраструктурних сектора.[212]

Критичне инфраструктуре (КИ) су ресурси, системи и мреже, физички или виртуелни, чије уништавање или онеспособљавање може ослабити националну

[210] Commission of the European Communities, Critical Infrastructure Protection in the Fight against Terrorism (Brussels, 20 October 2004), COM (2004) 702 final, p. 3, извештај Комисије доступан је на интернет адреси: http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf 17.11.2012

[211] Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM (2005) 576 final, p. 19, документ је доступан на интернет адреси: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf 17.11.2012

[212] Ibid, p. 19

безбедност, економску стабилност и утицати на друге аспекте нормалног функционисања друштва.

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

Заштита критичних инфраструктура се дефинише као стратегије, политике и спремност која је неопходна да би се одвратио или спречио напад, односно пружио одговор у случају да дође до напада на критичне инфраструктуре.[213] Заштита критичних информационих инфраструктура представља програме и активности реализоване 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 минимизирања последица и времена опоравка.[214]

Заштита критичних информационих инфраструктура (*Critical Information Infrastructure Protection* – CIIP) се базира на четири стуба: превенција и рано упозоравање (*prevention and early warning*), детекција (*detection*), реакција (*reaction*) и управљање кризама (*crisis management*).

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.

Зелени документ о европском програму заштите критичне инфраструктуре даје и преглед критичних инфраструктурних сектора. У критичне инфраструктуре се према овом документу убрајају:[215]

- Енергетика (производња нафте и гаса, рафинисање, прерада и складиштење укључујући и гасоводе и нафтоводе; производња струје; трансмисија струје, гаса и нафте; дистрибуција струје нафте и гаса),

[213] Lewis, G., Critical Infrastructure Protection i Homeland Security – Defending a Networked Nation, John Wiley & Sons Inc. Hoboken, New Jesey (USA), 2006.
[214] CI2RCO definition, http://www.ci2rco.org 20.02.2015
[215] Ibid

- Информационе и комуникационе технологије – ИКТ (информациони системи и мрежна заштита; интернет; пружање услуга у области фиксне телефоније; пружање услуга у области мобилне телефоније; радио комуникација и навигација; сателитска комуникација),
- Вода (обезбеђивање и дистрибуција пијаће воде; контрола квалитета воде; контрола доступности пијаће воде),
- Храна (снабдевање храном и очување безбедности и квалитета хране),
- Здравство (медицинска и болничка нега; лекови, серуми, вакцине; био-лабораторије; био-агенси),
- Финансијски системи (службе исплате; владине финансијске службе),
- Органи јавног реда и мира, јавне безбедности и судство (очување јавног реда, мира, безбедности; судска администрација),
- Цивилна администрација (владини органи; оружане снаге; службе цивилне администрације; службе за реаговање у ванредним ситуацијама; поштанске и курирске службе),
- Саобраћај и транспорт (друмски саобраћај; железнички саобраћај; ваздушни саобраћај; речни саобраћај; поморски и океански саобраћај и транспорт),
- Хемијска и нуклеарна индустрија (производња, складиштење и прерада хемијских и нуклеарних супстанци; цевоводи за транспорт опасних материја),
- Истраживање свемира.[216]

Иако велики део критичне инфраструктуре поседује и њоме управља приватни сектор, Комисија ЕУ је у свом извештају 574/2001 од 10. октобра 2001. године изнела констатацију да "јачање и увођење одређених безбедносних мера ради превенције напада усмерених на друштво у целости мора бити спровођена од стране јавних органа држава чланица ЕУ. Стога је значај јавног сектора у процесу заштите критичне инфраструктуре у оквиру ЕУ огроман".[217]

Принцип помоћи и чињеница да је заштита критичне инфраструктуре уско повезана са питањима државне безбедности, јесте једно објашњење чињенице да ниједна држава чланице ЕУ не жели да дели информације са другима нити да има

[216] Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM (2005) 576 final, p. 24
[217] Commission of the European Communities, *Critical Infrastructure Protection in the Fight against Terrorism*, (Brussels, 20 October 2004), COM (2004) 702 final, p.4

примат у овој области.[218] Међутим, због чињенице да су данашње инфраструктуре међусобно повезане и да се криза може осетити у суседним државама, учешће ЕУ се сматра оправданим иако она има само улогу координатора.

Природне катастрофе	ЕУ
Број догађаја	1,190
Број настрадалих	121,644
Просечно настрадалих по години	4,195
Просечно погођених	33,031,632
Просечно погођених по години	1,139,022
Економска штета (у хиљадама $)	266,918,923
Економска штета по годинама (у хиљадама $)	9,204,10

Табела 5.1. - Преглед природних катастрофа у ЕУ (1980-2008)[219]

У оквиру ЕУ постоји низ напора да се ЗКИ посматра посебно унутар сваког појединачног сектора.[220] Као резултат тога, стручњаци описују рад ЕУ на заштити критичне инфраструктуре као асистирање државама унутар јасно дефинисаних сектора, при чему између сектора постоји одговарајућа координација.[221] Проблем сарадње ЕУ и земаља чланица у процесу ЗКИ може да буде став самих земаља, да неки подаци морају бити задржани у националним оквирима.[222] Квалитет и интензитет сарадње на заштити критичне инфраструктуре између земаља чланицаи ЕУ доста варира од сектора до сектора − у појединим секторима кооперација доводи до формирања чврстих правила, регулатива и инспекција ЕУ, док у другим сама држава одлучује како ће и на који начин деловати. Такође, рад ЕУ је првенствено везан за давање смерница у процесу заштите КИ, дефинисање законских регулатива, а не за директно учествовање у обезбеђивању безбедности КИ.

Ефикасније спровођење мера ЗКИ унутар ЕУ је главна преокупација Европске комисије и држава чланица у оквиру Европског програма заштите критичне инфраструктуре. Циљ програма је да стимулише, промовише и развија мере ЗКИ у областима као што су кризни менаџмент, заштита животне средине, јавно здравље, саобраћај, истраживања, технолошки развој и други. Европски програм заштите критичне инфраструктуре је заснован на приступу заштите од свих опасности, али

[218] Eriksson, P., Barck-Holst S., (2005), *Critical Infrastructure Protection policy in the EU and in Sweden – comparative analysis*, FOI, Stockholm
[219] Видети на интернет адреси: *Disaster Statistics*, http://www.preventionweb.net 20.02.2015
[220] Eriksson, P., Barck-Holst S., (2005), *Critical Infrastructure Protection policy in the EU and in Sweden – comparative analysis*, FOI, Stockholm
[221] Larsson, R., (2007), *Tackling Dependency: The EU and its Security Chalenges*, Swedish Defense Research Agency, p. 9, p. 24
[222] Jarlsvik, H., Castenfors, K., (2004), *Security and Preparedness in the EU*, Stockholm, стр. 64

предност се даје заштити од тероризма. Приступ заштите од свих опасности значи да се морају узети у обзир и несреће настале као последица људског фактора, технолошке претње и природне катастрофе.[223]

Извор: *Natural Disaster Occurence Reported*, http://www.preventionweb.net 23.02.2015.

На националном нивоу поједине државе чланице ЕУ су још у раној фази примене мера заштите критичних инфраструктура, док је у другима степен развоја политика и стратегија ЗКИ на много вишем нивоу. Ипак, постоје и неке сличности између држава, нпр. у основним механизмима ЗКИ и изгледу система, који се бави прописивањем и спровођењем мера заштите (нпр. све државе чланице имају исти или бар сличан принцип поделе обавеза по секторима, са по једном надлежном институцијом за сваки сектор). Ипак, предузете мере и спроведени планови заштите разликују се од једне до друге државе.[224]

Истраживање постигнутог у процесу заштите критичне инфраструктуре на нивоу држава чланица ЕУ (2011. година) је показало да од 27 држава, 18 има дефинисану националну критичну инфраструктуру, док код 9 држава нема дефинисане националне критичне инфраструктуре. Међутим, већина тих држава предвиђа усвајање националне дефиниције критичне инфраструктуре у складу са принципима Европског програма за заштиту критичне инфраструктуре. Недостатак ове дефиниције значи да државе не спроводе специфичне заштитне мере заштите важних објеката и простора.

[223] Директива Савета Европе (2008/114/EC).
[224] Подаци потичу из истраживања развоја система заштите критичне инфраструктуре у 25 земаља ЕУ, које је спровела организација UNISYS, 2007.

Што се тиче држава које имају дефинисану националну критичну инфраструктуру главна разлика у њиховим тумачењима је да поједине државе дефинишу критичне објекте и инфраструктуру, а друге се концентришу на *виталне* фунције друштва. Као додатак томе, постоје и разлике у начину фокусирања држава чланица на спровођење ЗКИ. У појединим државама власти су фокусиране на заштиту важних објекта/инфраструктуре, док су у другим државама власти највише фокусиране на државну безбедност.[225]

Истраживање је даље показало да девет држава чланица ЕУ поседује списак јасно утврђене критичне инфраструктуре унутар своје територије. Све државе које имају дефинисану националну критичну инфраструктуру поделиле су их на секторе или подсекторе. Сектори који се најчешће јављају у националним програмима су: снабдевање енергијом, систем информација и телекомуникација, снабдевање храном, систем саобраћаја и дистрибуције, финансије и банкарство, здравство и снабдевање водом. Ово показује да су многе државе углавном фокусиране на заштиту оних сектора који се односе на основне животне потребе, а мање на тзв. симболичку инфраструктуру, као што су национални споменици (за разлику од САД-а, Аустралије и Канаде).[226]

Што се тиче организације система који је задужен за спровођење мера ЗКИ, она је иста или бар слична у свим државама чланицама ЕУ. У свакој држави, централно тело које спроводи ЗКИ је јасно дефинисано, иако се оно може разликовати у самој природи, дужностима или политичкој одговорности − у појединим државама координишуће тело нпр. може бити нека врста подршке и координатора, док у другим то исто тело може играти активну улогу у постављању стандарда и критеријума за оцењивање планова заштите. У појединим државама координишуће тело је део или је у надлежности Министарства унутрашњих послова или Министарства одбране, док је у другим део Центра цивилне заштите.[227] Такође, и друга министарства и агенције могу бити надлежни за обезбеђивање критичне инфраструктуре унутар подсектора за које су задужене. У свакој држави приватни сектор је укључен у заштиту критичне инфраструктуре, јер је већи део инфраструктуре у приватном власништву.[228]

[225] Ibid
[226] Ibid, p. 21
[227] UNISYS (2007), табела 2, стр.25-26, преглед кординишућих тела и законских/политичких оквира ЗКИ у 25 држава чланица ЕУ
[228] Ibid

У пет земаља дефинисана је и законска обавеза за спровођење заштите критичне инфраструктуре. Од оних земаља које немају међусекторско законодавство или политику заштите критичне инфраструктуре, у току су радови на изради таквог законодавства или политике. У осам земаља ЗКИ се сматра делом националне стратегије за кризни менаџмент или анти-терористичког плана. Даље, у осам земаља не постоји законска обавеза да се заштити критична инфраструктура, нити је дефинисана политика заштите критичне инфраструктуре, али су неке стратегије усвојене на нивоу заштите појединих сектора. Три државе немају никакву законску или правну основу за спровођење.[229]

Заштита критичне инфраструктуре у великој мери је децентрализована унутар самих држава чланица. У свакој од земаља значајан део инфраструктуре је у приватном власништву, тако да мора постојати сарадња са институцијама државе. Ниво и степен учешћа приватног сектора у заштити критичне инфраструктуре је различит. Док су у појединим државама представници приватног сектора активно или систематски укључени у развој политике, приватни сектор у осталим се укључује по потреби и то најчешће због имплементације минималних стандарда заштите које је установио државни сектор.

Директива Европског савета о идентификовању европске критичне инфраструктуре и неопходности заштитите критичне инфраструктуре из 2008. године,[230] прописује процедуру које се свака држава чланица мора придржавати, како би успешно иденти-фиковала и заштитила критичну инфраструктуру. По њој, свака држава чланица мора да идентификује потенцијалну критичну инфраструктуру у сектору енергетике и саобраћаја према дефинисаним критеријумима критичности инфраструктуре из члана 2 (а) и члана 2(б) Директиве.[231] Као подршка државама чланицама усвојено је и необавезујуће упутство које би помогло при примени Директиве.[232]

Одређивање критичности сваког појединачног инфраструктурног сектора пред-ставља комплексан задатак. Комисија ЕУ предложила је три фактора која се требају узети у разматрање приликом идентификовања потенцијалних критичних инфраструктура у оквиру сваке земље чланице:

[229] Ibid
[230] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[231] Процедура идентификације је описана у члану 3 и Анексу III Директиве Савета ЕУ (2008/114/EC).
[232] Необавезујуће упутство се ажурира по потреби, а засновано је на искуству које је стечено имплементацијом Директиве и неким критикама.

1. *Обим* – губитак елемента критичне инфраструктуре изазива негативне последице, али не изазива губитак сваког елемента нити губитак сваке инфраструктуре негативне ефекте у истој мери и тај негативни ефекат се може одразити на већи или мањи географски простор. Према величини географског простора на који губитак или оштећење неке инфраструктуре може имати утицај могу се разликовати инфраструктуре које имају међународни, национал-ни, покрајински и локални значај.
2. *Интензитет* – према степену у коме отказивање или уништење неке инфраструктуре може имати утицај на читаво друштво може се формирати неколико категорија: инфраструктуре чије уништење нема никакав или има занемарљив ефекат, затим инфраструктуре чије отказивање или уништење има минималан ефекат, инфраструктуре чије уништење или отказиваање има умерен ефекат, и на крају инфраструктуре чије уништење има велики ефекат на функционисање читавог друштва. Како би се проценио поменути степен у ком отказивање или уништење неке инфраструктуре има утицај постоји неколико критеријума (који у ствари представљају утицаје на различите сегменте друштва): утицај на јавност (број грађана који трпе негативне ефекте услед губитка инфраструктуре, број изгубљених живота, број оболелих, број озбиљно повређених грађана, број евакуисаних грађана), економски утицај (ефекат на БДП, значај економских губитака и/или деградација производње или служби), утицај на околину (загађење или уништавање околине), међуповезаност и међузависност са другим инфраструктурама (под овим се подразумева утврђивање степена у ком је одређена инфраструктура повезана са осталим инфраструктурама и у којој мери функционисање других инфраструктура зависи од исправног функциони-сања инфраструктуре чији се утицај разматра) и на крају политички утицај (који зависи од способности и успешности владе једне земље у намери да се избори са проблемом отказивања или губитака неког инфраструктурног сегмента).
3. *Временски ефекат* − овај критеријум заправо се односи на податак у ком тренутку ће губитак или отказивање одређене инфраструктуре имати озбиљан утицај (нпр. отказивање инфраструктуре може показати негативне ефекте моментално, у периоду од 24 до 48 сати од тренутка кад се десило отказивање, недељу дана након отказивања инфраструктуре).

У већини случајева предлаже се такође и испитивање психолошких ефеката отказивања или квара неке инфраструктуре.[233]

Након идентификовања критичних сектора на нивоу сваке државе чланице, могуће је извршити и одређивање оних које су критичне на нивоу Европске уније, и то најпре на основу дефиниције европске критичне инфраструктуре из Директиве Савета из 2008. где се наводи "европска критична инфраструктура обухвата објекте, системе или делове који се налазе у државама чланицама ЕУ, а који су важни за одржавање виталних животних функција, здравства, безбедности, заштите и економског или социјалног благостања људи, а чије нарушавање може имати катастрофалан утицај на све државе чланице".[234] У даљем процесу идентификовања инфраструктура које су критичне на нивоу ЕУ, јако је битан Члан 2(б) Директиве Европског савета који каже: "критична инфраструктура је она која се налази у било којој држави чланици ЕУ, а чије би нарушавање угрозило најмање две државе чланице ЕУ. Значај овакве критичне инфраструктуре процењује се на основу проучавања ефеката који настају као резултат међусекторске зависности од других инфраструктурних сектора".[235] Уколико нарушавање инфраструктуре остане у национал-ном оквиру, онда се она не сматра критичном на нивоу ЕУ.

Државе, а са њима и власници и оператери критичних инфраструктура у њима, учесници Европског програма заштите критичне инфраструктуре, имају најпре обавезу да поштују одредбе Директиве о заштити критичне инфраструктуре и европског програма, а затим имају још неколико захтева пред собом.

Директива наглашава три специфична захтева који власници и оператери европске критичне инфраструктуре морају да испуне а то су: да осмисле План заштите оператера (OSP), да спроведу анализу ризика на основу сценарија претњи и да именују официре за везе (SLO).

Први захтев обавезује државу да има План заштите оператера који идентификује критичне инфраструктуре, као и мере којим штити инфраструктуру.[236] План заштите оператера мора бити готов у року од годину дана након одређивања критичне инфраструктуре и мора се редовно надгледати.[237]

---

[233] Ibid, p. 3-5
[234] Члан 2(а) Директиве Савета ЕУ (2008/114/EC).
[235] Члан 2(б) Директиве Савета ЕУ (2008/114/EC).
[236] Минимум захтева Плана заштите оператера је да се утврди Анекс II Директиве Савета ЕУ (2008/114/EC)
[237] Анекс II, у необавезујућем упутству, наводи постојаће мере које испуњавају захтеве постављених официра за везу и спроведених планова заштите оператера.

Нераскидива са потребом осмишљавања Плана заштите оператера је анализа ризика и претњи по критичну инфраструктуру, што је уједно и друга обавеза оператера.[238] Трећа обавеза је да власници и оператери критичне инфраструктуре морају у програму заштите европске критичне инфраструктуре именовати официре за везу. Они су задужени за посредовање (представљање оператера) у договорима о безбедности критичне инфра-структуре између власника/оператера европске критичне инфраструктуре и надлежних власти држава чланица. Ово је битно због ефикасне размене информација о утврђеним ризицима и опасностима примене програма заштите критичне инфраструктуре.[239]

За све претходно наведене обавезе из Директиве надлежни су власници/оператери ECI-а и они морају проћи најбољу обуку, тренинге и размењивати информације о новим техничким процедурама и мерама заштите критичне инфраструктуре.[240]

Државе чланице су једино одговорне за спровођење Директиве и морају се постарати да све обавезе буду завршене у две године од утврђивања инфраструктура које су критичне на нивоу ЕУ. Као додатак овој генералној обавези, постоје четири специфична задатка које министри и власти у владама држава чланица морају да испуне. Први и најважнији је да држава чланица мора да буде ангажована у процедури идентификације. Други задатак је да се одреди европски контакт центар за заштиту критичне инфраструктуре у оквиру сваке државе чланице. Трећи задатак је повезан са контролом власника/оператера и њихових активности око доношења плана заштите оператера и постављања официра за везу. Овај задатак подразумева и контролу извештаја које власници/оператери критичне инфраструктуре морају редовно да подносе.[241]

Прва директна обавеза, која произлази из Директиве, за сваку државу чланицу је да мора да идентификује потенцијалне критичне инфраструктурне секторе унутар своје земље, али такође и критичну инфраструктуру држава чланица са којима се граничи. Прва *идентификациона рунда* мора бити завршена у року од две године и након тога се прегледи морају редовно спроводити. Када се идентификује потенцијална европска критична инфраструктура, држава чланица на чијој се територији она налази мора

[238] Члан 7:1 Директиве Савета ЕУ (2008/114/EC).
[239] Члан 6 Директиве Савета ЕУ (2008/114/EC).
[40] Члан 8 Директиве Савета ЕУ (2008/114/EC).
[241] Чланови 5 (Операторов план заштите критичне инфраструктуре), 6 (постављање официра за везу од стране власника/оператера критичне инфраструктруе) и 10 (тачка контакта) Директиве Савета ЕУ (2008/114/EC).

информисати другу државу чланицу у којој се могу осетити последице отказивања ове инфраструктуре. Очигледно је да се исте информације о обавезама јављају када је у питању власник/оператер који је задужен за инфраструктуру која је окарактерисана као критична на нивоу ЕУ унутар оквира једне државе. Када се инфраструктура означи као ЕКІ, ступа на снагу уговор који се тиче угрожених држава чланица.[242]

Утврђивање европског контакт центра за заштиту критичне инфраструктуре је друга обавеза коју морају да испуне државе чланице. Формирање контакт центра је мера која има циљ да обезбеди ефективну заштиту европске критичне инфраструктуре путем комуникације и координације. Главни задатак контакт центра је координирање активности у области заштите критичне инфраструктуре унутар саме државе чланице, као и координација активности са другим државама чланицама и са Европском комисијом.[243] У већини земаља, овај контакт центар је у надлежности Министарства унутрашњих послова или се налази у склопу постојећих центара за заштиту националне инфраструктуре.

Трећа обавеза власти држава чланица је да надгледају спровођење планова које су донели оператери, а који су везани за заштиту критичне инфраструктуре и да надзиру рад официра за везу и редовно буду у контакту са њима. Уколико држава чланица открије да оператери/власници нису испунили своје обавезе у погледу заштите критичне инфраструктуре, она мора да предузме све неопходне мере да се таква ситуација исправи, да се донесе план заштите критичне инфраструктуре, односно именује официр за везу.[244]

Четврта обавеза која произилази из Директиве Савета је да свака држава чланица направи и поднесе три врсте извештаја Комисији:

1. Свака држава је у обавези да једном годишње поднесе извештај о броју угрожених инфраструктура на својој територији,
2. Свака држава чланица мора да информише Комисију о броју означених критичних инфраструктура унутар сваког сектора као и томе колико би других држава чланица било угрожено отказивањем тих критичних инфраструктура и

[242] Видети члан 4:1; члан 4:2; члан 4:5; члан 4:3; и члан 4:4 Директиве Савета ЕУ (2008/114/ЕС).
[243] Члан 10 Директиве Савета ЕУ (2008/114/ЕС).
[244] Члан 5:3 и члан 6:3 Директиве Савета ЕУ (2008/114/ЕС). Не постоји временски оквир у коме би требало да се именује официр за везу, али се то мора обавити што пре, јер се именовање официра за везу сматра предусловом за формирање плана заштите оператера.

3. Свака држава чланица мора сваке друге године да достави Комисији основне податке о врстама ризика, опасностима и рањивостима инфраструктура по секторима.

На основу ових извештаја, Комисија држава чланица заједнички одлучује које ће мере ЕУ даље предузети.[245]

Као додатак директним обавезама, Европски програм заштите критичне инфраструктуре такође доноси неколико индиректних и добровољних задатака које би државе чланице требало да испуне. На пример, државе чланице се охрабрују да успоставе национални програм заштите критичне инфраструктуре и да учествују у раду експертских група. Другим речима, иако је за Европску унију најбитнија заштита оне инфраструктуре која се сматра критичном на нивоу Уније, она подстиче и сваку државу чланицу да усвоји сличне приступе и кад је у питању заштита националне критичне инфраструктуре.

Европска комисија је 2008. године покренула иницијативу и установила своју политику у области критичне комуникације и заштите критичне информационе инфраструктуре.[246] Циљ ове политике је да осигура адекватан и постојан ниво заштите и отпорности критичне информационе инфраструктуре у Европској унији. Ова иницијатива је само делић ширег европског програма заштите критичне инфраструктуре (*European Programme for Critical Infrastructure Protection* - EPCIP),[247] новијег је датума и указује на смер у ком се креће заштита критичне инфраструктуре како у Европи тако и у читавом свету.

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.[248] Дакле, у читавом свету информациона инфраструктура постаје све битнија, прожима све делатности друштва и самим тим ефекат који би њено отказивање имало на друштво био би огроман. Из тих разлога последњих година се огромна пажња поклања баш овом елементу критичне инфраструктуре, формирају се нове политике заштите и уводе се нове безбедносне мере.

[245] Члан 3.2, члан 4.4 и члан 7.2 Директиве Савета (2008/114/EC).
[246] http://ec.europa.eu/dgs/information_society/index_en.htm 17.11.2012
[247] Програм се може наћи на интернет адреси: http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infra- struct_en.htm 17.11.2012
[248] 2010 Critical Information Protection (CIP) Survey, www.symantec.com 20.02.2015

Стратегија Комисије ЕУ о безбедности информационог друштва указала је на то да нормално функционисање скоро свих критичних инфраструктура постаје у великој мери зависно од безбедности одговарајућих информационих система. Спровођење стратегије одобрио је резолуцијом Савет ЕУ, који је и промовисао унапређење поузданости, отпор-ности и издржљивости комуникационих мрежа и информационих система.[249]

Као део припрема за формирање стратегије заштите критичне информационе инфраструктуре компанија *Lucent Technologies* спровела је 2007. године *Студију о доступности и издржљивости електронске комуникационе инфраструктуре (Study on the Availability and Robustness of Electronic Communication Infrastructures* - ARECI*)*, у којој се даје десет препорука везаних за кључне активности које би Комисија ЕУ требало да предузме заједно са државама чланицама и приватним сектором, како би се на крају унапредили поузданост, отпорност и издржљивост информационих инфраструктура. Ове препоруке подразумевају савете у областима припремања за реаговање у ванредним ситуацијама, постављања приоритета у комуникацији у оквиру јавних мрежа, формирања уговора о заједничкој помоћи, размене информација о критичним инфраструктурама, међузависности инфраструктура, интегритета и функционисања ланаца снабдевања, тес-тирања оперативности, оснаживања власничких и партнерских уговора и размене искустава у области заштите информационих инфраструктура.[250]

Комисија ЕУ је основала *Мрежу обавештавања и упозоравања у области критичних инфраструктура* (*Critical Infrastructure Warning Information Network* – CIWIN), на нивоу ЕУ како би помогла државама чланицама, институцијама Европске уније, власницима, операторима и корисницима инфраструктуре у процесу размене информација о заједничким претњама по инфраструктуру и у формирању мера и стратегија које за циљ имају неутралисање ризика по критичну инфраструктуру.[251] Прецизно одређење чворова ове мреже је увек отворено питање и њихов број увек може да се прошири, али је сигурно да мрежа укључује органе управљања на различитим нивоима.CIWIN треба да функционише као допуна већ постојећем скупу

[249] Резолуција Савета ЕУ о заштити критичне информационе инфраструктуре може се наћи на интернет адреси: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf 17.11.2012
[250] Студија и коментари везани за резултате студија могу се наћи на:
http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm 17.11.2012
[251] Commission of the European Communities, *Critical Infrastructure Protection in the Fight against Terrorism*, Brussels, 20 October 2004, p.10

мрежа, које су директно или индиректно повезане са критичном инфраструктуром без преклапања функција са тим другим мрежама.

Комисија ЕУ предлаже три могућа начина развоја мреже за обавештавање и упозоравање у области критичних инфраструктура:[252]

- Мрежа може да узме облик форума, чија је улога ограничена на размену идеја о заштити критичне инфраструктуре и искустава њених власника и оператера,
- Мрежа може да функционише као систем раног упозорења који повезује државе чланице ЕУ са Европском Комисијом и
- Мрежа може да се конципира као систем за комуникацију и узбуњивање који повезује све нивое управљања критичном инфраструктуром и функционише као систем брзог узбуњивања са једне стране, повезујући притом државе чланице ЕУ са Комисијом ЕУ, и као форум за размену идеја и искустава у области заштите критичне инфраструктуре с друге стране.

Годишњи финансијски програм за превенцију, припрему и последице спречавања тероризма[253] Европски савет је покренуо 2007. године, као финансијски програм под називом *Превенција, припрема и санација последица терористичких напада и безбеднос-них инцидената*.[254] (у даљем тексту само *финансијски програм*) како би обезбедио финансирање мера које се односе на заштиту критичне инфраструктуре. Овај програм се спроводи у оквиру ширег Европског програма заштите критичне инфраструктуре и подржава (кроз финансирање спровођења одговарајућих мера заштите критичне инфраструктуре) напоре држава чланица да "спрече терористичке нападе, успоставе и очувају одговарајући ниво припремљености за случај напада и заштите људство и критичну инфраструктуру од терористичких напада и других безбедносних инцидената".[255]

Оно што се очекује од овог програма јесте да додатно допринесе развоју инструмената, стратегија и активности и мера на пољу ефикасне заштите критичне инфраструктуре (на нивоу ЕУ и на националном нивоу) као и развоју заједничког оквира заштите критичне инфраструктуре на нивоу ЕУ. Од пројекта се очекује и да подстакне развој метода, техника и инструмената за рад и обуку у оквиру разних

[252] Ibid
[253] Засновано на годишњем програму рада за 2007. годину − превенција, припрема и санација последица терористичких напада и других ризика.
[254] Одлука Савета ЕУ број 2007/124/EC - Council Decision 2007/124/EC of 12 February 2007, Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks".
[255] Ibid

инфраструктурних сектора, затим да подстакне размену информација и искустава у заштити критичне инфраструктуре, да подстакне развој и побољша сарадњу између јавног и приватног сектора у области заштите критичне инфраструктуре, унапреди системе заштите критичне инфраструктуре у оквиру држава чланица, да подстакне развој комуникације између власти и релевантних организација, агенција и компанија које се баве заштитом критичне инфраструктуре и на крају да утиче на стварање атмосфере поверења између учесника у процесу заштите критичне инфраструктуре.[256]

Поменути финансијски програм је део ширег програма *Безбедност и очување слобода*. Укупни буџет ширег програма за прву годину износио је близу 140 милиона евра, а формиран је средњорочни план спровођења програма за период од 2007. до 2013. године.[257] Конкурс за предлоге пројеката се редовно објављује на сајту Европске Комисије. Државе чланице имају рок од три месеца након сваког отварања конкурса да поднесу своје предлоге. Комисија охрабрује власти држава чланица и компаније да се пријаве за финансијску подршку, а обезбеђује и потребну обуку након прихватања пројеката. Годишњом одлуком о раду програма за 2009. годину износ буџета се попео на 177 милиона евра. Засновани на великом броју критеријума селекције, предлози за пројекат оцењују се на основу оперативних и професионалних компентенција кандидата, као и на основу квалификованости за спровођење пројекта и постојећих финансијских могућности.

Један од пројеката који се финансира путем финансијског програма је *Европска референтна мрежа за заштиту критичне инфраструктуре* (ERNCIP − *European Reference Network for Critical Infrastructure Protection*). Предлог за увођење ERNCIP-а дала је Комисије ЕУ која је сматрала да постоји огроман проблем у смислу доступности података о безбедности и рањивости инфраструктуре. Заштита критичне инфраструктуре захтева информације на којима се базирају анализе као што су дизајн, архитектура, различите процедуре и сл.[258]

---

[256] Кад је у питању нпр. сектор енергетике и система повезаних са енергетским, програм се бави и државним и међудржавним програмима за рестаурацију порушене инфраструктуре, проценом и смањењем ризика од напада на велике термоелектране, као и спречавањем угрожавања рада система на струјни погон. Кад је у питању сектора саобраћаја у државама чланицама, програм може нпр. да финансира пројекте везане за надзор превоза опасних материја.

[257] Програм превенције и унапређења спремности за терористичке нападе и санације последица тероризма и других безбедносних инцидената има буџет од 12,7 милиона евра. Оно што је важно јесте да се овај програм не примењује за финансирање пројеката који су покривени другим финансијским програмима (доста пројеката из области цивилне заштите покривено је другим фондовима).

[258] Интерни радни документ Европске Комисије; Европска референтна мрежа за заштиту критичне инфраструктуре (јун 2008).

И државни и приватни учесници у процесу ЗКИ имају приступ тестовима ERNCIP, који обавештава државе чланице о свим спроведеним тестовима и истраживањима, а онда заинтересоване државе чланице контактирају са ауторима истраживања и траже од њих приступ резултатима. Аутор истраживања даље одлучује да ли ће доставити информације заинтересованој страни.[259]

Европска агенција за безбедност мрежа и информациону безбедност (*European Network and Information Security Agency* − ENISA) оформљена је 14. марта 2004. године. Одлуком да ову агенцију уведе као правни субјект, ЕУ је интензивирала своје напоре у намери да унапреди координацију акција везаних за информациону безбедност.

Агенција настоји да обезбеди висок ниво безбедности мрежа и информационе безбедности у оквиру европске заједнице. Агенција доприноси развоју информационе безбедности и безбедности мрежа ради добробити свих грађана, корисника, компанија и организација из области јавног сектора Европске уније. Рад агенције доприноси и ефикасном функционисању тржишта у оквиру ЕУ.

Агенција помаже Комисији ЕУ, државама чланицама ЕУ, а последично и читавој пословној заједници у испуњавању захтева везаних за безбедност мрежа и информациону безбедност. Агенција је такође и центар за експертизу у области информационе безбедности, коме се обраћају и државе чланице и европске институције када имају проблема са спровођењем мера заштите критичне информационе инфраструктуре. Агенција је такође публиковала и спискове са описима активности којима се баве рачунарски тимови за ванредне ситуације у Европи,[260] а промене у надлежностима и обавештења о делатностима рачунарских центара агенција представља квартално у виду обавештења. Агенција такође организује и радионице за размену искустава између земаља чланица у области информационе безбедности. Осим свега наведеног, Агенција дефинише и прилагођене информационе пакете и издаје упутства за спровођење мера заштите информационе инфраструктуре за одређене групе корисника (нпр. за мала и средња предузећа, за кућне кориснике и сл.). На крају, Агенција за европске мреже и информациону безбедност креирала је мрежу својих специјализованих службеника који помажу у размени информација и свакодневној сарадњи са државама чланицама.[261]

---

[259] Ibid

[260] European Network and Information Security Agency (ENISA), ENISA Inventory of CERTActivities in Europe - Version 1.5, September 2007; Читав овај пројекат доступан је и на интернет адреси: http://www.enisa.europa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf 17.11.2012

[261] http://www.enisa.europa.eu/index.htm 17.11.2012

Један од скоријих програма носи назив *Остваривање утицаја на бази синергије*, његово спровођење је установила Агенција за европске мреже и информациону безбедност. Програм је започет 2008. године[262] и фокусира се на повећању утицаја који има агенција у процесу спровођења мера заштите критичне информационе инфраструктуре, на основу сарадње са релевантним учесницима. Програм је заснован на новом приступу, уз дефинисање три вишегодишња тематска програма, и то:[263]

1. Унапређење отпорности европских мрежа електронске комуникације,
2. Развој и одржавање модела сарадње и
3. Идентификовање актуелних ризика и учвршћивање поверења између учесника у процесу спровођења мера безбедности информационих система.

Програм даје и преглед активности које предузима Агенција, укључујући и активности на плану подизања свести о важности информационе безбедности, затим промовисање сарадње и размене информација и искустава између земаља чланица, као и активности везане за јачање сарадње између свих земаља чланица. Агенција је свесна важности своје улоге и подршке коју треба да пружи стратегији Европске комисије. Како би максимизирала утицај својих активности, агенција тежи да пренесе постојећу синергију и иницијативе на националне нивое и у све европске институције.[264]

Истраживање и развој у области заштите критичне инфраструктуре Развој технологија информационог друштва − 6. и 7. оквирни програм (Information Society Technologies (IST) FP6 and FP7) са општим циљем развоја технологија информационог друштва у складу са акционим планом *eEurope*. Сем овог основног циљ програма је формирање безбедносних оквира за развој информационог друштва, повезивање приват-ног и јавног сектора путем мрежа и интернета, електронско обезбеђивање друмског и ваздушног саобраћаја, спровођење програма *е-Здравство* (*e-Health*), унапређење кризног менаџмента и управљања ризицима. Спровођење 7. по реду плана развоја информационог друштва почео је 2007. године и трајао је до краја 2013. године.[265] ЕУ спроводи програме развоја информационог друштва од 1986. године, али овај програм је убедљиво највећи до сад.[266] Циљ истраживања информационих и комуникационих технологија у оквиру програма ЕУ за развој информационог друштва

[262] European Network and Information Security Agency (ENISA), Work Programme 2008: "Build on Synergies – Achieve Impact". План спровођења програма је доступан на интернет адреси: http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf 17.11.2012
[263] http://www.enisa.europa.eu/pages/02_01_press_2007_11_21_wp_2008.html 17.11.2012
[264] European Network and Information Security Agency (ENISA), Work Programme 2008: "Build on Synergies – Achieve Impact", p.3
[265] http://ec.europa.eu/research/future/themes/index_en.cfm 17.11.2012
[266] http://ec.europa.eu/information_society/research/eu_research/index_en.htm 17.11.2012

је унапређење компетенција ЕУ на свим нивоима кроз фокусирање на три кључне области развоја информационих и комуникационих технологија:[267]

1. Повећање продуктивности и увођење иновација, кроз унапређење креативности и менаџмента,
2. Модернизација јавних служби – здравства, образовања, транспорта и
3. Развој науке и технологије, кроз подржавање сарадње и приступ информацијама.

Званични портал 7 по реду програма развоја информационог друштва и са њим повезаних програма развоја наука и технологија у оквиру ЕУ јесте CORDIS.[268]

Европски програм безбедносних истраживања (European Security Research Programme − ESRP*)* има за циљ да простор Европске уније учини безбеднијим за грађане, уз очување конкурентности индустријског сектора у ЕУ. Кроз сарадњу и координисане акције на нивоу читаве Уније, могуће је боље разумевање и планирање реаговања на претње по критичну инфраструктуру у данашњем високоризичном друштву.[269]

Комисија ЕУ оформила је 1. јула 2005. године *Саветодавни одбор за европска истраживања безбедности* (*European Security Research Advisory Board* − ESRAB), који је повезан са Комисијом Европске уније и задужен је за сва питања везана за спровођење европског програма безбедносних истраживања. Саветодавни одбор обављао је своје дужности у складу са политиком Европске уније, посебно у складу са истраживачким и развојним активностима које се спроводе на националном нивоу[270] и издао је свој финални извештај 22. септембра 2006. године,[271] а престао је да постоји 31. децембра 2006. године. У овом извештају препоручује се оснивање *Форума за европска истраживања безбедности и иновације* (*European Security Researchand Innovation Forum* − ESRIF) како би се подстакао интензивнији дијалог и размена искустава и проблема везаних за европске безбедносне потребе.[272] Одлука о оснивању Форума донета је на другој Европској конференцији о истраживању безбедности у марту 2007. године, а предвиђено је да Форум буде нека врста приватно-јавног дијалога током безбедносних истраживања. Форум је почео да са радом у септембру

[267] Ibid
[268] http://cordis.europa.eu/ 17.11.2012
[269] http://ec.europa.eu/enterprise/security/index_en.htm 17.11.2012
[270] Official Journal of the European Union, Commission Decision of 22 April 2005 establishingthe European Research Advisory Board
[271] Видети на: http://ec.europa.eu/enterprise/security/articles/article_2006-04-06_en.htm 17.11.2012
[272]http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/346&format=HTML&aged=0&language=EN&guiLanguage=en 17.11.2012

2007. године. Циљ Форума (ESRIF) је развој средњерочних и дугорочних безбедносних планова и истраживачких програма у области безбедности, који ће повезати безбедносна истраживања са доношењем и имплементацијом безбедносних политика.[273]

Имајући у виду схватање да истраживања у области безбедности и приватно-јавна партнерства играју врло значајну улогу у процесу заштите критичне инфраструктуре, циљеви Форума су следећи:[274]

- окупљање свих релевантних учесника у процесима заштите критичне инфраструктуре и спровођења безбедносних мера, ради разматрања безбедносних питања од заједничког интереса,
- идентификовање предлога за обављање стратешких безбедносних истраживања и увођење иновација из области безбедности, уз активно учешће националних и европских учесника, и уз регистровање европских потреба и приоритета у области безбедности и
- размена идеја, схватања и искустава ради постизања боље искоришћености постојећих капацитета и ради интензивније употребе технологије у области безбедности.

Основна тема којом се Форум бавио била је заштита критичне инфраструктуре. Форум је престао да постоји крајем 2009. године.

У циљу *Координисања истраживања критичне информационе инфраструктуре (Critical Information Infrastructure Research* − CI2RCO*)* одлуком Европске уније основана је радна група која ће се бавити истраживањем мера које спроводи 28 држава чланица у борби против различитих безбедносних претњи по критичну инфраструктуру. Обим сарадње превазилази границе ЕУ, јер радна група има намеру да у своје активности укључи САД, Канаду, Аустралију и Русију. Пројекат CI2RCO покренут је на иницијативу 6. по реду програма развоја информационог друштва. Основни циљеви пројекта CI2RCO су:[275]

- подстрекавање координисаног приступа истраживању и развоју заштите критичне информационе инфраструктуре широм Европе,
- формирање европске истраживачке области (*European Research Area* − ERA) као део ширег програма развоја информационог друштва и

[273] О циљевима Форума детаљније на интернет адреси: http://www.esrif.eu/objectives.html 17.11.2012
[274] Ibid
[275] http://www.ci2rco.org/index.asp 17.11.2012

- праћење активности земаља ЕУ и земаља кандидата за улазак у Унију. На сајту овог пројекта износи се и извештај о заштити критичне информационе инфраструктуре у оквиру Европске уније и најављују се догађаји које организује ЕУ, а који су везани за заштиту критичне информационе инфраструктуре.

Законска регулатива везана за заштиту критичне инфраструктуре у ЕУ ослања се на принципе и норме које већ постоје у европском законодавству посебно кад је реч о областима информационе инфраструктуре, поверљивости комуникација, пресретању података, интелектуалној својини.[276] Навешћемо само битне, као: *Директива о заштити података из 1995. године* (95/46/EC)[277] даје регулаторне оквире, којима се гарантује безбедан и слободан проток информација преко националних граница земаља чланица ЕУ и поставља основе безбедносних протокола чији је циљ заштита информација; *Директива о електронском потпису из 1999. године* у области е-трговине (1999 / 93 / CE)[278] у потпуности је уведена у националне законске норме земаља чланица ЕУ; *Директива о заштити приватности у сектору електронске комуникације из 2002. године* 95/46/EC допуњена је директивом 97/6650 о заштити личних података у области телекомуникација, као и још битнијом европском директивом о заштити приватности у сектору електронске комуникације (2002/58/CE);[279]*Директива о регулацији мрежа и служби за електронску комуникацију из 2002. године* чији је циљ[280] хармонизација законских оквира у области регулисања рада мрежа и сервиса за електронску комуникацију, а даје и преглед националних регулаторних органа у овој области и издаје правила на основу којих се додељују на коришћење одређени национални ресурси попут радио фреквенција.

Одлука Савета ЕУ о нападима на информационе системе из 2005. године (200/ 222/ЈНА) има за циљ ојачавање сарадње свих одговорних националних органа у случајевима напада усмерених на информационе системе, кроз развој ефикасних модела реаговања и процедура, а државе чланице ЕУ су у обавези да оснују оперативне центре који ће бити доступни 24 часа дневно, сваког дана у недељи; *Директива о*

[276] Alain, E., Hanno, R., and Burkard, S., (edited by Burkard, S.) (2005), "Information security, A new challenge for the EU", Chaillo, Paper no. 76, Paris, March

[277] Report on the Economic Evaluation of the Data Protection Directive 95/46/EC; Извештај о директиви доступан је на: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf 17.11.2012

[278] http://ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/esignatures_en.pdf 17.11.2012

[279]http://www.jura.uniaugsburg.de/prof/moellers/materialien/materialdateien/010_europaeische_gesetze/eu_richtlinien/ril_2002_058_eg_datenschutz_en/ 17.11.2012

[280] http://www.bipt.be/ShowDoc.aspx?objectID=1020&lang=en 17.11.2012

чувању података из 2006. године о чувању података прикупљених од јавних служби и мрежа за електронску комуникацију (2006/24/ЕС и предлог Комисије COM(2005)0438), с тежњом да хармонизује националне законске регулативе држава чланица у области чувања телефонских података и података прикупљених са разних адреса електронске поште ради истага, налажења и кривичног гоњења криминалаца. Независни органи основани су како би се вршио надзор и контрола коришћења података, а ови органи су 2009. године преусмерени на акције везане за антитерористичка дејства;[281] *Лисабонски споразум из 2007. године*[282] су потписале све државе или владе 27 чланица ЕУ 13. децембра 2007. године, а који је ступио на снагу 1. јануара 2009. године и има за циљ реформу европских уставних оквира. Споразум између осталог садржи одредбе везане за заштиту личних података и реафирмише *право на заштиту личних података* (члан 16Б Лисабонског споразума).

Ставови држава чланица Европске уније о Европском програму заштите критичне инфраструктуре изнети у Извештају Комисије о резултатима *Зеленог документа* о Европском програму заштите критичне инфраструктуре из фебруара 2006. године показали су да 22 државе чланице које су поднеле иницијативу за Зелени документ о Европском програму заштите критичне инфраструктуре релативно спремно дочекале рад на развоју заштити критичне инфраструктуре.[283] Већина држава чланица сматра да Европски програм за ЗКИ треба подржати и да треба обезбедити неопходна средства за побољшање заштите критичне инфраструктуре.

Велико неслагање држава чланица око утврђења Европског програма односило се на саму његову природу и дилеме да ли програм треба да буде обавезан или добровољан, и да ли уопште постоји потреба за Директивом.[284] Несугласица је било и око формирања плана ЗКИ и око именовања официра за везу од стране оператера КИ,

[281] У директиви тачно стоји: "Свака држава чланица мора да именује надзорне органе одговорне за мониторинг примене директиве на својој територији. Ови органи могу да буду исти органи који су установљени чланом 28, Директиве 95/46/ЕС. Надзорни органи морају да функционишу потпуно независно".

[282] Пун текст Лисабонског споразума, такође познатог као реформског споразума, може се наћи на интернет адреси: http://europa.eu/lisbon_treaty/full_text/index_en.htm 17.11.2012

[283] Извештај Комисије (2006). Резултати Зеленог папира EPCIP и одговори држава чланица. Званичних резултата није било из Грчке, Италије и Малте.

[284] Седам држава чланица (Кипар, Шпанија, Литванија, Летонија, Луксембург, Португалија и Словачка) изразило је подршку законодавном приступу, седам држава је било против (Данска, Немачка, Финска, Француска, Холандија, Шведска и Велика Британија), а осам је било уздржано. Неке државе чланице су сматрале да оквир у почетку буде обавезан и добро успостављен (мишљења варирају о томе који делови оквирних радова могу бити обавезни). Такође, неке од држава чланица ЕУ имају мишљење да оквирни радови могу бити добровољни на почетку, а да треба да постану обавезни и добро установљени тек на крају. Видети извештај Комисије 2006, резултати Зеленог папира EPCIP-а и одговори држава чланица на то.

јер су се поједине државе чланице ЕУ побуниле да концепт формирања плана заштите критичне инфраструктуре, који је обавезан за све оператере, заправо не треба буде обавезан, већ треба да служи као пример добре праксе (због постојања власника/оператера критичном инфраструктуром који имају мало искуства у решавању сличних питања). Још један камен спотицања представљала је и сарадња између приватног и јавног сектора и начина на који се може створити поверење између ова два сектора. Заправо, већина држава чланица је имала став да се поверење између приватног и јавног сектора може створити само кроз добровољно партнерство и да мандатна правила представљају ризик за дијалог између државних-приватних актера. Такође, списак сектора критичних инфраструктура изазвао је дискусију и на њега је предложен већи број амандмана.[285]

Још једна разлика у мишљењу која је довела до релативно дуге расправе била је у вези са дефиницијом заштите критичне инфраструктуре. Државе чланице су биле подељене око питања дефинисања европске критичне инфраструктуре као инфра-структуре чије отказивање има утицај на две или више држава чланица.

Као што су стручњаци већ описали, политика заштите критичних инфраструктура унутар ЕУ је представљена као контролисани процес Комисије која идентификује и штити критичну инфраструктуру са једне стране, или као децентрализовани систем где је улога ЕУ да промовише координацију и размену искустава, али где највећу контролу над заштитом критичне инфраструктуре имају државе чланице с друге стране.[286] Током преговора о извештају Комисије, може се закључити да је предлог Комисије о Директиви мало по мало добио децентрализован приступ. Комисија то сматра природним будући да је потребно време за промене у области као што је ова.[287]

Приликом успостављања Европског програма ЗКИ, Комисија се суочава са два проблема: први је да слабости процеса заштите критичне инфраструктуре морају бити елиминисане, посебно међугранични ефекти отказивања критичних инфраструктура, а други је да додатни трошкови компанија које раде у више земаља чланица на заштити критичних инфраструктура морају бити елиминисани.

[285] Ibid
[286] Eriksson, P., Barck-Holst, S., (2005), *Critical Infrastructure Protection policy in the EU and in Sweden – comparative analysis*, FOI, Stockholm, p. 10
[287] Интервју, Генерални директорат за правосуђе, слободу и безбедност, Lindstrom, 9. јул 2008. године (2008б).

Критична инфраструктура ЕУ обухвата многе секторе економије, укључујући банкарски и финансијски сектор, транспорт и дистрибуцију, енергију, здравље, снабдевање храном, комуникације, као и остале владине функције и услуге. Заједно са унутрашњом безбедношћу КИ у ЕУ представља централно питање за европски социјални систем. Уништење КИ, са психолошког аспекта, водило би потпуном неповерењу јавности у европске институције. У овом моменту, концепти управљања кризама знатно се разликују у многим државама ЕУ. Из тих разлога Комисија, кроз Европски програм за заштиту критичне инфрастуктуре (EPCIP), обезбеђује опште процедуре за иденти-фиковање КИ. Предуслов за ефикасно управљање кризама је заштита неопходне информационе технологије и телекомуникационих система. Ови сектори имају трансверзалну инфраструктуру и истовремено чине КИ за друге КИ као што су, на пример, монетарни, финансијски и осигуравајући сектори.

Исправност приступа *одоздо на горе* је заснована на чињеници да националне службе најбоље познају стање у својим земљама. Примарна и неспорна одговорност за заштиту КИ лежи на државама чланицама и власницима/операторима КИ. Велике корпорације су ограничене националним оквирима (правним, економским, политичким) када обављају своје активности на међународном нивоу. Ценећи њихова искуства, вештине и специфичне захтеве у односу на заштиту КИ, генерално не сме бити потцењена улога приватног сектора.

Необавезујуће мере, иако флексибилне, не представљају поуздану основу, будући да, када су у питању заинтересоване стране, није јасно рашчлањено ко, шта и каква права и обавезе има у погледу заштите ЕКИ. Уколико се укаже неопходним, могу бити развијене заједничке методологије процене структурне рањивости, претњи и ризика европске КИ.

Заштита критичне инфраструктуре унутар Европске уније, као и у суседним државама је изузетно сложено питање које налаже државама да предузму низ корака на том подручју. Државе Европске уније су суочене са чињеницом да је приоритет новог концепта управљања кризним и ванредним ситуацијама заштита националних ресурса. Такође, јасно су конципирани основни ресурси за управљање критичном инфра-структуром и кризним и ванредним ситуацијама, а њих чине: људски и материјални ресурси, простор, ресурси знања и информација, инфраструктура, финансијски ресурси и време.

Истовремено, безбедносни изазови са којима се земље Европске уније суочавају данас или ће се суочити у будућности су застрашујуће. Повећана сложеност критичне

инфраструктуре, климатске промене, изузетне технолошке иновације, промена међународ-них односа снага, несташица енергије, сајбер-напади, деградација животне средине и др. стварају нове и непредвидиве изазове. Поред тога, Европска унија се суочава и са врло високим безбедносним ризицима и изазовима природних катастрофа, терористичких претњи и сл. Европа ће стога све више морати да сарађује са суседима, регионалним организацијама, цивилним друштвом, међународном заједницом и приватним сектором.[288]

Сарадња је веома битна и чланице ЕУ морају да продубе своје разумевање, као и да буду спремне да уче једни од других, јер различите државе и региони имају различите правне оквире, политике приоритета, као и различита искуства и вредности. Јачање међусобне сарадње, уз поштовање разлика и сличности националних система безбедности, треба да се одвија уз поштовање локалних и националних различитости. Управо је истраживање могућности за сарадњу између чланица Европске уније у ванредним ситуацијама суштински циљ и допринос АНВИЛ-а (Анализа цистема цивилне заштите у Европи), који указује на културну, институционалну, правну и оперативну разлику 22 национална система цивилне заштите и 8 регионалних организација у Европи. Овако широко схваћен приступ помаже да се превазиђу поједностављене претпоставке за избор "најбољег начина" кризног менаџмента, било да су кризе националне, регионалне или наднационалне. Анализа је открила да се административна одговорност, правни оквир и оперативна пракса земаља изразито разликују и да су последица националног контекста и историјских искустава. Интересантно је да истраживање није открило значајне разлике у ефективности, ефикасности и легитимности система цивилне заштите. Не постоји јединствен начин поступања у цивилној заштити, који одговара свима, али постојећи има простора за измене, прилагођавања и побољшања у многим областима.

Координација свих активности цивилне заштите Европске уније има широку подршку међу грађанима, јер се ЕУ доказала и као водитељ – модератор и као промотер истих. Грађани очекују од својих влада да планирају, предвиде и пронађу могућности да спрече ризик за настајање критичних инфраструктура, да се припреме за кризе и катастрофе, за заштиту вредности критичних инфраструктура и да ефикасно реагују да спрече кризу, умање могуће последице и да обезбеде брз опоравак после

[288] ANVIL (Analysis of Civil Security Systems in Europe) project: CIVIL SECURITY AND THE EUROPEAN UNION, A survey of European civil security systems and the role of the EU in building shared crisis management. Интернет адреса: capacitieshttp://anvil-project.net/results/ 23.02.2015.

кризног удара. За ЕУ је битно да за земље чланице или регионе истакне по чему се разликују. Тако се, на пример, последњих година видело много пожара у јужној Европи (Грчка, Шпанија, Италија, Хрватска), индустријске несреће у Француској, бројни земљотреси у Италији, поплаве у централној и источној Европи, терористички напади у Великој Британији, Шпанији, Француској и Холандији, што је само неколико недавних догађаја. У одговорима на ове различите кризе стичу се и различита искуства, уз уважавање претходних искустава и традиције.

Све државе чланице Европске уније су у периоду од 2010-2012. године извршиле битне реформе својих система заштите критичних инфраструктура, али и даље постоје значајне разлике по питању форме, разумевања и последица трансформације. Тако АНВИЛ истраживање указује да је већина земаља направила посебне одредбе за проглашење "стања катастрофе" које омогућавају хитно поступање (Аустрија, Хрватска, Шведска и Швајцарска). Оперативно управљање кризом током већине сценарија пренето је на заједничку одговорност неколико локалних агенција за хитно реаговање, пре свега ватрогасне бригаде, хитну помоћ, полицију и добровољне организације. У већини земаља поступци су само до одређеног нивоа централизовани, док локални и регионални нивои имају важну улогу у вођењу политике цивилне заштите. Добровољне организације чине важан фактор и допринос у цивилној заштити у већини АНВИЛ земаља, али степен организационе конхерентности и формализација сарадње агенција и јавности и осталих друштвених актера значајно варира. Земље централне Европе, посебно Аустрија, инсистирају на формализованом укључивању званично регистрованих организација са великим бројем чланова и то истичу као кључну предност свјих система, док друге земље, попут Велике Британије, више цене неформалне *ad-hoc* облике добровољног учешћа. У неким земљама Југоисточне Европе, попут Румуније и Србије, постоји тенденција да се од владе очекује висок допринос у заштити грађана, уз све више формалног волонтеризма. Грађани очекују од владе да обезбеди основни степен заштите у ванредним ситуацијама и кризама, а посебно када се ради о другим питањима који оптерећују државу, као што су привредни раст, незапосленост или заштита животне средине.

Такође, истраживање АНВИЛ-а показује општи низак ниво знања грађана у погледу кризе и спремности на реаговање (просек 27% за чланице Европске уније[289]), што указује на одређене недостатке од јавног интереса и свести, али се може тумачити

[289] Ibid

и као знак неповерења у земље чланице ЕУ. У периоду од 2000-2012. године само четири АНВИЛ земље тражиле су помоћ у току катастрофа два или више пута (Француска, Мађарска, Италија, Словачка), шест земаља добило је помоћ једном или два пута (Чешка Република, Ирска, Пољска, Румунија, Шведска, Велика Британија) док 12 земаља није добило никакву помоћ (Аустрија, Хрватска, Естонија, Финска, Немачка, Летонија, Литванија, Малта, Холандија, Норвешка, Србија, Швајцарска). Захтев за помоћ никад није тражила Немачка, која експлицитно истиче став да велике и јаке земље морају бити у стању да саме управљају великим кризама.

Механизам цивилне заштите је у Европској унији на снази од 2001. године и тренутно се налази у фази реформисања. Грађани Европе великом већином (преко 70%)[290] верују да је заједничка акција земаља Европске уније примеренија од решавања ванредних ситуација акцијама појединачних држава.

5.2. Политике заштите критичних инфраструктура у технолошки развијеним државама

5.2.1. Сједињене Америчке Државе

У САД-у се критична инфраструктура према Закону о уједињењу и јачању Америке кроз обезбеђивање одговарајућих средстава потребних за прекидање и спречавање тероризма. (USA PATRIOT ACT)[291] из 2001. године, у поглављу 1016е, дефинише на следећи начин: "термин *критична инфраструктура* означава системе, сервисе и постројења, физичке и виртуелне, који су толико витални за САД да њихово онеспособљавање или уништавање може да има врло негативан утицај на безбедност, националну економију, јавно здравље, или комбиновани негативни утицај на све ове наведене области".[292]

На основу горње дефиниције, 7. председничка директива Службе државне безбедности (HSPD7 – *Homeland Security Presidential Directive 7*), из децембра 2003. године, идентификовала је 17 *Критичних сектора* и *кључних ресурса* и дала кратки приказ улога и одговорности укључених страна у процесу заштите ових сектора.

[290] Ibid

[291] USA PATRIOT ACT (пун назив на енглеском: *Unitingand Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*), настао је као одговор на терористичке нападе који су задесили САД 11. септембра 2001. године. Донет је од стране америчког конгреса, а званично га је потписао и озваничио Џорџ Буш 26. октобра 2001.

[292] Macaulay, T., (2008), *Critical Infrastructure - Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies*, CRC Press, London, p. 8

Национални план заштите инфраструктуре из 2006. године[293] и стратегија Службе државне безбедности из 2007. године[294] потврдиле су ову листу од 17 критичних сектора изнету у Председничкој директиви и одговарајући распоред дужности и улога у процесу заштите инфраструкуре. Ипак, листа критичних инфраструктурних сектора и ресурса није финална и могуће су њене измене (у смислу додавања нових критичних сектора). У поменутој председничкој директиви стоји да: "Служба државне безбедности (*Department of Homeland Security* − DHS) треба да континуирано врши процену неопходности да се одређени сектори и ресурси уврсте у критичне".[295] Захваљујући овој одредби, Служба државне безбедности је у марту 2008. године уврстила сектор индустријске производње[296] на листу критичних сектора. На тренутној листи критичних инфраструктурних сектора у САД-у налазе се:[297]

- Информационе технологије (ИТ),
- Телекомуникације,
- Хемикалије,
- Комерцијалне установе,
- Бране,
- Нуклеарни реактори, нуклеарни материјали и нуклеарни отпад,
- Институције Владе,
- Саобраћајно-транспортни систем (који укључује инфраструктуру неопходну за функционисање масовног транспорта, авио-саобраћаја, водног, друмског и железничког саобраћаја и система цевовода),
- Хитне службе (службе за које реагују у ванредним ситуацијама),
- Поштанске и шпедитерске службе и сервиси,
- Пољопривреда и производња хране,

[293] Department of Homeland Security, (2006), "National Infrastructure Protection Plan", Washington, p. 3; Документ се може наћи на интернет адреси: http://cipp.gmu.edu/archive/NIPP_Plan6-06.pdf 17.11.2012
[294] The White House, (2007), "National Strategy for Homeland Security", Washington, p. 27; Документ о националној стратегији доступан је на сајту Беле куће: http://www.whitehouse.gov/infocus/homeland/nshs/NSHS.pdf 17.11.2012
[295] The White House, (2003), "Homeland Security Presidential Directive/ HSPD-7", Washington, 17.12.2003, part 15; Документ је доступан на сајту Беле Куће: http://www.whitehouse.gov/news/releases/2003/12/200312175.html 17.11.2012
[296] Под критичном индустријском прозводњом обухваћени су следећи сектори: примарна метална индустрија (производња челика, гвожђа, алуминијума и њихових легура), фабрике за производњу мотора и турбина фабрике за производњу електричне опреме и компоненти и фабрике за проиводњу транспортних средстава (аутомобила, авиона, возова и вагона). Детаљнији опис елемената који чине сектор критичне производње може се наћи на сајту Одељења државне безбедности: http://www.dhs.gov/critical-manufacturing-sector 17.11.2012
[297] Ibid

- Јавно здравље и здравствена нега,
- Вода за пиће и системи за третирање отпадних вода,
- Енергетика (под чим се подразумевају постројења за производњу, рафинисање, складиштење и дистрибуцију нафте и гаса, електричне струје (осим за комерцијална нуклеарна постројења)
- Банкарство и финансије,
- Национални споменици и знаменитости,
- Индустријска производња за потребе одбране земље и
- Критична индустријска производња.

5.2.1.1. Преглед садашњих и будућих иницијатива и мера које САД предузима у циљу заштите критичне инфрасртуктуре

Још од деведесетих година 20. века до данас заштита целокупне (посебно критичне информационе инфраструктуре) у САД представља изузетно важну ставку у федералној стратегији националне безбедности. Стратегија националне безбедности из 2007. године указује на значај заштите критичне инфраструктуре, пре свега информационе критичне инфраструктуре зато што се "функционисање великог дела есенцијалних сервиса и служби, као и скоро целокупна критична инфраструктура ослањају на неспутано коришћење интернета и комуникационих система, података, мониторинг и контролних система у чијем је саставу информациона (сајбер) инфраструктура. Сајбер-напади могу да имају изузетно негативан утицај на готово све секторе критичне инфраструктуре који у огромној мери зависе од информационе инфраструктуре, што на крају може да изазове негативне последице по економију и националну безбедност".[298]

С обзиром на то да одговорност за очување националне безбедности по правилу преузима Влада САД-а уз помоћ разних државних органа и институција (војске, министарстава спољних и унутрашњих послова, обавештајних служби), очување и заштита критичне инфраструктуре посматра се као заједничка одговорност која захтева координисану акцију великог броја државних сектора.[299] Пошто је број актера који су укључени у заштиту критичне инфраструктуре у САД-у јако велик, америчка Влада

[298] "National Strategy for Homeland Security", p. 28
[299] Ibid, p. 4

развила је низ институција, иницијатива, директива и правила реаговања како би се обезбедила координисана акција свих учесника, као што су:[300]

- *Председничка комисија за заштиту критичне инфраструктуре (Presidential Commissionon Critical Infrastructure Protection* − PCCIP*)*, је био први покушај да се укаже на рањивост ове инфраструктуре у САД-у.[301]

- *Председничке директиве 62 и 63 (Presidential Decision Directives (*PDD*) 62 and 63)* изнете су у мају 1998. године у склопу председничке одлуке.[302] Директивом 63 установљене су радне групе у оквиру Федералне Владе и позива се на дијалог између Владе и приватног сектора, како би се формирао Национални план обезбеђења инфраструктуре.[303]

- *Национални план за заштиту информационих система* представљен од председника САД 7. јануара 2000. године први је опсежни Национални план за заштиту критичне информационе инфраструктуре, чији је фокус био на обезбеђивању сајбер-компоненти критичне инфраструктуре. Пун назив овог плана био је Одбрана сајбер-простора Америке.[304] Овај план је указао на то да сајбер-безбедност представља заједничку одговорност Владе и приватног сектора.

- *Извршне наредбе о оснивању службе националне безбедности и Савета за националну безбедност* од 8. октобра 2001. године, првом наредбом председика (ЕО 13228), основана је Служба националне безбедности и са њом повезан Савет за националну безбедност.[305] Другом наредбом (ЕО 13231) под називом *Заштита критичне инфраструктуре у информационом добу*, установљен је Председнички одбор за заштиту критичне инфраструктуре. Задатак одбора је да "препоручује начин вођења политике заштите критичне инфраструктуре и да координише извршења програма заштите информационих система битних за функционисање свих осталих сектора критичне инфраструктуре".[306] Овом наредбом такође је установљено Национално

[300] Ibid
[301] The President's Commission on Critical Infrastructure Protection (PCCIP), "Critical Foundations: Protecting America's Infrastructures", Washington, 1997.
[302] William, J. C., (1998), "Protecting America's Critical Infrastructures: Presidential Decision Directives 62 and 63", Washington.
[303] Ibid
[304] William, J. C., (2010), "Defending America's Cyberspace: National Plan for Information Systems Protection Version1.0", An Invitation to a Dialogue, Washington.
[305] George, W. B., (2001), "Executive Order 13228", Establishing the Office of Homeland Securityand the Homeland Security Council, Washington: http://www.fas.org/irp/ offdocs/eo/eo-13228.htm 17.11.2012
[306] George W. B., (2001), "Executive Order 13231", *Critical Infrastructure Protection in the Informaion Age*, Washington, http://www.fas.org/irp/offdocs/eo/eo-13231.htm 17.11.2012

саветодавно веће за инфраструктуру[307] (*National Infrastructure Advisory Council* − NIAC), као председнички саветодавни орган састављен од власника и оператера критичне инфраструктуре државе.

- *Председничка директива Службе националне безбедности (HSPD-7)* од 17. децембра 2003. године издата је председничка директива Службе за националну безбедност (HSPD-7), која смењује председничку директиву 63 (PDD63) из маја 1998. године, као и све остале раније издате председничке директиве. Овом директивом установљен је став који сва одељења, све федералне службе и агенције треба да заузму кад је у питању заштита критичне инфраструктуре од терористичких напада.[308]

Директивом се именује Секретар за националну безбедност који треба да буде "највиши федерални званичник који ће водити, интегрисати и координисати све акције везане за заштиту националне безбедности, критичне инфраструктуре и кључних ресурса и који ће активно сарађивати и подстицати сарадњу између федералних одељења и служби, затим између државне и локалних влада и приватног сектора".[309]

- *Национална стратегија* државне безбедности објављена је јула 2002. године и њоме је постављена основа за заштиту критичне инфраструктуре у САД. У фебруару 2003. године Бела кућа издала је две председничке националне стратегије – националну стратегију о обезбеђивању сајбер-простора и националну стратегију за физичку заштиту критичне инфраструктуре и кључних ресурса, оне представљају пратеће документе уз националну стратегију државне безбедности.

- *Национална стратегија Службе државне безбедности*[310] донета јула 2002. а ажурирана октобра 2007. године везана је за одбрану САД од терористичких напада.[311] Једна од шест *критичних мисија* које се налазе у Националној стратегији је и заштита критичне инфраструктуре и кључних ресурса.

- *Национална стратегија обезбеђивања сајбер-простора* (*National Strategy to Secure Cyberspace* − NSSC)[312] указала је на важност изазова који представља обезбеђивање сајбер-простора. Стратегијом се сајбер-простор дефинише као *међузависна мрежа информационих инфраструктура* и сликовито указује на то да

[307] Ibid
[308] http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html 17.11.2012
[309] Ibid
[310] Papa, M., and Shenoi, S., (2008), Critical Infrastructure Protection II, International Federation for Information Processing, New York, p. 21-22
[311] Office of Homeland Security, (2002), "National Strategy for Homeland Security", Washington, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf 17.11.2012
[312] The White House, (2003), "National Strategy to Secure Cyberspace", Washington, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf 17.11.2012

сајбер-простор представља *нервни односно контролни систем америчког друштва*. Стратегија настоји да прецизно дефинише националну политику на пољу заштите сајбер-простора.

У складу са Националном стратегијом државне безбедности циљеви Националне стратегије обезбеђивања сајбер-простора су следећи:[313]

- Превенција сајбер-напада на националну критичну инфраструктуру,
- Смањење рањивости државе на сајбер-нападе,
- Минимизирање оштећења насталих услед сајбер-напада и опоравак инфраструктуре након ових напада.

- *Национална стратегија физичке заштите критичне инфраструктуре и кључних ресурса*[314] наглашава да критични инфраструктурни сектори САД-а и њихово неометано функционисање представљају основу националне безбедности, управе, економске стабилности и *америчког начина живота*. Главни циљ ове стратегије је смањење рањивости државе услед терористичких напада смањењем рањивости националне критичне инфраструктуре и кључних ресурса услед физичких напада.

Служба државне безбедности одговорна је за целокупну међусекторску координацију активности у овој организационој шеми и представља везивно ткиво које спаја све одговорне федералне агенције, државне и локалне управе и приватни сектор. Активности које Служба државне безбедности надзире и потпомаже су планирање и алокација ресурса, размена информација, истраживање и развој заштитних мера, моделирање, симулација и анализа могућих напада. Служба државне безбедности обавља и провере свог особља у свим институцијама које учествују у активностима везаним за физичку заштиту критичне инфраструктуре и брине о безбедности особља.

- *Национални план заштите инфраструктуре и појединачни планови заштите критичних сектора* (*National Infrastructure Protection Plan* − NIPP), који дефинише оквире за спровођење постојећих и будућих пројеката програма и активности у циљу заштите критичне инфраструктуре и кључних ресурса донела је Служба државне безбедности у јуну 2006. године. Планом су дефинисана три различита концепта заштите: одвраћање терориста од напада на критичну инфраструктуру, смањење степена рањивости државе и критичне инфраструктуре, ублажавање потенцијалних последица.

---

[313] Ibid

[314] The White House, (2003), "*National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*", Washington

Појединачни планови заштите критичне инфраструктуре по секторима,[315] представљају допуну Националног плана заштите критичне инфраструктуре и додатно објашњавају начине на које се врши имплементација Националног плана у различитим критичним инфраструктурним секторима. Стога су за заштиту националне имовине идентификована основна министарства, која морају да преузму надлежност. Главну одговорност сносе Министарство националне безбедности, министарство одбране и унутрашњих послова. У тим активностима учествују и остала министарства попут Министарства енергетике, правде, државне управе, здравља, финансија и др.

- *Национална стратегија за размену података* објављена је октобра 2007. године[316] и даје смернице за безбедну размену података између различитих организација, агенција и служби, у сврху заштите критичне инфраструктуре. Стратегија јасно указује на неопходност размене података које "треба да буде правило, а не изузетак".[317]

5.2.1.2. Организациона структура система заштите критичне инфраструктуреу САД

Напади који су САД задесили 11. септембра 2001. године подстакли су реструктурирање целокупног организационог оквира очувања националне безбедности укључујући и оне који се тичу заштите критичне инфраструктуре (ЗКИ). У националној стратегији ЗКИ и кључних материјалних добара САД идентификовани су основни елементи инфраструктуре које је неопходно заштитити у условима различитих кризних ситуација.[318] Сектор хране и агрокултуре обухвата 1.912.000 фарми и 87.000 плантажа, сектор водоснабдевања обухвата 1.800 федералних резервоара и 1.600 локалних капацитета за водоснабдевање, област јавног здравства односи се на 5.800 регистрованих болница. Базна индустрија, која је у функцији одбрамбеног система, садржи 250.000 фирми и 215 индустрија, док телекомуникације обухватају 2.000.000.000. (две милијарде) миља каблова. Енергетски сектор је подељен на област електричне енергије, која поседује 2.800 енергетских постројења, и област нафте и гаса, која има 300.000 хиљада производних објеката. Ресурси транспорта веома су разноврсни и садрже 5.000 јавних аеродрома, 120.000 миља главних путева, 590.000

[315] Department of Homeland Security, (2007), "*Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*", Washington.
[316] The White House, (2007), "National Strategy for Information Sharing", Washington, http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf 17.11.2012
[317] Ibid, p. 1
[318] The White House, (2003), "*National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*", Washington

мостова, 200.000 миља гасовода, 300 лука, 500 главних, урбаних и јавних прелаза. Финансијски сектор обухвата 26.000 осигуравајућих институција. Хемијска индустрија која се користи заступљена је са 66.000 постројења. Нуклеарних електрана има 104, као и 80.000 насипа.[319]

У оквиру разних сектора, велики број агенција је укључен у заштиту и у координирање акција у оквиру истих (Националним планом за заштиту инфраструктуре прописано је да одговорност за заштиту критичне инфраструктуре у оквиру посебних сектора преузимају баш те агенције).[320] Навешћемо најбитније.

- *Служба државне безбедности (Department of Homeland Security* − DHS*)* координише све акције везане за заштиту критичне инфраструктуре. Марта 2003. године, 23 федералне агенције, програми и канцеларије спојене су у једна орган – Службу државне безбедности.[321] која координише акције више федералних, државних и локалних управа и обухвата велики број агенција које обављају различите задатке везане за државну безбедност.[322] Унутар Службе државне безбедности агенције које се баве заштитом критичне инфраструктуре међусобно су спојене са Директоратом за националну заштиту и програме, чији је задатак редуковање физичких и виртуалних претњи државној безбедности.[323] Две канцеларије у оквиру Службе државне безбедности баве се заштитом критичне инфраструктуре: Канцеларија за заштиту инфраструктуре (*Office of Infrastructure Protection* − OIP) и Канцеларија за сајбер-безбедност и телекомуникације (*Office for Cyber security and Communications* − CS&C).

- *Канцеларија за заштиту инфраструктуре (Office of Infrastructure Protection* − OIP*)*[324] координише акције у различитим секторима везане за заштиту критичне инфраструктуре и кључних ресурса. Неки од задатака ове канцеларије су:[325]

  - Управљање организацијом која се бави идентификацијом критичне инфраструктуре и кључних ресурса, координацијом и заштитом те инфраструктуре,
  - Развој, спровођење и ажурирање Националног плана заштите инфраструктуре,

[319] Purpura, A., (2007), Terorism and Homeland Security, The Maple-Vail Book Manufacturing Group, British Library, Cataloguing in Publication Data.
[320] "National Infrastructure Protection Plan", p. 92
[321] http://www.dhs.gov/xabout/history/editorial_0133.shtm 29.11.2012
[322] http://www.dhs.gov/xabout/structure/index.shtm 29.11.2012
[323] http://www.dhs.gov/xabout/structure/editorial_0794.shtm 29.11.2012
[324] http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm 29.11.2012
[325] Ibid

- Кординација и асистирање приликом процене рањивости свих 18 критичних инфраструктурних сектора и кључних ресурса у САД-у и обавештавање власника и оператера критичном инфраструктуром о стандардима везаним за безбедност инфраструктуре које морају испунити,
- Контролисање управа одговорних за управљање критичном инфраструктуром и контрола размене података,
- Прикупљање података, анализирање ризика и претњи по критичну инфра-структуру и пружање информација Влади и приватном сектору о начину постављања приоритета приликом алокације ресурса и
- Успостављање и одржавање међународних програма и односа, којима се промовише глобална култура заштите критичне инфраструктуре.

- *Канцеларија за сајбер-безбедност и телекомуникације (Office for Cyber Security and Communications* - CS&C*)*[326] координише, заједно са приватним сектором, акције идентификовања претњи, управљања ризицима и унапређења свести о ситуацији, како би читава држава била припремљена за катастрофалне инциденте, који би могли да оштете или чак униште мрежу информационих и комуникационих технологија.[327] Канцеларија за сајбер-безбедност и телекомуникације извршила је имплементацију три програма:

1. *Национални систем за комуникацију* (*National Communications System* − NCS)[328] има задатак да осигура националну безбедност и омогући комуникацију у ванредним ситуацијама између свих органа федералне управе и под свим условима.
2. *Национално одељење за сајбер-безбедност* (*National Cyber Security Division* − NCSD)[329] сарађује са државним, приватним и међународним партнерима на заштити информационе инфраструктуре. Овај задатак обавља и кроз сарадњу са партнерима на развијању и имплементацији програма управљања ризиком и кризног менаџмента у функцији заштите критичне информационе инфра-структуре.

[326] Papa, M., and Shenoi, S., (2008), *Critical Infrastructure Protection II – Cyberspace Policy for Critical Infrastructures*, International Federation for Information Processing, New York, p. 17-31
[327] http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm 29.11.2012
[328] http://www.ncs.gov/about.html 29.11.2012
[329] http://www.dhs.gov/xabout/structure/editorial_0839.shtm 29.11.2012

3. *Канцеларија за комуникацију у ванредним ситуацијама* (*The Office of Emergency Communications* − OEC)[330] бави се развојем, имплементацијом и координацијом интероперабилне и операбилне комуникације на свим државним нивоима за потребе реаговања у ванредним ситуацијама.

- *Министарство спољних послова* (*State department*) има уставна овлашћења да управља спољним пословима и стога обавља и међуагенцијску координацију кад је у питању заштита критичне инфраструктуре у складу са међународним програмима. Стејт департмент блиско сарађује са Министарством одбране САД-а (*Department of Defense* - DoD) на развоју и имплементацији међународних иницијатива оформљених са циљем да охрабре сарадњу између држава, како би се побољшала безбедност критичних инфраструктурних сектора и кључних ресурса од којих зависе операције и функционисање америчке војске.[331]

- *Оба дома Конгреса САД* оформила су своје органе који се баве питањима заштите критичне инфраструктуре. У оквиру Комисије за државну безбедност Представничког дома Конгреса, проблемима заштите критичне инфраструктуре баве се следеће поткомисије:[332]

- Поткомисија за безбедност транспорта и заштиту критичне инфраструктуре,
- Поткомисија за нове претње по критичну инфраструктуру, сајбер-безбедност, науку и технологију,
- Поткомитет за обавештавање, размену података и процену ризика од тероризма.

У оквиру Комитета за правосуђе[333] америчког Сената налази се поткомитет за тероризам, технологију и државну безбедност, који има надзор над законима везаним за информациону политику Владе, електронском приватношћу, безбедношћу рачунара и над Законом о слободи информација.[334]

Комитет за државну безбедност и послове владе[335] америчког Сената има јурисдикцију над већином безбедносних питања везаних за државну безбедност, укључујући и јурисдикцију над питањима везаним за заштиту критичне инфраструктуре. Његови поткомитети за управљање државним финансијама,

[330] http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm 29.11.2012
[331] http://www.state.gov/t/pm/ppa/icipt 29.11.2012
[332] http://homeland.house.gov/about/index.asp 29.11.2012
[333] http://judiciary.senate.gov 29.11.2012
[334] http://judiciary.senate.gov/subcommittees/110/technology110.cfm 29.11.2012
[335] http://hsgac.senate.gov/public 29.11.2012

обавештавање владе и међународну безбедност имају јурисдикцију над питањима везаним за безбедност информационе инфраструктуре.

- *Истражна канцеларија Владе (Government Accountability Office* − GAO)[336] представља истражни орган Конгреса. То је независно и непристрасно тело које се бави истраживањем и праћењем трошкова Владе, ради на препорукама којима би требало да се побољша учинак и осигурају надлежности Владе. Конгрес често захтева од Истражне канцеларије да проучи програме и расходе Владе. Канцеларија је за време свог постојања издала неколико извештаја и исказа везаних за заштиту критичне инфраструктуре и информациону безбедност.[337]

- *Министарство одбране САД (Department of Defense* − DoD*)* је маја 2007. године објавило План заштите критичне војно-индустријске инфраструктуре, као додатак Националном плану заштите инфраструктуре (*National Infrastructure Protection Plan*) из 2006. године.[338] Критична војно-индустријска инфраструктура укључује Министарство одбране, Владу САД и компаније из приватног сектора, које дизајнирају, производе, дистибуирају и одржавају војне оружане системе, подсистеме, компоненте или делове за такве системе. Војно-индустријска критична инфраструктура не укључује комерцијалну комуникациону и информациону инфраструктуру, чија заштита је прописана другим плановима о заштити инфраструктуре. Програме обезбеђивања информационионе инфраструктуре спроводила је Канцеларија заменика секретара за одбрану мрежа и информациону интеграцију (*Office of the Assistant Secretary of Defense for Networks and Information Integration* − (OASD/NII),[339] а којима је управљао главни официр за информатику Министарства одбране.

- *Одељење за компјутерски криминал и интелектуалну својину* (CCIPS) при Министарству правде, одговорно је за имплементацију националних стратегија министарства везаних за борбу против компјутерског криминала и повреда интелектуалне својине широм света.[340]

- *Системи за аутоматизацију и управљање индустријским процесима, њихова рањивост и начини заштите у оквиру програма заштите критичне инфраструктуре (Supervisory Control And Data Acquisition* − SCADA) имају широку примену у управљању и праћењу рада индустријских постројења и опреме (као што је

[336] http://www.gao.gov/about/index.html 29.11.2012
[337] United States Government Accountability Office (GAO), (2005), "Information Security: Federal Agencies Need to Improve Controls over Wireless Networks", http://www.gao.gov/new.items/d05383.pdf 29.11.2012
[338] http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf 29.11.2012
[339] http://www.defenselink.mil/cio-nii/index.shtml 29.11.2012
[340] http://www.usdoj.gov/criminal/cybercrime/index.html 29.11.2012

водопривреда и хемијска индустрија) али и у телекомуникацијама, енергетици и системима управљања. SCADA системи служе за аутоматизацију индустријских процеса, односно за прикупљање података са сензора и инструмената лоцираних на удаљеним станицама као и за пренос и приказивање тих података у централној станици у сврху надзора или управљања. Прикупљени подаци се обично посматрају на једном или више SCADA рачунара у централној станици. SCADA систем може да прати и управља и до стотинама хиљада улазно-излазних вредности.[341]

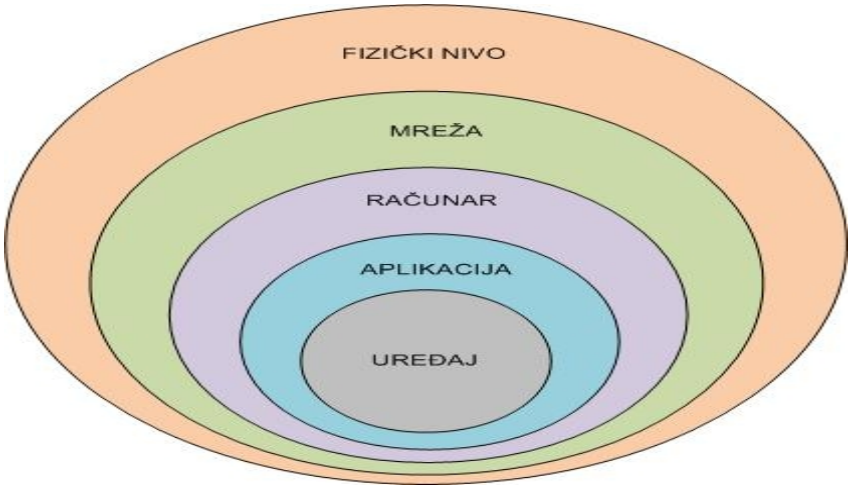
За заштиту SCADA мрежа у САД користи се неколико приступа од којих је најчешћи и основни тзв. *Defense in Depth* модел. Овај модел представља безбедносни концепт Америчке службе државне безбедности (*US Department of Homeland Security*), заснован на контроли на више нивоа унутар IT мреже. Овај приступ подразумева контролу на више нивоа и обухвата све видове заштите мреже који се могу поделити у слојеве. То може бити *firewall* уређај, заштита портова на свичевима, мењање шифри приступа с времена на време и све друго што доприноси додатној сигурности у мрежи сматра се одређеним слојем (нивоом) безбедности. У оквиру овог модела мрежа се сегментира на демилитаризовану зону (ДМЗ), корпоративну мрежу, контролну мрежу и удаљене станице. Свакој зони се додељују права приступа.[342]

У пракси овај модел се имплементира кроз неколико нивоа:[343]

1. Безбедност физичког нивоа − физичка заштита уређаја, блокирање неискориш-ћених портова, заштита каблова од случајних или намерних искључивања, закључавање опреме у одговарајућим рековима. Безбедност на овом нивоу се постиже ограничавањем физичког приступа опреми.
2. Мрежни периметар − између локалне мреже и спољашње поставља се *firewall* уређај; на основу заглавља пакета *firewall* одређује да ли ће пропустити пакет или не; овај уређај може да провери да ли постоје *рупе* у мрежи које би биле мета *нападача*. Поред овога, за заштиту мрежног периметра могу се користити и IDS (*Intrusion Detection System* – Систем за детектовање незакони-тих упада) и IPS (*Intrusion Prevention System* – Систем за превенцију незаконитог упада) технологије.

[341] Маринковић, Д., (1998), "*Основе прикупљања података и управљања*", Микроелектроника, Београд, бр. 1, мај.
[342] Recommended Practice, (2009), "Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies", Homeland Security, October
[343] Didier P., F.Macias, J. Harstad, R. Antholine, S. A. Johnston, S. Piyevsky, M. Schillace, G. Wilcox, D. Zaniewski, S. Zuponcic, (2011), "*Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*", CISCO Systems and Rockwell Automation, September, pp. 252-255

3. Осигуравање рачунара – управљање програмским *закрпама* и употреба антивирус апликација.
4. Безбедност апликације – заштита управљачких апликација преко метода аутентикације и ауторизације.
5. Осигуравање уређаја, контрола административних промена на уређају, забрана приступа неауторизованом лицу конфигурационим параметрима уређаја.



Слика бр. 5.1. - Графички приказ нивоа заштите у оквиру 'Defense in Depth' модела[344]

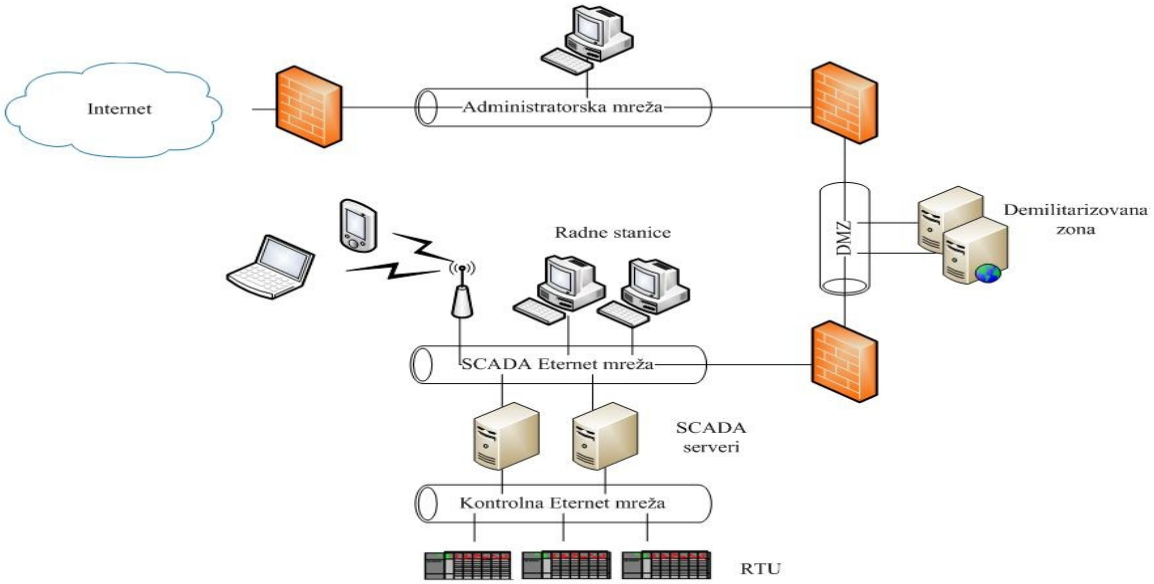
За SCADA систем критичне позиције су:[345]

- Рупе у мрежном периметру,
- Рањивост отворених протокола (OPC – *OLE for Process Control*),
- Напади на RTU (*Remote Terminal Unit*) уређаје (RTU уређаји представљају микропроцесоре који посредују између централног сервера и удаљене опреме у оквиру SCADA архитектуре; у суштини помоћу њих се обавља прикупљање података са удаљених станица у оквиру SCADA система),
- Напади на сервере и
- Напади на комуникацију.

У оквиру *Defensein Depth* стратегије препоручује се раздвајање мреже у мрежне сегменте, којима су додељена различита права (стварање демилитаризованих (ДМЗ) зона, одвајање IT мреже од контролне). По *Defense in Depth* топологији за креирање

[344] "Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies", *Homeland Security*, October 2009; Цукић, Н., Кисић, С., Мандић-Лукић, Ј., (2012), *Безбедност SCADA система*, извештај са 11. скупа Инфотех Јахорина, март, стр. 397
[345] Ibid

ДМЗ зоне, између сваког сегмента би требало да се постави по *firewall* уређај за филтрирање пакета.



Слика 5.2. – Графички приказ постављања firewall уређаја за филтрирање пакета ради креирања демилитаризованих (ДМЗ) зона и одвајања ИТ мреже од контролне[346]

- *Приватно-јавна партнерства* су један од најбитнијих предуслова ефикасне заштите критичне инфраструктуре у САД-у. Председничка комисија за заштиту критичне инфраструктуре (*The President's Commission on Critical Infrastructure Protection* - PCCIP) донела је закључак да је неопходност заштите инфраструктуре даље условила неопходност поделе одговорности и сарадње приватног и јавног сектора.[347] Од тад, приватно-јавна партнерства и квалитетна размена података између приватног и јавног сектора представљају један од најбитнијих задатака у процесу заштите критичне инфраструктуре у САД-у.

У наставку дајемо преглед најбитнијих облика приватно-јавних партнерстава у областима заштите критичне инфраструктуре и сајбер-безбедности.

Међуагенцијски комитети Службе државне безбедности су одговорни за координацију и надзор сарадње приватног и јавног сектора као – Национално

[346] Цукић, Н., Кисић, С., Мандић-Лукић, Ј., (2012), *Безбедност SCADA система*, извештај са 11. скупа Инфотех Јахорина, март, стр. 398
[347] The President's Commission on Critical Infrastructure Protection (PCCIP), стр.35

саветодавно веће за инфраструктуру[348] и Саветодавно веће за партнерства (сарадњу приватног и јавног сектора) приликом заштите критичне инфраструктуре.[349]

Национално саветодавно веће за инфраструктуру (The National Infrastructure Advisory Council − NIAC*)* врши функцију саветовања председника о заштити критичних инфраструктурних сектора и информационих система. Веће је састављено од максимално 30 чланова из редова приватног сектора, академске заједнице и представника државних и локалних власти, а све чланове именује председник САД-а.

Саветодавно веће за сарадњу приликом заштите критичне инфраструктуре (*Critical Infrastructure Partnership Advisory Council* − CIPAC) основано је 2006. године како би се олакшала и побољшала координација између акција које се предузимају у склопу федералних програма заштите инфраструктуре и акција заштите критичне инфраструктуре које предузима приватни сектор. Чланови Већа су представници свих релевантних приватних и јавних сектора – челници координационих већа приватног сектора, као и представници државних и локалних органа.

Програм заштите информација о критичној инфраструктури (The Protected Critical Infrastructure Information Program - PCIIP*)* тежи да заштити одређене информације које размењује приватни сектор, и да спречи њихово обелодањивање, услед постојања Закона о слободи информисања.[350]

Центри за размену и анализу података (Information Sharing and Analysis Centers − ISACs*)* приватног сектора су организације којима управља приватни сектор.[351] Функција центра за размену и анализу података је прикупљање, анализа и размена информација о безбедности, инцидентима и начинима одговора на кризне ситуације, између чланова једног центра као и између различитих центара.[352]

Инфрагард је облик партнерског односа између индустријског сектора и америчке Владе, коју у овом конкретном случају партнерства представља (заступа) Федерални истражни биро (*Federal Bureauof Investigation* - FBI). Инфрагард представља иницијативу, која је развијена ради охрабривања размене информација између чланова Владе и приватног сектора.

Национална алијанса за сајбер-безбедност (The National Cyber Security Alliance - NCSA*)* представља партнерство између индустријских сектора и владиних

[348] http://www.dhs.gov/xlibrary/assets/niac/NIAC_Brochure.pdf 12.12.2012
[349] http://www.dhs.gov/xprevprot/committees/editorial_0843.shtm 12.12.2012
[350] http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm 12.12.2012
[351] Radvanovsky, R., McDougall, A., (2010), *Critical Infrastructure, Homeland Security and Emergency Preparedness,* Second edition, CRC Press, Taylor & Francis Group, New York, p. 192-194
[352] Ibid, p. 194-223

организација, које настоји да својим активностима створи свест о сајбер-безбедности кроз едукационе садржаје. Циљ алијансе је подизање свести грађана о критичној улози коју информациона безбедност има у процесу заштите националне интернет инфраструктре и да подстакне кориснике рачунара да заштите своје кућне и мале пословне системе.[353]

Партнерство за безбедност критичне инфраструктуре (Partnership for Critical Infrastructure Security - PCIS*)*[354] проистекло је из иницијатива изнетих кроз Председничку директиву 63 (PDD 63), како би се омогућила међусекторска координација акција у циљу заштите критичне инфраструктуре, У октобру 2005. године Национално саветодавно веће за инфраструктуру (*National Infrastructure Advisory Council* − NIAC) препоручило је да Партнерство за безбедност критичне инфраструктуре буде нека врста међусекторског координационог механизма као део партнерског модела Службе државне безбедности, а што је остало до данас.

Међусекторска радна група за сајбер-безбедност (The Cross Sector Cyber Security Working Group - CSCSWG*)* функционише као форум, који на једном месту окупља представнике Владе и приватног сектора, како би се кроз сарадњу утврдили ризици по критичним секторима.

Међусекторском радном групом заједно управљају индустрија и влада. Радна група се фокусира на стратешка питања међусекторске сајбер-безбедности.

Институт за заштиту информационе инфраструктуре (Institute for Information Infrastructure Protection - I3P*)* којим управља Дартмут колеџ (*Dartmouth College*) представља конзорцијум водећих националних институција које се баве сајбер-безбедношћу, укључујући центре за академско истраживање, владине лабораторије и непрофитне организације.[355] Основан је септембра 2001. године, са основном улогом координације националних истраживања из области сајбер-безбедности, развој програма сајбер-безбедности и успостављање чвршћих веза између академске заједнице, индустрије и државних органа. Институт за заштиту информационе инфраструктуре идентификује и указује на проблеме заштите критичне информационе структуре.[356]

[353] http://www.staysafeonline.info 22.12.2012
[354] http://www.pcis.org/index.html 23.01.2013
[355] Brunner, M. E., and Manuel, S., (2009), *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich, p. 453
[356] http://www.thei3p.org 23.01.2013

Системи раног упозорења и пружања помоћи јавности служе за размену информација, што је један од основних фактора неопходних за ефикасну мрежу институција за рано упозорење.

*Координциони центар рачунарског тима за реаговање у ванредним ситуацијама при Карнеги Мелон Универзитету (*CERT - *Coordination Center, Carnegie Mellon University)* један је од најстаријих и најважнијих програма за рано упозорење у области информационе безбедности. То је државни истраживачки и развојни центар у склопу Карнеги Мелон Универзитета. Основан је 1988. године након што је компјутерски црв *Морис* срушио 10% светског интернета. Координациони центар функционише као координационо чвориште за експерте током безбедносних инцидената. Центар такође ради и на превенцији будућих инцидената.[357]

*Рачунарски тим за ванредне ситуације (*US-CERT*)* је у сарадњи са Службом државне безбедности САД-а, септембра 2003. године, оформио амерички рачунарски тим за ванредне ситуације (US-CERT).[358] Овај тим ради заједно са Националним одељењем за сајбер-безбедност (*National Cyber Security Division* - NCSD) на превенцији напада и смањењу степена рањивости интернета и интернет сервиса. Ове две службе су заједно основале Национални систем за узбуну услед опасности од кибер- напада – поуздани систем за упозоравање који државни органи нуде како приватним корисницима − аматерима, тако и технолошким експертима.[359]

Федерални истражни биро (Federal Bureau of Investigation - FBI*)*[360] изабран је 1997. године за прелиминирани национални центар за упозоравање у случају напада на инфраструктуру у САД-у. Има одговорност за развој аналитичких метода на основу којих би се добијале информације о променама безбедносне ситуације, новим претњама и ризицима који би могли да угрозе критичну инфраструктуру.[361]

Центри за размену и анализу података (Information-Sharing and Analysis Centers − ISACs*)* представљају системе раног упозорења, који пружају информације о претњама, рањивости и инцидентима. Центри за размену и анализу података сређују све информације које прикупе из различитих извора, анализирају их и на основу тога саопштавају упозорења и узбуњују чланове тих центара. Многи центри, као нпр.

[357] http://www.cert.org 23.01.2013
[358] Brunner, M. E., and Manuel, S., (2009), *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich, p. 454-455
[359] http://www.us-cert.gov 23.01.2013
[360] President's Commission on Critical Infrastructure Protection (PCCIP), (1997), "*Critical Foundations: Protecting America's Infrastructures*", Вашингтон, октобар
[361] William, J. C., (1998), "*Protecting America's Critical Infrastructures: Presidential Decision Directives 62 and 63*", Washington.

Центар за размену и анализу података у ИТ сектору (IT-ISAC), коначне информације које се добију анализом дистрибуирају кроз читав сектор, па и шире, како би сви релевантни сектори, као и јавност, били упознати са тренутном ситуацијом, потенцијалним претњама и ризицима.

Функција сајта www.onguardonline.gov, који је настао под покровитељством Владе САД-а, је давање препорука како би се помогло приватним корисницима рачунара. На сајту се налазе савети који би тебало да заштите кориснике од интернет превара и да их упуте на квалитетне начине заштите личних података. На веб-сајту су и чланци, видео материјали и интерактивни садржаји. Државна трговинска комисија (*Federal Trade Commission* − FTC) ради на одржавању сајта уз помоћ неколико министарстава и уз помоћ Службе државне безбедности.[362]

Законске регулативе везане за заштиту критичне инфраструктуре. Закон федералног саветодавног комитета из 1972. године (Federal Advisory Committee Act - FACA) донет је од стране Конгреса САД. Задатак овог закона је да спречи сваку особу или компанију да негативно утиче на доношење одлука државних органа. Закон није само формализовао процес оснивања, функционисања, надзора и прекида функционисања ових саветодавних тела, већ је на основу Закона настао и Секретаријат за управљање комитетима, чији је задатак био да контролише и подноси извештаје о функционисању извршних органа и усклађености деловања ових органа са Законом.

Закон о компјутерским преварама и злоупотребама из 1986. године (*Computer Fraud and Abuse Act* − CFAA) настао је као резултат неколико година истраживања и дискусије између законодаваца.[363] Законом су дефинисана два нова кривична прекршаја: неауторизовани приступ рачунарима од *државног интереса*[364] и неауторизована трговина компјутерским шифрама. Кршењем овог закона сматрало се и неовлашћено проваљивање у државне, финансијске и медицинске компјутере од *државног значаја*. Закон је проширен и пооштрен 1994. године, а посебно 2001. године, када је 26. октобра донет Закон о уједињењу и јачању Америке кроз

[362] http://onguardonline.gov/index.html 23.01.2013
[363] http://www4.law.cornell.edu/uscode/18/1001.html 23.01.2013
[364] Рачунари *од државног интереса* у Закону о компјутерским преварама и злоупотребама дефинисани су као два или више рачунара умешана у криминални прекршај, уколико су лоцирани у различитим државама.

обезбеђивање одговарајућих средстава потребних за прекидање и спречавање тероризма (USA PATRIOT ACT).[365]

Закон о државној безбедности из 2002. године[366] је формиран са основним разлогом одређивања законског оквира за функционисање Службе државне безбедности. Први део закона је посвећен дефинисању функција и начина деловања Службе државне безбедности, док се други део закона односи на анализу информација и заштиту инфраструктуре. Законом се такође предвиђа пребацивање већег броја федералних агенција које се баве заштитом критичне инфраструктуре, у састав Службе државне безбедности и прописује категорије информација којима секретар државне одбране има приступ.

Закон о слободи информисања (*Freedom of Information Act* - FOIA) регулише обавезе према држави, где је приватни сектор, који поседује или управља критичном инфраструктуром, дужан да редовно подноси извештаје о раду, али и да открива неке осетљиве информације везане за критичну инфраструктуру Влади САД-а.[367] Велики проблем представља чињеница да кад се ове информације нађу у Влади, на основу Закона о слободи информисања јавност може да захтева приступ тим подацима или њихово објављивање, што може да доведе критичне инфраструктурне секторе у опасност. Ово је превазиђено тако што су се на основу Закона о државној безбедности из 2002. године дефинисали изузеци из Закона о слободи информисања. Наиме у Закону о државној безбедности стоји да свака информација везана за критичну инфраструктуру (укључујући информације о безбедносним системима, системима упозорења, студијама међузависности различитих сектора итд) представља изузетак у односу на Закон о слободи информисања и не сме се обелодањивати јавности.

Након терористичких напада на САД 11. септембра 2001. године, Федерална регулаторна комисија за енергетику (*Federal Energy Regulatory Commission* − FERC) уклонила је неке информације са свог веб-сајта. Међу документима које је комисија уклонила са сајта налазиле су се детаљне мапе и информације о електранама, гасним и нафтним постројењима и фабрикама за прераду нафте и гаса. Иако се ове информације нису морале јавно приказивати, јер су изузете из Закона о слободи информисања, по некој врсти традиције ове информације биле су доступне читавој јавности. У фебруару

[365] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, 2001, http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf 23.01.2013

[366] President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations, 1997, p. 81

[367] Radvanovsky, R., Mc Dougall A., (2010), *Critical Infrastructure, Homeland Security and Emergency Preparedness,* Second edition, CRC Press, Taylor & Francis Group, New York, p. 268-270

2003. године Федерална регулаторна комисија за енергетику утврдила је правило да појединци који желе приступ овим информацијама морају да поднесу званичан захтев и да прођу све прописане безбедносне процедуре. У захтеву се морају навести сви тражени лични подаци, као и разлози због којих се тражи приступ подацима. Не постоје правила о томе да ли ће се и коме приступ информацијама дозволити, већ се одлучује за сваки случај посебно и дозвољене су само појединачне пријаве.

Закон о информацијама о критичној инфраструктури: процедуре за поступање са информацијама о критичној инфраструктури из 2002. године регулише да су све информације које Служба државне безбедности прослеђује државним и локалним органима, и обрнуто, у потпуности заштићене од свих закона који су повезани или сагласни са Законом о слободи информисања.

Закон о осигурању од ризика од тероризма из 2002. године је нови закон којим је омогућено креирање федералног програма за приватне и јавне компензације за осигуране губитке настале услед терористичких напада. Сва комерцијална осигуравајућа друштва морају да понуде осигурање од ризика од тероризма, а федерални органи су у обавези да и сами покрију део губитака, уколико дође до терористичког напада. У склопу овог закона, терористичким чином се сматра сваки чин насиља над елементима инфраструктуре.[368] То укључује како катастрофалне нападе на интернету и на разне интернет сервисе, тако и физичке нападе на инфраструктуру.

Природне катастрофе	**САД**
Број догађаја	640
Број настрадалих	12,366
Просечно настрадалих по години	399
Просечно погођених	26,889,582
Просечно погођених по години	867,406
Економска штета (у хиљадама $)	544,287,010
Економска штета по годинама (у хиљадама $)	17,557,645

Табела бр. 5.2. - Преглед природних катастрофа у САД (1980-2010)[369]

[368] Terrorism Risk Insurance Act of 2002, Pub, L. No. 107-297, 116 Stat. 2322
[369] Видери на интернет страници: Disaster Statistics, http://www.preventionweb.net 20.02.2015.

Кризе и катастрофе у савременом свету су реалност и део свакодневнице. У данашњем *глобалном селу* оне су постале глобална опасност и светски проблем. Будући да ови догађаји не познају никакве границе, они прете локалној заједници, држави, територији више држава, регији или чак континенту. Посебно је то показао и потврдио развој најважнијих безбедносних догађаја у посхладноратовском периоду, јер опстанак нација и грађана све више зависи од безбедности најважнијих функција друштва. Способност да се обезбеди функционисање власти и институција цивилног друштва и одржи критична инфраструктура и демократски принципи функционисања владиних институција су под огромним притиском у условима насталих кризних ситуација. У САД систем мониторинга и превенције катастрофа неопходан је из простог разлога што истраживања указују на то да се ризик од природних катастрофа и великих технолошких катастрофа константно увећава. Истовремено, из статистичких покатеља уочава се да се економски и укупни материјални трошкови ванредних ситуација, односно природних катастрофа, из године у годину повећавају. Према званичној статистици 640 ванредних догађаја збило се у САД у протеклих 30 година са укупном штетом преко 544 милијарде долара.

Графикон: Природне непогоде у САД

Извор: *Natural Disaster Occurence Reported*, http://www.preventionweb.net 23.02.2015.

Безбедносни изазови су у САД посебно дошли до изражаја после 11. септембра 2001. године, који је у потпуности променио концепте и инструменте за постизање опште безбедности, безбедности грађана и управљању кризама у нарастајућем

међузависном окружењу, посебно са становишта терористичког угрожавања критичне инфраструктуре још увек најмоћније силе света. Зато су САД предузеле свеобухватне стратегије у заштити критичне инфраструктуре, с основним циљем координираног и ефикасног одговора на ове ризике, што смо аргументовано и потврдили.

5.2.2. Русија

Током последњих неколико година Русија је начинила значајан напредак кад је у питању унапређење и заштита критичне инфраструктуре. Национална безбедност и економско благостање Руске Федерације зависе од стварног степена заштите критичне инфраструктуре, што ће у будућности бити још значајнија зависност, посебно кад је у питању информациона инфраструктура на коју ће се убудуће све више ослањати сви остали инфраструктурни сектори. Колико Русија брине о безбедности информационе инфраструктуре, може се закључити на основу напора који улаже на пољу заштите људских права у области информатике, на основу подршке сектору информационих технологија, развоја домаће информационе индустрије и на основу заштите информационих и телекомуникационих система у разним сферама јавног живота.

У Русији се следећи инфраструктурни сектори сматрају *критичним секторима*:

- економија,
- унутрашња и спољна политика,
- наука и технологија,
- државни информациони и комуникациони системи,
- одбрана,
- правосуђе,
- службе за реаговање у ванредним ситуацијама.

Руска доктрина информационе безбедности у складу је са Повељом групе Г8 о информатичком друштву, потписане на Окинави 2000. године.[370] Ипак, у руској доктрини информационе безбедности примећују се неке специфичности, проистекле из специфичне економске ситуације и дугорочних реформи, као и из искустава Русије са терористичким нападима.

[370] Okinawa Charter on Global Information Society, Okinawa, 22 July 2000, http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm 23.01.2013

5.2.2.1. Историјски осврт на еволуцију политике заштите критичне инфраструтуре у Русији

Ранија истраживања везана за руску политику заштите критичне инфраструктуре углавном су се везивала за реформу војске, модернизацију војно-индустријских комплекса, економију, спољну политику и сличне интересе.[371] С друге стране, Русија се често помињала и у западним дискусијама о сајбер-претњама. У овом контексту, Русија се сматра "постојбином неких од најкомпетентнијих сајбер-криминалних мрежа у свету"[372] и местом где обавештајна служба спроводи "застрашујући систем надзора, под именом СОРМ-2".[373] Први чеченски рат (1994–1996) и *први светски сајбер-рат* између Русије и Естоније 2007. године[374] представљају примере руске способности и спремности за борбу против сајбер-криминала, за учествовање у сајбер-рату и за заштиту своје информационе инфраструктуре. Истовремено у Русији се води јавна дебата о рањивости државне индустрије и других критичних објеката и постоји идеја да се то може поправити тиме што ће се унапредити информациона безбедност,[375] што је контрадикторно претходно изнетом ставу да је на пољу заштите информационе инфраструктуре Русија прилично оспособљена. Свеједно, фокусирање на само један елемент критичне инфраструктуре (информациона инфраструктура) не даје јасну слику о квалитету система заштите критичне инфраструктуре у Русији, па је стога неопходно проћи кроз историјат руске политике заштите критичне инфраструктуре. Највећи проблем Русије и заштите критичне инфраструктуре јесте тај што Русија има нешто више од 45.000 објеката који се сматрају опасним и преко 90 милиона људи који живе у зонама високог ризика.[376]

Концепт националне безбедноси Русије одобрен председничким декретом 11. јануара 2000. године ставља нагласак на карактеристике и развој мултиполарног света, затим износи идеју о статусу Русије као једне од највећих сила и, коначно, указује на

[371] Таква су на пример истраживања шведске одбрамбене истраживачке агенције о утицајима унутрашњег развоја Русије на перцепцију претњи по државу и формирање државне политике, затим рад В. Палина из 2011. године о руским војним капацитетима и десетогодишњој перспективи тих капацитета, и рад А. Савељева (март, 2011) о руској одбрамбеној доктрини и војној политици Русије.
[372] Glenny, M., (2011), "'The Cyber Arms Race Has Begun'", the Nation, October 31, p. 18
[373] СОРМ-2 је систем којим управља Федерална служба безбедности, која сакупља све податке који се појаве на руском интернету. (Glenny, M., (2011), "'The Cyber Arms Race Has Begun", The Nation, October 31, p. 18)
[374] KaIser, R., (2012), "*Estonia and the Birth of Cyberwar*", Presentation at Aleksanteri Institute, 4 October.
[375] Михаилов, А., (2010), *Критичесская инфраструктура оказалась в киберопасности*, Business FM, 17 November.
[376] Цаликов, П., Акимов, В. А., Козлов А., (2009), *Оценка природной, техногенной и екологической безопасности Росии*, ФГУ, МЦХС Росии.

покушаје других земаља да "ослабе Русију политички, економски, војно и на друге начине".[377] Овај концепт националне безбедности представља јасну промену у односу на претходну верзију концепта коју је одобрио председник Јељцин децембра 1997. године, а која говори о економској нестабилности као примарној претњи по Русију и помиње унутрашње проблеме пре него неке друге земље и алијансе, као изазове и претње по територијални интегритет Русије.[378] Иако су као главни извор претњи у концепту из 2000. године идентификовани спољни фактори, идентификовани су и бројни фактори унутар земље. *Погоршање унутрашње ситуације у држави и црпљење природних ресурса* поменути су између осталих као фактори који имају негативан утицај на стање економије и вољу друштва да схвати важност ових питања. Повезано са тим је и мишљење да "недовољна ефикасност законских и економских механизама за отклањање и решавање ванредних ситуација могу да доведу до повећања ризика од катастрофа које изазива људски фактор, у свим секторима економске активности".[379] Према томе, приоритетне области владиних активности у Русији обухватају "еколошки безбедно и нехазардно складиштење и/или коришћење деактивираног оружја, нуклеарне муниције, хемијског оружја" и "хитна заштита животне средине и формирање заштитних мера", које би требало да се прво примене у еколошки најопаснијим регионима у држави. Како би се извршили ови задаци, морају се установити побољшани, јединствени државни системи упозорења на опасност од катастрофа и помоћ грађанима" уз даље интегрисање тих система са сличним системима страних држава".[380]

Пре усвајања Концепта националне безбедности 1999. године, усвојен је први владин програм "за редукцију ризика и сузбијање последица ванредних ситуација насталих услед природних и технолошких катастрофа у Русији до 2005. године". Овај програм дао је кратак преглед основних принципа формирања већ поменутог јединственог система за упозорење и помоћ приликом катастрофа.[381] Програм, међутим, не идентификује специфичне инфраструктурне објекте као критичне, већ више говори о становништву и територији, који су рањиви у случају ванредних ситуација изазваних катастрофама природног или технолошког карактера. Циљ овог

[377] '*Concept of National Security of the RF*', approved by Presidential decree no. 24, 10 January 2000, p. 1–2
[378] "*Concept of National Security of the RF*", approved by Presidential decree no. 130, 17 December 1997.
[379] "*Concept of National Security of the RF*", p. 8
[380] Ibid, 16
[381] Правительство Росийской Федерации, *О федеральной целевой программе – Снижение рисков и смягчение последствий чрезвичайных ситуаций природного и техногенного характера в Росийской Федерации до 2005. года*, Постановление no. 1098, 29. Сентябрь, 1999.

програма је унапређење комплексног система превенције различитих типова криза, како би се омогућило смањење ризика по становништво које живи у регионима угроженим катастрофама за 40% до 50%.

Крајем 20. века политика Русије није била децидирано фокусирана на заштиту критичне инфраструктуре, већ се уместо тога оријентисала на *сверизични приступ*. Основа овог приступа формирана је кроз федерални **Закон о заштити становништва и територије од ванредних стања и опасности узрокованих природним и технолошким факторима**, који је ступио на снагу у новембру 1994. године. Овај Закон дефинише организационо-законске норме везане за заштиту становништва и окружења, а такође и за заштиту вода, ваздушног простора и објеката који су индустријски и друштвено значајни, од катастрофа изазваних природним и технолошким факторима.[382] Чињеница је да је овај програм превенције катастрофа био доста апстрактан, а није разматран ни у оквирима националне безбедности. Ситуација се доста променила неколико година касније.

У јулу 2003. године Владимир Рушаило, секретар Безбедносног већа (савета) Русије, изнео је предлог да Русија формулише принципе државне политике у областима безбедности околине и технолошке безбедности. Према Рушаиловим речима "циљ Закона је да уједини све ресурсе државне администрације, да унапреди тренутну законску регулативу, да развије технолошке основе и креира модеран јединствени систем физичке заштите (стратешких) објеката".[383] Тамбов је касније изабран као регион у ком ће се спровести пилот пројекат заштите критично важне инфраструктуре.[384]

Заједничка седница Безбедносног већа и Државног савета новембра 2003. године сматра се почетном тачком у формулисању руске политике у области заштите критичне инфраструктуре. Тада је истакнуто "да је заштита објеката критичних за националну безбедност од претњи везаних за технолошке и природне факторе, као и од тероризма изузетно битан задатак и да захтева заједничко деловање државних органа и *економских организама*.[385] Тада је још наглашено да је нова политика неопходна због

[382] *Федеральный Закон О защите населения и территории от чрезвичайныхситуаций природного и техногенного характера*, no 68-ФЗ, 21. Декабря, 1994.
[383] Поляков, Р., (2003), *Владимир Рушаило обсудил проблеми национальной безопасности Росии*, Коммерсант (Воронеж), 7. июля.
[384] Пројекат је био фокусиран на унапређење безбедности хемијске индустрије и унапређење система мониторинга у најгушће насељеним центрима (у овом случају у региону Тамбов).
[385] Путин, В., (2003), *Вступительное слово на совместном заседании Совета Безопасности и президиума Государственного совета по вопросу о повишении защити критически важных для*

исцрпљености руске инфраструктуре која је склона кваровима, као и због опасности од технолошких катастрофа. Стање је још сложеније и озбиљније због распрострањене незаинтересовано-сти за правила и норме који би бар мало смањили ризик. Уз све то, сваке године се на територији Русије појави све већи број разорних ветрова, земљотреса и шумских пожара. Како би се ови проблеми решили и предупредили, неопходно је било изменити државну политику.

Први скуп докумената којима се редефинишу државни интереси и циљеви у области заштите критичне инфраструктуре (документи везани за дефинисање критичних објеката и критичне инфраструктуре) појавио се децембра 2003. године. Државна политика унапређења хемијске, биолошке и нуклеарне безбедности поставила је основу за реформулисање целокупне политике заштите критичне инфраструктуре и померање од безбедносне политике у којој елементи критичне инфраструктуре као ни типови ванредних ситуација и опасности нису дефинисани (или су врло површно дефинисани) ка политици заштите критичних објеката од терористичких напада и других претњи по виталне људске активности, националну безбедност и социо-економски развој.[386] Тако је августа 2005. године представљен *концепт федералног система мониторинга* критично важних инфраструктурних објеката и опасних добара. Безбедносна политика је тада везана за критично важне објекте чији прекид функционисања може довести до негативних последица по економију и административно јединство државе, као и по безбедност и благостање становништва.[387]

Септембра 2006. године објављен је документ под називом "Концептуални основи државне политике у области заштите становништва и критично важних и потенцијално опасних објеката од ванредних ситуација изазваних природним и технолошким катастрофама и терористичким актима".[388]

Државна политика у области критичне инфраструктуре указује на следеће претње (опасности):[389]

национальной безопасности объектов инфраструктури и населения страны в условиях обострения угроз природного, техногенного и террористического характера, Москва, Кремль, 13. ноябрь.

[386] Президент РФ В. Путин, указ Пр-2194. *Основы государственной политики в области обеспечения химической и биологической безопасности РФ на период до 2010. года и дальнейшую перспективу*, 4. Декабря, 2003.

[387] Распоряжением Правительства РФ, *Концепция федеральной системи мониторинг критически важных объектов и/или потенциально опасных объектов инфраструктури РФ и опасных грузов*, но. 1314, стр. 27, 2005.

[388] Президент РФ В. Путин, *Основы государственной политики в области обеспечениябезопасности населения РФ и защищености критически важных объектов и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов*, 28. Сентябрья 2006.

[389] Ibid

- Увећање опасности која прети од технолошких и природних катастрофа, као и увећање броја оваквих катастрофа,
- Увећање броја потенцијално ризичних објеката, од којих су многи лоцирани у великим градовима и густо насељеним областима,
- Физичка истрошеност и технолошка заосталост система и комплекса оформљених како би унапредили безбедност ризичних објеката,
- Низак ниво образовања и обуке особља које ради у ризичним објектима, непостојање технолошке дисциплине, низак ниво безбедносне културе,
- Неадекватан степен финансирања мера којима се намерава побољшати безбедност становништва и менаџмент ризичних објеката,
- Увећана опасност од међународног и унутрашњег тероризма и повећање нивоа криминалитета и послова везаних за наркотике.[390]

5.2.2.2. Критеријуми за дефинисање критично важних објеката

Термин *заштита критичне инфраструктуре* ретко се користи у руској литератури и медијима. Уместо тог термина, овај феномен се разматра и о њему се дискутује уз коришћење различитих термина (стратешки објекти, ризични индустријски објекти, врло важни објекти, врло опасни и технички сложени објекти, потенцијално опасни објекти).[391] Ови термини замењују се термином *критично важни објекти* који се касније појављује у званичној државној политици заштите критично важних објеката из 2006. године.

Критично важни објекти идентификују се на основу 3 критеријума: типа претње, размере катастрофа и важности објекта.[392]

Тип претње. У измењеној верзији Федералног програма заштите критичне инфраструктуре из 2006. године побројано је 2.500 хемијски ризичних објеката, преко 1.500 нуклеарних објеката, 8.000 објеката код којих је повећан ризик од пожара и експлозија и преко 30.000 хидротехничких система, од којих већина објеката има

[390] Ibid

[391] Pynnöniemi, K., (2012), *Russian critical infrastructures – vulnerabilities and policies – The evolution of Russian policy on critical infrastructure protection*, The Finish Institute of International Affairs, p. 42 - истраживање којим су утврђени сви термини који се користе уместо термина *заштита критичне инфраструктуре*, као и њихова учесталост, спроведено је помоћу претраживача "Интегрум" у који је унет низ чланака о критичној инфраструктури у Русији, који су се појављивали у свим већим руским медијима у периоду од 2000-2010. године.

[392] Emercom administrative orderno 2-4-60-10-14, *Методические рекомендации по проведению инвентаризации критически важных и потенциально опасных объектов РФ и формированию оеречения критически важных объектов на регинальном уровне*, 19.июнь, 2008

велики економски, војни и друштвени значај за државу, али истовремено представља потенцијалну опасност за здравље и живот људи и за природу.[393] Индустријски развојни пројекти у еколошки рањивим подручјима, наведени су као посебно ризични. Министарство за ванредне ситуације, које координише имплементацију политике Владе о превенцији катастрофа и реаговању у случају ванредних ситуација, уврштава на основу типа претње у критично важне оне објекте који захтевају високи степен заштите од пожара. Неки други објекти попут објеката финансијског и банкарског сектора, и информационе и телекомуникационе инфраструктуре такође се на основу одлуке Министарства за ванредне ситуације сматрају критично важним објектима, односно критичном инфраструктуром.

Размере катастрофа. Овај критеријум такође представља важну референтну тачку за категоризацију критично важних објеката. Септембра 1996. године руска Влада је дефинисала скалу на основу које се утврђују размере катастрофа, а која је заснована на три критеријума: људски, материјални и просторни утицај катастрофе. Сем тога, подела међу катастрофама извршена је и према територији на коју катастрофа има утицај. На основу ове поделе, катастрофе су подељене на локалне, градске, територијалне, регионалне, државне и оне катастрофе чији се утицај шири ван граница Русије. Локалне катастрофе су оне катастрофе током којих има мање од 10 настрадалих, и не више од 100 особа чије су виталне функције угрожене, материјални трошкови су незнатни, а просторни утицај катастрофе не превазилази границе одређеног индустријског или пак друштвеног објекта.[394] На другом крају скале налазе се катастрофе чији се утицај простире ван територије Русије, које нису дефинисане кроз конкретне бројке, али је наглашено да им се мора поклонити огромна пажња. Наведена скала ревидирана је 2007. године и тренутно постоји следећих шест типова катастрофа: локалне, градске, међуградске, регионалне, међурегионалне и државне, при чему су катастрофе које се простиру ван граница државе искључене из ове поделе.[395] Критично важним објектима сматрају се објекти чије отказивање може да изазове регионалне, међурегионалне и државне катастрофе.

---

[393] Постановление Правительство РФ, *О Федеральной целевой программе снижения рисков и смягчение последствий чрезвичайных ситуаций природного и техногенного характера в Росийскои Федерации до 2010. года*, 6. январь 2006.

[394] Остановление Правительство РФ, но. 1094, *О классификации чрезвичайных ситуаций природного и техногенного характера*, 13. сентябрья 1996.

[395] Постановление Правительство РФ но. 304, *О класификации чрезвичайных ситуаций природного и техногенного характера*, май 2007.

Важност објекта. Важност критично заначајних објеката операционализована је кроз три критеријума: утицај објеката на регионалну економију, могућа штета коју би катастрофа могла да нанесе угледу државе и утицају који држава има (нпр. штета која је нанета државној управи, банкарском сектору, војној безбедности) и могуће опасности по становништво и територију (заправо утицај који ометање виталних система има на локално становништво). На основу ова три критеријума створена је основа за идентификовање и регистровање критично важних објеката, што је статус који неки објекат може да добије од институција које управљају регионом.

Природне катастрофе	Руска Федерација
Број догађаја	139
Број настрадалих	61,120
Просечно настрадалих по години	1,972
Просечно погођених	4,270,425
Просечно погођених по години	137,756
Економска штета (у хиљадама $)	8,267,161
Економска штета по годинама (у хиљадама $)	266,683

Табела 5.3. – Преглед природних катастрофа у Руској Федерацији (1980-2010)[396]

Извор: Natural Disaster Occurence Reported, http://www.preventionweb.net 23.02.2015.

[396] Видети на интернет адреси: *Disaster Statistics*, http://www.preventionweb.net 20.02.2015.

Руска политика заштите критичне инфраструктуре формулисана је 2006. године кроз низ докумената, укључујући концепт са основама за формулисање критеријума за идентификовање и регистровање критично важних објеката (септембар 2006. године) и федерални програм превенције катастрофа. Први федерални програм спроводио се до 2010. године, да би у јулу 2011. године настао нови програм превенције који ће се спроводити до 2015. године.[397] Новим програмом дефинисан је даљи развој превенције који подразумева померање од идентификовања критичних објеката (пошто је идентификација критичних инфраструктура великим делом обављена) ка увођењу система надзора критичних објеката и система извештавања о ванредним ситуацијама и могућим претњама.

У државном програму превенције катастрофа из јула 2011. године стоји да "програм превенције катастрофа, а тиме и гарантовање националне безбедности у ванредним ситуацијама могу бити остварени кроз унапређење државне управе и локалних самоуправа у области контроле безбедности виталних активности становништва, кроз обнављање техничке опреме, производњу технологија за потенцијално ризична постројења, затим кроз упознавање са модерним начинима информисања становништва, као и развојем система мера које би смањиле ризик и евентуалне последице катастрофа (природних, антропогених и терористичких напада) свеле на минимум".[398]

Програм пропагира развој научно – методолошке основе менаџмента ризика и кризног менаџмента и предлаже низ дугорочних стратегија и организационо-финансијских механизама који унапређују интеракцију, координацију и усмеравање ресурса.[399] Напредак система мониторинга и превенције катастрофа у Русији је неопходан из простог разлога што истраживања указују на то да се ризик од природних катастрофа и великих технолошких катастрофа константно увећава. Истовремено, скорашње статистике показују да се економски и људски трошкови ванредних ситуација, односно катастрофа смањују. Према званичној статистици 238 ванредних ситуација догодило се у Русији 2011, у односу на 360 ванредних ситуација 2010.

[397] Постановление Правительство РФ, *О Федеральной целевой программе снижения рисков и смягчения последствий чрезвичайных ситуаций природного и техногенного характера в Росийской Федерации до 2015.*

[398] Постановление Правительство РФ, *О Федеральной целевой программе снижения рисков и смягчения последствий чрезвичайных ситуаций природного и техногенного характера в Росийской Федерации до 2015*, p. 9

[399] Постановление Правительство РФ, *О Федеральной целевой программе снижения рисков и смягчения последствий чрезвичайных ситуаций природного и техногенного характера в Росийской Федерации до 2015. года*, no. 555, 7 июля 2011, p. 13

године. На целој територији Русије 2009. године је регистровано 429 ванредних ситуација.[400] Број погинулих или повређених особа током природних или технолошких катастрофа такође равномерно опада. Према извештају о имплементацији програма заштите критичне инфраструктуре из 2010. године, број погинулих током ванредних ситуација умањен је за 15,1%, а број повређених умањен је за 10,2%. Економски трошкови катастрофа умањили су се за 8%.[401] Када се упореде статистике које дају различите институције или пак статистике за две узастопне године, могу се, међутим, уочити одређене контрадикције. Тако, на пример, ако се упореди укупан број ванредних ситуација за 2008. и 2009. годину, може се приметити да је разлика у броју ванредних ситуација између те две године прилично велика.

Ванредне ситуације	2011.	2010.	2009.	2008.	2007.	2006.
Укупан број ванредних ситуација	297*	360*	429*	2154	2693	2847
Технолошке катастрофе	185	178	270	1966	2248	2541
Природне катастрофе	65	118	133	152	402	261
Биолошко-социјалне катастрофе	42	43	21	36	43	44

Табела бр. 5.4. – Упоредни приказ броја ванредних ситуација у Русији по годинама са поделом по типовима катастрофа[402]

Разлог за то може бити смањење индустријске производње у Русији током економске кризе на прелазу 2008. у 2009. годину. Такође је могуће да су се технике извештавања о ванредним ситуацијама, или чак и дефиниција технолошких катастрофа преформулисале, што је за последицу имало драстично смањење укупног броја ванредних ситуација.

Из наведених података може се извући закључак да је спровођење државних програма превенције катастрофа и ванредних ситуација (најпре програма из 2006. године, а и новог из 2011. године) успело да значајно умањи број ванредних ситуација, што значи да су мере предострожности предвиђене програмом превенције биле

[400] Pynnöniemi, K., *Russian critical infrastructures – vulnerabilities and policies – The evolution of Russian policy on critical infrastructure protection*, The Finish Institute of International Affairs, p. 45
http://www.fedstat.ru/indicator/data.do?id=41317&referrerType=0&referrerId=947198 23.01.2013

[401] Ibid

[402] Извор: подаци у колонама у којима је укупан број ванредних ситуација обележени звездицом (*) потичу са сајта руске статистичке агенције: http://www.fedstat.ru/indicator/data.do 23.01.2013; подаци који су у колонама у којима укупан број ванредних ситуација није означен звездицом потичу са сајта Министарства за ванредне ситуације Русије: http://www.mchs.gov.ru/stats/index.php?SectIoN_Id=253 23.01.2013

прилично ефикасне. Оснивање **Националног центра за кризни менаџмент 2006**.[403] године и развој сличних центара на нивоу региона представљају пример напретка државе на пољу заштите критичних инфраструктура и кризног менаџмента. Примери ефикасног кризног менаџмента у Русији су војни конфликти између Грузије и јужне Осетије, технолошка несрећа у Сајано−Шушенко хидроелектрани 2009. године, шумски пожари 2010. и друге технолошке катастрофе.[404] На трећу годишњицу несреће у хидроелектрани Сајано−Шушенко руска Влада проширила је опсег надзора и контроле опасних индустријских објеката и хидроелектричних система. Од јула 2012. године руски државни Институт за рударство и индустрију обавља широки надзор над постројењима везаним за секторе индустрије и рударства.

Надзор и извештавање о ситуацији у којој се налази критична инфраструктура, указивање на рањивости критичне инфраструктуре, ставља ризик и процене ризика у центар истраживања. Циљ који је записан у државном програму превенције је унапређење мониторинга и капацитета предвиђања у мери која покрива 80% ризика везаних за технологију и природу.[405] Нова култура понашања и реаговања у ванредним ситуацијама је неопходна како би се овај циљ остварио. Та *нова култура* је култура обавештавања (информисања) и узбуњивања у случају ванредних ситуација, формирана је на бази система за мониторинг ванредних ситуација следеће генерације, ширег коришћења нових информационих технологија у ове сврхе и имплементације система мера за обезбеђивање безбедности становништва и територије (мера из Националног плана за превенцију ванредних ситуација и катастрофа са важењем до 2015. године).

Оснивање Националног центра за кризни менаџмент 2006. године представљено је као одговор на растућу потребу да се унапреди "оптимизација активности које се предузимају приликом реаговања на ванредне ситуације са коришћењем модерних технологија".[406] Још од 1998. године у Русији постоји специјално одељење одговорно за мониторинг и предвиђање ванредних ситуација и оно сваке године објављује извештаје о ризицима повезаним са технолошким и природним катастрофама.

[403] http://www.mchs.gov.ru/eng/powers/?SectIoN_Id=609 23.01.2013
[404] Правительство РФ, *Концепция Федеральной целевой программы снижения рисков и смягчения последствий чрезвичайных ситуаций природного и техногенного характера в Росийской Федерации до 2015. года*, распоряжение но. 534, 29. мартам 2011.
[405] Постановление Правительство РФ, 2011, p. 25–26
[406] МЦХС Росии, Прогноз чрез вичайной обстановки на территории РФ на 2012. год, Центр Антистихия, Москва, 2011.

Поплаве које су задесиле јужне делове Русије у региону Краснодар током јула 2012. године указале су на то колико је систем мониторинга и предвиђања ризика и ванредних ситуација у суштини слаб.[407] Убрзо после ових поплава објављено је да ће бити формирана ***Национална служба за превенцију катастрофа*** у саставу новооснованог комитета, који је под надзором вицепремијера Русије.[408]

Иако су претерано широка тема да би се детаљније разматрале административне реформе спроведене од 2000. године до данас врло важан фактор који се треба узети у разматрање у настојању да се објасни тренутна ситуација везана за заштиту критичне инфраструктуре у Русији.

На пример, документ Владе о класификовању катастрофа према размерама из 2007. године не указује на административне агенције одговорне за превенцију катастрофа и пост кризно деловање ради свођења последица катастрофа на минимум, за разлику од претходног документа који је садржао и одељак са побројаним одговорним агенцијама. Ревизију Закона о безбедности 2010. године, треба размотрити у контексту заштите критичне инфраструктуре. Првобитна верзија Закона о безбедности из 1992. године садржи читаве листе агенција одговорних за реаговање у кризним ситуацијама – ватрогасце, јединице за заштиту околине, одговорне административни органе и све остале агенције и службе које су задужене за безбедност у било ком облику, док с друге стране, нова ревидирана верзија Закона о безбедности указује само на неке државне, регионалне и градске органе, а оно што се наглашава је неопходност координације и организације државних акција путем *стратешког планирања*.

Током последњих 20 година административни и финансијски ресурси за превенцију ванредних ситуација су консолидовани захваљујући раду Министарства за ванредне ситуације Русије. Министарство је оформљено на темељима руске цивилно-војне агенције јула 1991. године,[409] а данас има преко 200.000 запослених, организује међународне и домаће службе спасавања и обавља акције цивилне мобилизације у Русији. Након шумских пожара 2010. године, Министарству су обећане донације у

[407] Скоро 200 људи је погинуло током ових поплава. Власти су претрпеле велике критике, пре свега због лошег и неправовременог реаговања и необавештавања локалног становништва о могућој ванредној ситуацији.

[408] Према извештајима руских медија, основни задатак новог комитета на чијем челу је Рогозин јесте обављање научне и политичке анализе, која ће помоћи у ремодернизацији руских војно-индустријских комплекса.

[409] У новембру 2012. године председник Путин је Шоигу-а поставио за министра одбране, сменивши пре тога министра одбране Анатолија Сердјукова.

виду нови ресурса, посебно нове опреме, почев од авиона до мањих уређаја за гашење пожара.

5.2.2.3. Концепт националне безбедности

Концепт (касније стратегија) националне безбедности представљен маја 2009. године, даје потпуно нови тон политици заштите критичне инфраструктуре. Прва реченица стратегије одмах указује на то: "Русија је превазишла последице системске политичке и социо-економске кризе с краја 20-ог века... Држава сада има потенцијал да ојача своје компетенције и одбрани своје интересе као кључни играч у оквиру мултиполарних међународних односа".[410] Ова изјава указује на то да постоји генерално мишљење руских власти да ће упркос светској економској и финансијској кризи, која траје од 2008. године и упркос утицају који она има на економију Русије, руски политички систем опстати и одупрети се и да ће чак моћи да настави модернизацију у оквиру одређених економских сектора.

Слично сратегијама националне безбедности других земаља, и у тексту Стратегије националне безбедности Русије се као једна од опасности по земљу региструју активности терористичких организација, група и појединаца који настоје да узурпирају нормално функционисање државних тела да униште војне и индустријске објекте, предузећа и институције које пружају најбитније социјалне услуге или да застраше јавност на начине који могу да укључују нуклеарно и хемијско оружје или опасне радиоактивне, хемијске и биолошке супстанце. За разлику од многих дефиниција критичне инфраструктуре, текст Стратегије националне безбедности не бави се питањем сајбер-сфере и информационе инфраструктуре, као ни међузависности комплексних система и критичних инфра-структура. Скретање ка дефиницијама заштите критичне инфраструктуре, које се користе у развијеним земљама Запада, у оквиру руске Стратегије националне безбедности, може се приметити код помињања идеја о *начину живота* као нечему што треба заштитити, као и *унапређења квалитета живота грађана Русије* и *пропагирање здравог стила живљења*. Безбедност снабдевања храном, високо квалитетне медицинске услуге и брига о здрављу, не помињу се у значајној мери у Стратегији националне безбедности, али се детаљно обрађују у оквиру посебних докумената и закона и при томе их је могуће концептуално и стилски поредити са америчким и европским законима.

[410] *Russia's National Security Strategy*, (2009), approved by Presidential decree no. 537, 12 May, p.1

Еволуција руске политике о заштити критичне инфраструктуре ка терминологији која се користи на Западу комплетирана је доношењем реформулисане државне сајбер-стратегије.[411]

Иако постоје сличности у политикама заштите критичне инфраструктуре САД, европских земаља и Русије на терминолошком и концептуалном нивоу, то још увек не значи да су праксе у областима кризног менаџмента и менаџмента ризика исте. Интензивнија истраживања су неопходна како би се из праксе увидело какви све утицаји на имплементацију руске политике заштите критичне инфраструктуре постоје. Оно што се може разматрати без неких интензивнијих посматрања праксе Русије у заштити критичне инфраструктуре јесу промене на нивоу панирања политике. Из табеле 6.2. могу се уочити промене у политици заштите критичне инфраструктуре у Русији током претходни 20-ак година. Такође, може се видети да се пре 2000. године политика фокусирала уопштено на ванредне ситуације. Начин вођења безбедносне политике мења се од 2000. до 2003. године и тада се политика реформулише у смеру дефинисања концепта критичне инфра-структуре, дефинисања претњи по инфраструктуру, критичних објеката и сл. Последњих година, као и у многим развијеним и великим државама, највећа пажња поклања се сајбер-сфери, доношењу закона и правила везаних за ИТ сектор и његову заштиту и утврђивање модела борбе против сајбер-криминала.

Година	Закони који се фокусирају на ванредне ситуације	Закони који се фокусирају на критичну инфраструктуру
1994.	Федерални Закон о заштити становништва и територије од природних катастрофа и ванредних ситуација изазваних технолошким факторима	
1996.	Владина уредба о класификацији ванредних ситуација (катастрофа)	
1999.	Федерални програм за смањење ризика и последица ванредних ситуација изазваних природним и технолошким факторима	
2000.	Концепт националне безбедности	Концепт националне безбедности
2003.		Државни концепт унапређења хемијске, биолошке и нуклеарне безбедности
		Владина наредба о оснивању

[411] Иванов, М., (2012), *Совет федерации за нялсяцифровым суверенитетом*, Коммерсант, 6. ноябрь

Година	Закони који се фокусирају на ванредне ситуације	Закони који се фокусирају на критичну инфраструктуру
2005.		државног система мониторинга крично важних објеката
2006		Концептуална основа државне политике заштите становништва и критично важних објеката од катастрофа изазваних природним и технолошким факторима и терористичким нападима.
2007.	Владина уредба о класификацији ванредних ситуација (ревидирање уредбе из 1996. године)	
2009.		Стратегија националне безбедности
2011.		Концептуална основа државне политике заштите становништва и критично важних и потенцијално опасних објеката од катастрофа изазваних природним или технолошким факторима и терористичким нападима до 2020. године.

Табела бр. 5.5. – Приказ најбитнијих закона, подзаконских аката, стратегија и уредби, везаних за заштиту критичне инфраструкутре у Русији (са изузетком закона везаних за заштиту информационе инфраструктуре)

5.2.2.4. Преглед садашњих и будућих иницијатива и мера које Русија предузима у циљу заштите критичне инфрасртуктуре

Стратегија развоја информационог друштва у Русији и Мере информационе безбедности у области употребе информационих и комуникационих система у међународној размени информација донети су 2008. године.

Раније је руска Влада донела неколико програма: Програм развоја јединственог информационог окружења у образовању (2001. године), Концепт коришћења информационих технологија у државним институцијама (2004. године), Федерални програм под називом *Електронска Русија* (2002-2010. године) и програм назван *Националне технолошке основе* (2007. године).

Доктрина информационе безбедности Руске Федерације[412] усвојена је 9. септембра 2000. године и представља додатак Националном безбедносном концепту[413] (одобрен 10. јануара 2000. године). Доктрина тежи да ојача државну политику на пољу

[412] "*Doctrine of the Information Security of the Russian Federation*", approved by the president of the Russian Federation, Vladimir Putin, 2000. http://www.medialaw.ru/e_pages/laws/project/d2-4.htm 23.01.2013
[413] http://www.kremlin.ru/eng/articles/institut04.shtml 23.01.2013

информационе безбедности, формулише легалне, методолошке, техничке и организационе основе за постизање високог степена информационе безбедности у Русији и да помогне развој одређених програма у ту сврху. Доктрина дефинише националне интересе у информационој сфери и даје основе за процену претњи по информациону инфрструктуру, које могу да угрозе грађане, друштво и државу. Доктрина је врло обимна и обухвата теме попут државних политика у областима заштите података, личне приватности, ауторских права, хакерских напада на државне информационе системе, приступа информацијама и функционисања медија.[414]

Русија посматра информационе системе својих грађана и националне информационе системе као јединствени систем.[415] Сем тога, Русија сматра да неконтролисано ширење страних медијских мрежа у Русији представља претњу информационој безбедности Русије и стога настоји да *ојача* руске медије.[416]

Доктрина се правно ослања на руске федералне законе о безбедности, државној тајни, заштити података и на учешћу у међународној размени информација. Документ је подељен на четири поглавља, распоређена у два одељка. Четири главна поглавља су:

1. Информациона безбедност – ово поглавље дефинише националне интересе Руске Федерације у информационој сфери, уз указивање на уставна права, помоћ ИТ сектору, развој информационе индустрије и на спречавање неовлашћеног приступа информацијама. Сем тога, у овом поглављу дефинишу се унутрашњи и спољашњи извори претњи по информациону безбедност Русије.
2. Методи постизања информационе безбедности – поглавље обухвата легалне, организационо-техничке и економске методе за постизање информационе безбедности. Поред тога, описане су бројне одлике информационе безбедности у различитим сферама као што су економија, унутрашња политика, спољна политика, наука и технологија, информациони и телекомуникациони системи, одбрамбена политика, ванредне ситуације. Помиње се и међународна сарадња у области информационе безбедности

[414] Leigh, I., "*Information Security Doctrine of the Russian Federation*".
[415] Timothy, L. T., (2001), "*Information Security Thinking: A Comparison of U.S., Russian and Chinese Concepts*"
[416] Овај аспект Путинове доктрине доста је критикован од стране новинара, који се прибојавају да таква политика угрожава слободу мишљења и слободу говора. Један од таквих текстова је текст новинарке Јевгеније Албатс, у листу *The Moscow Times* под називом "*Information Security Doctrine Redux*", од 14. септембра 2000.

(подршка размене информација, координи-сање полицијских активности, превенција недозвољеног приступа поверљивим информацијама).

3. Основне одредбе државне политике о информационој безбедности; приоритетне мере за имплеменацију политике − где су дати предлози за унапређење информационе безбедности, најпре у виду развојних смерница за државне институције.
4. Организациона основа за побољшање информационе безбедности –описује функције система информационе безбедности, као и организационе елементе и чиниоце руског система информационе безбедности међу којима су председник, Савет државне скупштине, државна Дума, Влада Русије, Безбедносни Савет и други извршни органи, председничке комисије, правосудне институције, јавна удружења и грађани.

Доктрина информационе безбедности ставља велики нагласак на формирање законске основе система информационе безбедности. Посебно се помињу закони о државним тајнама, информисању, компјутеризацији, заштити информација, партиципи-рању у међународој размени искустава и информације и формирању државне архиве. Доктрина даље указује на претње које за руску информациону инфраструктуру представљају различите врсте напада. Такође, додатна пажња поклања се развоју телекомуникационих система, интегритета информационих ресурса, извиђању ситуације у информационој области и постројења за одбрану од елекртонских напада.

Програм електронска Русија[417] настао је почетком 2001. године, када је Министарство трговине и економског развоја објавило план стратешког развоја Русије до 2010. године. Програм је заснован на идеји да је ради ублажавања економског заостатка државе неопходно радити на развоју сектора високих технологија, у ком би било могуће остварити виши ниво продуктивности него у сектору производње сировина. Ништа од оног што је предвиђено планом стратешког развоја Русије до 2010. године није могуће постићи без рачунара и моћног сектора информационих и комуникационих технологија (ИКТ).[418]

[417] Federal Target Program, (2002), "*Electronic Russia (years 2002–2010)*", approved by the government of the Russian Federation, Decree No. 65, 28 January

[418] Сви градови у Русији са популацијом преко 30.000 грађана треба да буду повезани у систем државне оптичке мреже, иако ће конекције индивидуалних домова и канцеларија у Русији врло вероватно остати *примитивне* бар још неко време. Хиљаде села у Русији немају чак ни телефонску линију, па ће стога вероватно проћи доста година пре него што се сва ретко насељена места опреме потпуно оперативном телекомуникационом инфраструктуром. Разматра се више опција везаних за довођење ове

Укључивање различитих министарстава[419] и координацију од стране Министарства телекомуникација и информатизације (од 2004. године Министарство информационих технологија и комуникације), програм *електронска Русија* представља срж програма развоја информационих технологија, који ће даље поставити темеље ефикасније економије и државне администрације кроз масовну имплементацију информационих и телекомуникационих технологија.[420] Овај програм такође има за циљ олакшавање напретка цивилних институција (у технолошком смислу) обезбеђивањем права грађанима на неспутан приступ информацијама и ширењем могућности школовања специјалиста и квалификованих корисника у области информационих технологија.[421]

Програмом *електронске Русије* планиран је деветогодишњи развој ИТ сектора у Русији, уз посебан нагласак на четири области:[422]

1. Формирање институционалног оквира и утврђивање служби одговорних за надзор спровођења програма,
2. Развој интернет инфраструктуре,
3. Формирање сајта и сервиса е-Владе и
4. Увођење система електронског образовања.

Основни циљеви *електронске Русије* су побољшање ефикасности економије, унапређење менаџмента у јавном сектору и повећање аутономије државних служби применом информационих и комуникационих технологија.[423]

Влада Русије је 2006. године модификовала неке од циљева и задатака програма. Основни циљ програма *електронска Русија* је у почетку био ограничен на побољшање квалитета и ефикасности државне администрације кроз имплементацију информационих и телекомуникационих технологија у институције Владе, како би се

инфраструктуре, укључујући чак и сателитску инфраструктуру за недоступне области. Програм *електронска Русија* настоји да учини што већи број државних служби доступним на интернету (да оформи он-лајн сервисе државних служби) и да олакша бирократске поступке руским грађаним и фирмама. Тиме би се нпр. омогућило да се путем интернета плаћају порези или региструју фирме. Огромна пространства Русије и велики број места без информационе и комуникационе инфраструктуре, као и финансијске потешкоће образовног система, били су додатни подстрек за развој овог програма и за налажење нових креативних решења како би се омогућило образовање у свим деловима државе. Формирање програма за учење на даљину путем интернета сматра се потенцијално ефикасним решењем проблема образовања у недоступним крајевима Русије. На сајту *електронске Русије* могу се видети и сви остали планови који се овим прогамом требају спровести у дело: http://www.e-rus.ru 23.01.2013

[419] Министарство трговине и економског развоја, Министарство образовања, Министарство индустрије, науке и технологије, државна ваздухопловна и свемирска агенција, Владина агенција за информисање и комуникације са председником, Агенција за менаџмент система.

[420] http://www.uni-koblenz.de/~kgt/PM/SemB/Russland.ppt 23.01.2013

[421] http://www.bisnis.doc.gov/bisnis/bisdoc/011001E-Russia.html 23.01.2013

[422] Ibid

[423] Federal Target Program "*Electronic Russia*", op. cit, p. 3 f

побољшале вештине државних службеника везане за коришћење информационих технологија и квалитет државних сервиса које би користили грађани. Стога је 2006. године направљен вишегодишњи план развоја информационих технологија, који је углавном везан за развој е-Владе.

Један од регионалних огранака програма *елктронска Русија* је градски програм *електронска Москва*.[424] Овај програм, представљен крајем 2002. године, тежи да ојача улогу Москве као центра информационе индустрије. Програм је заснован на моћној градској телекомуникационој инфраструктури – московској мрежи оптичких влакана. Задаци укључени у план *електронске Москве* укључују формирање нормативне и законске основе неопходне за функционисање информационог друштва, успостављање ефикаснијег градског менаџента заснованог на раду е-Владе, развој градске економије, изградњу оквира за заједничко функционисање градских административних органа и интегрисање свих постојећих пројеката везаних за информационе и комуникационе технологије на нивоу градских власти.[425]

Међународна сарадња је важна компонента напора Русије на пољу остваривања информационе безбедности. Међународна борба за технолошке и информационе ресурсе и за доминацију на тржиштима је добила веће размере, а водеће светске економске силе остариле су и велики технолошки развој, чиме су повећале и готовост државе у случају сајбер-ратовања. Русија посматра ову борбу за технолошке и информационе ресурсе и читав технолошки развој са извесним резервама, јер би могао да доведе до нових трка у наоружавању у информационој сфери и да увећа опасност од пробоја страних обавештајних служби у Русију, помоћу информационих система и кроз глобалну информациону инфраструктуру.

У складу са одуком Генералне скупштине УН-а бр. 58/32 од 8. децембра 2003. године, организована је група владиних експерата из области информационе безбедности.[426] Група експерата укључује представнике 15 земаља.[427] Даље, руска Влада има посебна партнерства са државама чланицама Шангајске организације за сарадњу (*Shanghai Cooperation Organization* − SCO)[428] и са државама чланицама Организације за

[424] http://mgd.iis.ru 23.01.2013
[425] Filippov, S., (2005), "Policy for ICT Adoption in Moscow", *Electronic Moscow Programme*, Institute of the Information Society, октобар 14
[426] Kremer, A., (2004), "*Cyber Security in Russia*", Presentation held at ITU-T Cyber security Symposium, Florianopolis, Brazil, October 4.
[427] Уједињено краљевство, Кина, Русија, Француска, Белорусија, Бразил, Немачка, Индија, Јордан, Малезија, Мали, Мексико, Јужна Кореја и Јужна Африка.
[428] Русија у склопу SCO има потписана партнерства са Кином, Казахстаном, Киргистаном, Таџикистаном и Узбекистаном.

колективну безбедност (*Collective Security Treaty Organization* - CSTO)[429] у области информационе безбедности.

5.2.2.5. Организациона структура система заштите критичне инфраструктуре у Русији

Најбитније организације одговорне за безбедност критичне инфраструктуре у Русији су: Безбедносни савет Руске Федерације, Федерална служба безбедности Руске Федерације, Федерална одбрамбена служба Русије, Федерална служба за техничку контролу и контролу извоза и више министарства Руске Федерације.

Кад су у питању приватно-јавна партнерства, треба поменути Руску асоцијацију мрежа и сервиса, која доприноси развоју норми за имплементацију и коришћење безбедних информационих технологија и ПРИОР који представља државну иницијативу за уједињење државних, приватних и непрофитних организација у циљу развоја информационог друштва у Русији.

Савет безбедности Руске Федерације[430] именован је од стране председника, а у складу са Уставом и државним законом о безбедности. Савет је одговоран за утврђивање националних интереса у области инфраструктуре и дефинише информационе ресурсе који се морају заштитити, као и концептуалне приступе националној безбедности.[431]

Федерална служба безбедности Руске Федерације (ФСБ)[432] је федерална агенција и извршни орган Владе Русије са задатком да гарантује за безбедност Русије. Под тим се подразумева одбрана и заштита државних граница Русије, унутрашњих водних путева, територијалних вода, ексклузивних економских зона, природних ресурса и целокупне критичне инфраструктуре.[433]

Кад је у питању техничка подршка, ФСБ има свој сопствени истраживачки институт специјализован за информационе технологије. Институт врши процене безбедности, нарочито по питању криминалних претњи.[434] ФСБ је такође одговоран за

[429] Русија има партнерства са следећим чланицама CSTO: Јерменијом, Белорусијом, Казахстаном, Киргистаном, Таџикистаном и Узбекистаном.
[430] http://www.scrf.gov.ru 23.01.2013
[431] http://www.kremlin.ru/eng/articles/institut04.shtml 23.01.2013
[432] http://www.fsb.ru 23.01.2013
[433] *Statute on the Federal Security Service of the Russian Federation and Structure of the Federal Security Service Agencies*, approved by presidential edict no. 960, 11 August 2003, signed by V. Putin, President of Russian Federation.
[434] Ibid

праћење у случајевима сајбер-тероризма.[435] ФСБ-ов Директорат за компјутерску и информациону безбедност (Директорат-Р) основан је у октобру 1998. године. Основни задаци Директората су контраобавештајна делатност и борба против сајбер-криминала, тако да је и Директорат за компјутерску и информациону безбедност сада део ФСБ, односно контраобавештајне службе.[436]

Најбитнији задаци ФСБ-а на пољу безбедности информационе инфраструктуре јесте планирање и имплементација државних и научно-техничких стратегија, организација и подршка при обезбеђивању информационих и телекомуникационих система, заштита државних тајни и система комуникације у Русији и руским институцијама у иностранству. Још једна функција ФСБ-а је и сертификовање опрема за заштиту информационе инфраструктуре, телекомуникационих система и мрежа. Сем тога, ФСБ регулише развој, производњу, продају, употребу, извоз и увоз криптографске опреме, телекомуникационих система и мрежа које су енкрипцијски заштићене.[437]

Федерална одбрамбена служба Руске Федерације је федерални извршни орган Владе Русије, са задатком да обликује државну политику и законску регулативу и да спроводи надзор и контролу ради обезбеђивања председника Русије, председника руске Владе и друге важне јавне личности. Специјална комуникациона и информациона служба је као додатни орган припојена Федералној одбрамбеној служби у августу 2004. године, као резултат административних реформи Федералне одбрамбене службе.[438]

До 2004. године Федерална комуникациона и информациона агенција Владе била главни одговорни орган за заштиту информационе инфраструктуре и информациону безбедност. Федерална комуникациона и информациона агенција Владе укинута је 2003. године и њене функције су расподељене између Федералне службе безбедности (ФСБ) и Федералне одбрамбене службе Руске Федерације. Федерална комуникациона и информа-циона агенција Владе се такође борила против домаћег

[435] http://www.russia-gateway.ru/content/NEWS/NewsItem_2376921.jsp 23.01.2013
[436] http://www.agentura.ru/english/dosie/fsb/structure 23.01.2013
[437] *Statute on the Federal Security Service of the Russian Federation and Structure of the Federal Security Service Agencies*, approved by presidential edict no. 960, 11 August 2003, signed by V. Putin, President of Russian Federation.
[438] Decree of the President of the Russian Federation No. 1013, 7 August, 2004: "*Issues ofthe Federal Guard Service of the Russian Federation*" with Amendments and Additions of 28 December 2004, 22 March and 1-6 October 2005

криминала, страних обавештајних служби, учествовала је у борби против електронског криминала и обезбеђивала проток информација у финансијском сектору.[439]

Федерална служба за техничку контролу и контролу извоза основана је у августу 2004. године,[440]а њеним активностима управља председник Русије, док се сама служба налази под јурисдикцијом Министарства одбране.

Министарство комуникација и информационих технологија је огранак федералне Владе који спроводи државну политику и надгледа телекомуникациони сектор. Међу осталим задацима, Министарство комуникација и информационих технологија заједно са другим министарствима и агенцијама Владе предузима мере обнове информационих и комуникационих мрежа у Русији у случају ванредних ситуација, када дође до оштећења ових мрежа.

Приватно-јавна партнерства нису практично ни постојала јер је у Русији дуго била пракса да се мере заштите инфраструктуре примењују само за заштиту инфраструктуре која је блиско повезана са војском, системима и институцијама Владе и другим државним институцијама и службама. Данас је ситуација другачија и доста се ради на решавању питања заштите инфраструктуре која је у власништву приватног сектора, што се највише примећује у сектору заштите информационе инфраструктуре.

Права сарадња приватног и јавног сектора на пољу информационе безбедности остаје и даље ограничена у односу на друге развијене државе.

Руска асоцијација мрежа и сервиса је државна организација која се бави развија-њем норми и законских аката везаних за имплементацију и употребу информационих технологија. Оснивање Агенције иницирало је Министарство комуника-ција и информа-ционих технологија Русије 1994. године. Тренутно Асоцијација има 122 члана из читаве Русије, укључујући универзитете, научне институције, министарства, компаније које се баве осигурањем, затим операторе за критичну инфраструктуру, трговце и кориснике. Асоцијација има неколико комитета и радних група које покривају различите теме: интернет, безбедност и приватност корисника информационих технологија, едукацију и обуку, ај-пи (IP) телефонију. Једна од радних група бави се надгледањем стандарда.[441]

[439] http://www.fas.org/irp/world/russia/fapsi/index.html 23.01.2013
[440] Edict no. 314 of the president of the Russian Federation of 9 March 2004 on the System and Structure of Federal Executive Bodies
[441] http://www.rans.ru/eng/directions 23.01.2013

ПРИОР[442] представља националну иницијативу, која за циљ има уједињење државних, приватних и непрофитних организација. Кроз своје активности ова иницијатива настоји да допуни постојеће државне и друге програме и пројекте усмерене ка развоју информационог друштва у Русији. ПРИОР препознаје важност учествовања у великим развојним пројектима, укључујући и оне које спроводи држава (какви су програми *електронска Русија*, градски пројекти *е-Москва*, *е-Санкт-Петербург* и други).

Највећи пројекат ПРИОР-а је креирање програма под називом *Развојни пут Русије* који је замишљен као платформа за сарадњу приватног и јавног сектора ради достизања заједничких циљева и као основа за интегрисање сазнања и постојећих информација из оба сектора ради даљег развоја. Идеја је да то буде коалиција сарадника са подједнаким правима, што је огромна промена на традиционални руски систем хијерарије у ком је држава изнад свих.

ПРИОР је волонтерски скуп организација и појединаца који улажу напоре и доступне ресурсе како би обезбедили информациону, технолошку, финансијску, организациону, саветодавну и друге врсте подршке ради постизања заједничких циљева. Ови циљеви укључују оснивање електронских управа, стварање основе за развој е-бизниса, умрежавање друштва и ширење интернета у Русији, развијање програма за учење на даљину, креирање дигиталних библиотека и помогање међународних, националних и локалних пројеката и пројеката и иницијатива кроз изношење сопствених искустава и практичних знања.

Системи раног упозорења и пружања помоћи јавности су део руске доктрине информационе безбедности где се помиње развој неких механизама раног упозорења: "У специфичним условима у којима се Русија налази информациона безбедност се може остварити и развијањем ефикасних система надзора и контроле критичних објеката чији кварови или неисправност могу да доведу до ванредне ситуације и да угрозе безбедност читавог друштва".[443]

Руски рачунарски тим за реаговање у ванредним ситуацијама[444] основан је 1998. године и под управом је руског Института за јавне мреже.[445] Тим је део РБнет

[442] http://prior.russia-gateway.ru 23.01.2013
[443] "*Doctrine of the Information Security of the Russian Federation*", approved by the president of the Russian Federation, Vladimir Putin, 9. септембар 2000.
[444] http://www.cert.ru/index_eng.html 23.01.2013
[445] http://www.ripn.net:8080/en/index.html 23.01.2013

мрежног оперативног центра.[446] РБнет је основан као интернет сервис за научну и средњошколску заједницу у Русији. Овај пројекат је основан на иницијативу Владе Русије, а за функционисање РБнета-а задужен је руски Институт за јавне мреже. Руски рачунарски тим за реаговање у ванредним ситуацијама врши превенцију компјутерских инцидената и пружа услуге корисницима РБнет-а. Првобитни разлог оснивања тима била је координација напора у борби против хакера на ширем подручју Москве.[447]

Научна подршка је један од битних фактора политике државе у области система раног упозорења и пружања помоћи јавности. Координација активности руских научних организација на овом пољу поверена је Институту за питања информационе безбедности Московског универзитета. Технички аспект ове области покрива Криптографска Академија Русије.

Законске регулативе везане за заштиту критичне инфраструктуре, осим већ поменутих навешћемо још неколико битних за функционисање система заштите критичне инфраструктуре у Русији, пре свега заштите критичне информационе инфраструктуре.

Законски оквир информационе безбедности у Русији укључује три основна елемента: (1) постављање законске основе за обављање задатака везаних за информациону безбедност, (2) постављање законске основе за програме заштите информационе инфраструктуре (заштита компјутерских програма и база података као једног сегмента информационе инфраструктуре обавља се у складу са Законом о заштити компјутерских програма и база података Руске Федерације)[448] и (3) формирање законског статуса елемената информационе инфраструктуре.

Законску основу за обављање задатака везаних за информациону безбедност представљају Закон о медијима Руске Федерације, Закон о рекламирању, Закон о борби против екстремистичких активности, Закон о политичким партијама, Закон о администра-тивним прекршајима, Закон о државним тајнама,[449] Закон о информисању и заштити података (који се фокусира на коришћење информационих ресурса, на право приступа подацима и на заштиту података ради превенције неовлашћеног приступа подацима који може да изазове велику штету органима државе).

[446] http://www.rbnet.ru/en/about_en.shtml 23.01.2013
[447] Те 1998. године је у Москви постојао велики проблем са хакерима. Наиме, хакери су користили украдене dial-up шифре и изазивали прилично велику материјалну штету.
[448] http://www.russoft.org/docs/?doc=131 23.01.2013
[449] http://www.medialaw.ru/laws/russian_laws/txt/8.html 23.01.2013

Законски основ за спровођење програма заштите критичне информационе инфраструктуре представља Закон о комуникацијама, који такође покрива и менаџмент комуникационих мрежа у ванредним ситуацијама. Бројни други закони су усвојени, а почео је и рад на њиховој имплементацији. Такође, донети су и предлози закона којима се регулишу друштвени односи у информационој сфери. Влада Русије нада се да ће нови Закон о електронском дигиталном потпису служити као помоћно средство за регулисање стања критичне информационе инфраструктуре. Нови Закон о техничким прописима такође нуди нову дефиницију концепта безбедности. У овом Закону стоји да *безбедност представља стање непостојања ризика од оштећења*.

Руски Кривични закон у заштити информационе критичне инфраструктур, по свом садржају, указује да број сајбер-напада на предузећа, организације и грађане у Русији има тенденцију сталног раста. Према подацима Одељења за специјалне техничке мере Министарства унутрашњих послова Русије, број компјутерских напада у Русији увећао се за 150% од 2005. до 2009. године.[450] Руски Кривични закон, ревидиран 2004. године, даје основе за кажњавање и прописује казне за криминалце који почине следеће злочине: незаконити приступ законом заштићеним информацијама, развој компјутерских програма који доводе до уништавања, блокирања, модификовања и копирања законом заштићених података, ремећење функционисања компјутера, компјутерских система и мрежа, кршење правила коришћења компјутера, компјутерских система или мрежа.

Кривични закон Русије укључује и чланове којима се утврђују казне за кривична дела за која раније није постојала казна. Поглавље 28 Закона: "*Кривична дела у сфери информационих технологија*" састоји се од три члана, којима се дефинишу казне за незаконит приступ информацијама (Члан 272), за креирање, коришћење и даље ширење малициозних компјутерских програма (Члан 273) и за кршење правила коришћења компјутера, компјутерских система и мрежа (Члан 274).[451]

5.2.3. Јапан

Критична инфраструктура у Јапану дефинисана је 2005. године Акционим планом о мерама заштите критичне инфраструктуре, који је издао Савет за безбедносну политику. Дефиниција каже да "критичну инфраструктуру чине службе

[450] Brunner, M. E., and Suter, M., (2009), *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich, p. 358
[451] http://books.nap.edu/openbook.php?isbn=0309089719&page=102 23.01.2013

које се баве пружањем услуга, а које су апсолутно неопходне за функционисање друштва и економије Јапана. Уколико дође до прекида функције неке критичне инфраструктуре или уколико је функционисање неке инфраструктуре угрожено, функционисање читавог друштва и економије Јапана биће поремећено".[452]

Природне катастрофе	Јапан
Број догађаја	157
Број настрадалих	8,568
Просечно настрадалих по години	276
Број погођених	3,361,979
Просечно погођених по години	108,451
Економска штета (у хиљадама $)	208,230,800
Економска штета по годинама (у хиљадама $)	6,717,123

Табела бр. 5.6. – Преглед природних катастрофа у Јапану (1980-2010)[453]

Акционим планом о мерама заштите критичне инфраструктуре дефинисано је десет критичних инфраструктура:

1. Телекомуникације,
2. Владине и административне службе,
3. Финансије,
4. Цивилно ваздухопловство,
5. Железнице,
6. Логистика,
7. Струја,
8. Гас,
9. Медицинске службе и
10. Вода.

[452] Information Security Policy Council: "*Action Plan on Information Security Measures for Critical Infrastructures*", p.2, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf 23.01.2013
[453] Видети на интернет адреси: *Disaster Statistics*, http://www.preventionweb.net 20.02.2015.

Извор: *Natural Disaster Occurence Reported*, http://www.preventionweb.net 23.02.2015.

Након несреће у нуклеарној електрани "Фукушима" од 11. марта 2011. године, која је донела и највише људских жртава икад (15.881), Јапан је био изложен и другим природним непогодама. Тако се често истиче да је Јапан једна од водећих земаља које су највише погођене елементарним непогодама. Две од пет највећих и најскупљих природних катастрофа у новијој историји десиле су се у Јапану (1995. и 2011), а укупна штета износила је 181 милијарду долара. Јапан је такође био поприште неких од најгорих природних катастрофа 21. века. Врсте природних катастрофа у Јапану укључују цунамије, поплаве, тајфуне, земљотресе и вулканске ерупције. Као острвска земља Јапан је веома често изложен екстремним тајфунима, односно ураганима, који наносе велике штете острвима, градовима и целокупној инфраструктури. Тако је најпознатији тајфун "Хаикуи" из 2012. године донео 105 људских жртава и штету од 2.09 милијарди долара.[454]

И поред усавршавања техничких средстава, развоја и образовања људских ресурса, глобалне информатизације пословних и других процеса, као и осмишљавања и имплементације нормативне регулативе (аката међународног права, закона, других прописа и стандарда) ванредни догађаји који се не могу контролисати редовним

[454] Видети интернет страницу: http://en.wikipedia.org/wiki/Natural_disasters_in_Japan 28.02.2015.

мерама надлежних органа и институција остају озбиљан и тежак изазов за савремено друштво. Удес у нуклеарном постројењу у Фокушими у Јапану, 2011. године, показује да знање корисника и системи безбедности постројења са опасним материјама и даље нису довољно поуздани, а организациона култура, чак ни у високо технолошки развијеним заједницама, није на потребном нивоу. Природне непогоде, катастрофе и ванредне ситуације последњих година, наглашавају потенцијал екстремних сеизмичких и климатских догађаја који могу изазвати велике последице, пошто уништавају и/или прекидају функционисање најзначајнијих, а често и глобалних инфраструктира и токова информација на којима су пост-индустријска друштва изграђена.[455]

Влада Јапана је спроводећи Акциони план о основним препорукама о промоцији развоја информационог и телекомуникационог друштва из 1998. године,[456] дала значајан допринос развоју информационих технологија и телекомуникација.[457]

Стратегија информационе безбедности, објављена 2003. године од стране Министарства економије, трговине и индустрије, био је следећи корак у развоју програма заштите критичне информационе инфраструктуре. У овом документу се из перспективе националне безбедности разматрају сви проблеми, ризици и претње везани за информационе и комуникационе технологије.[458]

Прва национална стратегија информационе безбедности објављена је 2005. године. Ово је тренутно најважнији документ везан за заштиту критичне информационе инфраструктуре и информационе безбедности у Јапану.

Октобра 2003. године Комисија за информациону безбедност Министарства економије, трговине и индустрије објавило је свеобухватну стратегију информационе безбедности. Овај документ представља почетну тачку у развоју националне стратегије информационе безбедности, јер је први документ који указује на неопходност свеобухватног приступа како би се унапредило и обезбедило информационо друштво у Јапану. Предлози и захтеви изнети у свеобухватној стратегији имплементирани су 2005. године. Основани су Савет за информациону безбедност и Национални центар за информациону безбедост, а донета је и национална стратегија информационе безбедности. Пуно име стратегије гласи "Прва национална стратегија информационе

[455] Млађан, Д. (2014), *Безбедност у ванредним ситуацијама*, Београд, Криминалистичко полицијска академија.

[456] *Decision of the Advanced Information and Telecommunications Society Promotion Headquarters,* 9 November, 1998.

[457] *Outline of the First Follow-up of the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society*, 19. May, 2000.

[458] Стратегија је доступна на сајту Министарства економије, трговине и индустрије Јапана: http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf 23.01.2013

безбедности – формирање безбедног информационог друштва".[459] Стратегија се бави средњерочним и дугорочним циљевима. Савет за информациону безбедност издао је одвојене имплемента-ционе планове за сваки од циљева.[460]

Циљ Стратегије је да начини Јапан развијеном нацијом у области информационе безбедности. Што је најважније, Стратегија настоји да установи нове моделе приватно-јавног партнерства ради унапређења информационе безбедности. Стратегијом се даље дефинишу улоге Владе, критичних инфраструктура, компанија и појединаца. Такође, Стратегијом се дефинишу мере које морају бити имплементиране од стране свих учесника.

Акциони план о мерама безбедности за заштиту критичне инфраструктуре донео је Секретаријат 2000. године у циљу спровођењу мера заштите од сајбер-тероризма и сајбер-напада на критичну инфраструктуру,[461] који је у децембру замењен акционим планом о безбедносним мерама за заштиту критичне инфраструктуре,[462] а који је издао Савет за информациону безбедност као додатак Првој националној стратегији о информационој безбедности.

У акционом плану се налазе и анализе зависности између критичних инфра-структура. Баш због тога што постоји велика зависност између критичних инфраструктура планом су предвиђене заједничке обуке оператера и власника различитих критичних инфраструктура. Овакве вежбе спроводе се сваке фискалне године, а то које ће се вежбе конкретно спроводити зависи од целокупне безбедносне ситуације и безбедносних претњи које су тренутно актуелне.

У циљу унапређења нивоа информационе безбедности читаве Владе, Савет за информациону безбедност објавио је *Стандарде за увођење мера заштите у области информационе безбедности за централне владине компјутерске системе*. Стандарди које је формулисао Савет за информациону безбедност представљају номинални ниво информационе безбедности у оквиру владиних агенција. Национални центар за информациону безбедност проверава и врши оцену стварног нивоа безбедности и

[459] http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf 23.01.2013
[460] Secure Japan 2006: First Step Towards a Trustworthy Society, http://www.nisc.go.jp/eng/pdf/sj2006_eng.pdf 23.01.2013
[461] Special Action Plan on Countermeasures to Cyber-terrorism of critical infrastructure, 15. December 2000 http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN009986.pdf 23.01.2013
[462] http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf 23.01.2013

упоређује га са постављеним стандардима[463] и формира препоруке за сваку агенцију Владе.

5.2.3.1. Организациона структура система заштите критичне инфраструктуре у Јапану

У оквиру Владе Јапана, Кабинет Секретаријата за заштиту критичне инфраструктуре 2005. године оформљени су Савет за информациону безбедност и Национални центар за информациону безбедност, који су тренутно најодговорнији за доношење и спровођење политике заштите критичне информационе инфраструктуре у Јапану.

У оквиру *Кабинета секретаријата за заштиту критичне инфраструктуре* основан је јула 2000. године Стратешки штаб за информационе технологије, који укључује сва министарства и експерте из приватног сектора, како би се промовисао низ мера које би Јапан требало да учине конкурентним у међународним оквирима кад су у питању информационе технологије. Истовремено је основан и стратешки савет за информационе технологије, који ће се такође бавити стратешким развојем информационих технологија и који ће подстицати приватно-јавна партнерства.[464] У јануару 2001. године, стратешки штаб за промоцију напредних технологија и телекомуникационих мрежа (тј. стратешки штаб за информационе технологије) је путем одредбе *Основног закона* о развоју напредних технологија и телекомуникационих мрежа променио облик у ком је постојао тих првих годину дана. И штаб и стратешки савет за информационе технологије су се ујединили у оквиру ове нове организације, а на чело постављен је премијер. Велику улогу у овој организацији имали су чланови приватног сектора из области информационих технологија. [465]

- *Савет за политику информационе безбедности* основан 2005. године, чиниле су одређене јединице стратешког штаба за информационе технологије, чланови министарства и експерти из приватног сектора. Овај Савет има централну улогу у развоју и ревизији стратегија и политика информационе безбедности.

[463] National Information Security Center (NISC): "Japanese Government's Efforts to Address Information Security Issues – Focusing on the Cabinet Secretariat's Efforts", Chapter 3.1. "Standards for Information Security Measures for the Central Government Computer Systems".
[464] E-Japan Priority Policy Program, http://www.kantei.go.jp/foreign/it/network/priority-all/1.html 23.01.2013
[465] Basic Law on the Formation of an Advanced Information Telecommunication Network Society, http://www.kantei.go.jp/foreign/it/network/0626_e.html 23.01.2013

- *Национални центар за информациону безбедност* основан је априла 2005. године, са циљем да функционише као централно тело за имплементацију мера безбедности у области информационих технологија. Центар блиско сарађује са Саветом за политику информационе безбедности.

Министарство економије, трговине и индустрије[466] одговорно је за планирање и спровођење различитих политика заштите критичних инфраструктура и информационе безбедности уз сарадњу са свим осталим релевантним институцијама. Министарство се такође бави проблемима безбедности електронске трговине, безбедности службе електронске Владе, проблемима везаним за заштиту података и истраживањима везаним за развој заштите информационих инфраструктура, као и промовисањем мера заштите критичне инфраструктуре у јапанским компанијама.

Државна полиција Јапана[467] бави се очувањем безбедности критичне инфраструктуре и истраживањем криминалних дела повезаних са оштећењем, узурпирањем нормалног функционисања и уништењем критичних инфраструктура. У последњих 15-ак година у оквиру полиције се пре свега ради на заштити информационе инфраструктуре на коју се читава држава и сви остали системи ослањају. Тако је, у оквиру полиције Јапана крајем прошлог века отворено одељење за превенцију високотехнолошког криминала, које се бави безбедносним проблемима из области информацио-них технологија и истраживањем сајбер-криминала. Године 1999. формиран је програм борбе против високотехнолошког криминала. Тада је у оквиру информационо-комуникационог бироа формирано технолошко одељење за високотехнолошки криминал, а у оквиру полиције је формиран Национални центар за информационе технологије. Априла 2004. године полиција је у оквиру информационо-комуникационог одељења сваког регионалног огранка полиције формирала посебна одељења која се баве само превенцијом сајбер-криминала. Циљ овога је унапређење технолошке подршке и заштите критичне информационе инфраструктуре.[468]

Државна полиција задужена је и за креирање службе за контролу, мониторинг и реаговање приликом инцидената везаних за информациону безбедност. Оснивање ове службе требало би да спречи или да бар минимизира последице инцидената из области информационе безбедности, а служба је такође задужена и за сарадњу са свим осталим одељењима полиције приликом откривања тзв. сајбер-терориста. Један огранак ове

[466] Министарство економије, трговине и индустрије Јапана, http://www.meti.go.jp/english 23.01.2013
[467] http://www.cyberpolice.go.jp/english/action01_e.html 23.01.2013
[468] Државна полиција Јапана, http://www.npa.go.jp/english/kokusai/pdf/Poj2007-52.pdf 23.01.2013

служе чине мобилни технички тимови или *сајбер-јединице*. Ови тимови стационирани су широм Јапана и имају један командни центар. Ове јединице баве се контролом безбедности интернета и сакупљањем и анализом података.

Министарство унутрашњих послова и комуникација[469] одговорно је за креирање основа заштите критичне инфраструктуре Јапана и бави се проблемима безбедности свих врста комуникација. Како би се критична инфраструктура успешно заштитила, током година је формирано доста политика заштите критичне инфраструктуре. Мере које су у скорије време донете углавном се односе на безбедност критичне информационе инфраструктуре, безбедност комуникација, безбедност информационих технологија и интернета. У области заштите осталих сегмената критичне инфраструктуре Јапан ради на усаглашавању својих норми са међународним законима о заштити критич-них инфраструктура. Министарство је све своје политике везане за информациону безбедност поделило у три групе: безбедност мрежа, безбедност терминална и опреме и безбедност појединаца (корисника).

Министарство једном годишње објављује извештај о информационим и комуникационим технологијама у Јапану. Извештај увек има посебна поглавља која се баве заштитом приватности и информационом безбедношћу. Циљ ових извештаја је јачање сарадње приватног и јавног сектора на питањима везаним за информациону безбедност.

Извештај о информационим и комуникационим технологијама у Јапану из године у годину бави се и проблемима настанка и заштите информационог друштва у Јапану. Министарство наглашава да су све политике везане за креирање информационог друштва (које је званично настало 2010. године) засноване на четири принципа (четири основне одлике информационог друштва): свеприсутност, универзалност, оријентисаност ка корисницима и јединственост. Поента развоја информационог друштва јесте стварање могућности да се корисници повежу на било коју мрежу, било кад и било где да се налазе, уз максимално безбедну размену.

[469] Подаци о делатностима Министарства унутрашњих послова и комуникација у области заштите критичне инфраструктуре преузети су са сајта министарства, http://www.soumu.go.jp/english/index.html 23.01.2013

5.2.3.2. Организације за формирање мера заштите, техничке операције, анализу и реаговање у области заштите критичне инфраструктуре

Партнерства приватног и јавног сектора битан су сегмент заштите критичне инфраструктуре у Јапану.[470] Тако, на пример, свеобухватна стратегија информационе безбедности из 2003. године већ садржи у једном делу предлоге везане за сарадњу државног и приватног сектора. Прва национална стратегија о информационој безбедности и акциони план безбедносних мера за заштиту критичне инфраструктуре такође указују на неопходност сарадње приватног и јавног сектора. У овим документима се указује и на неопходност за формирањем организација које ће се бавити мерама заштите, техничким операцијама, анализом и реаговањем везаним за заштиту инфраструктуре у оквиру сваког критичног сектора. Ове организације су задужене и за безбедну размену података између државних организација и приватног сектора.

Како би се омогућио безбедан проток података, Национални савет за информациону безбедност издао је протокол за размену података на основу ког се информација може класификовати према значају као *црвена* (информација која се сматра тајном и не прослеђује се даље), *жута* (информација која се може проследити, али само одређеним компанијама, никако свим учесницима у заштити критичне инфраструктуре, а још мање се сме презентовати јавности; притом и компанија која добија информацију не мора да је добије у целости, већ уз одређене рестрикције), *зелена* (информација која се може проследити свим учесницима у заштити критичне инфраструктуре) и *бела* (информација која се може проследити јавности).[471]

Државни тим за реаговање током инцидената везаних за критичне информационе инфраструктуре део је Канцеларије за безбедност информационих технологија, која функционише у склопу кабинета секретаријата за заштиту критичне инфраструктуре. Тим је основан априла 2002. године и задужен је за реаговање у случајевима сајбер-криминала као нека врста Владиног рачунарског тима за реаговање у ванредним ситуацијама. На основу Акционог плана о информационој безбедности е-Владе Јапана (план је усвојен 10. октобра 2001. године, а донела га је Комисија за промоцију безбедности информационих технологија), Државни тим за реаговање

[470] Comprehensive Strategy on Information Security (executive summary): http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf 23.01.2013

[471] Податак је преузет са званичног сајта Националног савета за информациону безбедност Јапана, http://www.nisc.go.jp/eng/pdf/overview_eng.pdf, p. 51, 23.01.2013

током инцидената везаних за критичне информационе инфраструктуре чини 17 експерата из области информационе безбедности из државног и приватног сектора,[472] где су дефинисани и конкретни задаци тима:[473]

Јапански рачунарски тим за ванредне ситуације и координациони центар рачунарског тима за ванредне ситуације[474] представљају независну, непрофитну организацију која функционише као државни центар за комуникацију свих рачунарских тимова за реаговање током безбедносних ицидената, а распоређени су по читавом Јапану.

Азијско-пацифички рачунарски тим за ванредне ситуације и координациони центар тима имају задатак подстрекивања и унапређења блиске сарадње међу рачунарским тимовима за ванредне ситуације у региону, уз очување поверења међу чланицама организације, а све са циљем развијања свести о важности информационе безбедности.[475]

Телекомуникациони центар за размену и анализу података представља независну организацију, основану јула 2002. године. Центар ради на унапређењу безбедности критичне инфраструтуре кроз прикупљање, анализу и размену података о претходним инцидентима, затим кроз саветовање и препоручивање противмера којима би се у случају инцидента заштитила критична инфраструктура, кроз координисање сарадње разних организација које учествују у заштити критичне инфраструктуре итд.[476]

Сајбер-јединица представља одсек у оквиру полиције који се бави прикупљањем података и доказа са интернета везаних за сајбер-криминал. Када сајбер-јединица детектује неки неуобичајени феномен, она шаље обавештење операторима критичне инфраструктуре податке о догађају уз одређене препоруке о начину реаговања, како би спречила сајбер-нападе. Истовремено, шаље операторима критичне инфраструктуре и савете о томе како да ограниче ефекте напада и минимизирају последице, а затим и

[472] http://www.nisc.go.jp/en/sisaku/h1310action.html 23.01.2013
[473] http://www.nisc.go.jp/en/shoukai/nirt 23.01.2013
[474] Више информација о активностима јапанског рачунарског тима за ванредне ситуације и координационог центра могу се наћи на званичном сајту, http://www.jpcert.or.jp/english 23.01.2013
[475] Све земље чланице азијско-пацифичког рачунарског тима за ванредне ситуације и координационог центра овог тима побројане су на званичном сајту, http://www.apcert.org/about/structure/members.html 23.01.2013
О циљевима и делатностима азијско-пацифичког рачунарског тима за ванредне ситуације и координационог центра овог тима може се наћи на интернет адреси, http://www.apcert.org/about/mission/index.html 23.01.2013
[476] Информације о телекомуникационом центру за размену и анализу података налазе се на сајту, https://www.telecom-isac.jp/index.html 23.01.2013

како да безбедно изврше опоравак инфраструктуре након напада и како да пронађу разлоге инцидената или починиоце сајбер-напада.[477]

Електронска полиција Јапана (*@police*) има задатак да обезбеди превенцију сајбер-напада већих димензија или спречавање ширења оваквих електронских инцидената, кроз брзу размену података везаних за информациону безбедност. Сем тога, *@police* ради на развијању свести о опасностима сајбер-напада међу корисницима интернета. С тим циљем, *@police* пружа низ различитих савета везаних за коришћење интернета, како би се пружила помоћ што већем броју људи и како би што више људи унапредило своју сопствену безбедност. Између осталог, служба *@police* нуди низ он-лајн безбедносних курсева, затим указује на примере интернет криминала и начине за избегавање таквих напада, омогућава брзе безбедносне провере рачунара и указује на недостатке у заштити интернет корисника. Служба електронске полиције корисна је како за кориснике интернета и рачунара, тако и за администраторе сервера и пружаоце услуга.[478]

5.2.3.3. Законске регулативе везане за заштиту критичне инфраструктуре у Јапану

Закон о неовлашћеном упаду у рачунаре из 1999. године забрањује неовлашћене упаде у рачунаре и системе којима је приступ ограничен преко контроле приступа, кроз уношење било које информације (сем идентификационог кода) или команде преко телекомуникационе линије, чиме се притом заобилази систем контроле приступа, као и прослеђивање или ширење туђег идентификационог кода за приступ неком систему (који иначе има ограничен приступ), некој трећој особи (особама), која тиме може неовлашћено да упадне у рачунарски систем.

Сем тога, јапански Кривични закон у члану 258 као незаконито дефинише и оштећивање докумената, електронских и магнетних записа било да су у јавном или приватном власништву.[479]

Закон о електронском потпису из 2000. године има за циљ унапређење дистрибуције и обраде података електронским путем уз лако коришћење електронског

[477] Подаци о сајбер јединици налазе се на сајту Сајбер полиције Јапана, http://www.cyberpolice.go.jp/english/action02_e.html 10.02.2013
[478] http://www.cyberpolice.go.jp/english 10.02.2013
[479] http://www.cybercrimelaw.net/laws/countries/japan.html 10.02.2013

потписа, а последично циљеви су и побољшање квалитета живота грађана и развој националне економије.[480]

Закон о развоју напредног информационог друштва из 2001. године има за циљ промовисање мера за формирање и развој напредних информационих и телекомуникацио-них мрежа, како би сви становници Јапана могли да уживају у бенефитима модерних информационих и телекомуникационих технологија. Ове мере обухваћене су члановима 16 до 24 Закона и укључују промоцију отвореног тржишта на ком су сви учесници равноправни, реформу прописа и олакшавање електронске трговине кроз мере заштите, промоцију и развој електронске Владе и дигитализацију свих државних управа и администрација, подизање нивоа безбедности мрежа као и унапређење заштите личних података, промоцију креативног истраживања и развоја и на крају мере наравно укључују и унапређење међународне сарадње.[481]

[480] Више података о садржају и циљевима закона о електронском потпису може се наћи на сајту: http://www.cas.go.jp/jp/seisaku/hourei/data/aescb.pdf 10.02.2013

[481] Садржај Закона о развоју напредног информационог друштва може се наћи на сајту: http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html 10.02.2013

6. СПЕЦИФИЧНОСТИ УГРОЖАВАЊА КРИТИЧНИХ ИНФРАСТРУКТУРА У ЗЕМЉАМА У ТРАНЗИЦИЈИ

6.1. Појам транзиције и основне карактеристике и проблеми земаља у транзицији

Појам транзиције употребљава се у различитим областима – како у природним тако и друштвеним наукама. Реч транзиција изведена је од латинских речи *trans* − преко и *eo, ire* − ићи и означава прелаз. Иако многе дефиниције овог појма полазе од његове примене у појединим областима (економија, политика, итд), транзиција у суштини означава прелаз из једне друштвено-економске формацију у другу, изражавајући при томе комплекс политичких, економских, безбедносних, културних и других промена у свим областима друштва или државе.

Транзицију прати темељна измена система вредности једне заједнице која се између осталог изражава као тежња за плурализмом друштвених вредности. Тај плурализам означава: плурализам власништва, демократски и вишестраначки политички систем, цивилно друштво, као и социо-културни плурализам. У оваквом одређењу, појам транзиције односи се на прелазак друштва из једнодимензионалне вредносне димензије у вишедимензионалну.[482] Полазећи од плурализма као нормативно пожељног циља, многи аутори говоре и о три транзиције или три аспекта транзиције: *транзицији власништва и тржишта*, *транзицији политичког система* и *социо-културној транзицији*. Тако нпр. Војнић дефинише транзицију као "интеракцију транзиције власништва, транзиције тржишта и транзиције политичког система".[483]

У геополитичком значењу, које је присутно у савременој дневнополитичкој употреби, под појмом транзиција подразумева се процес демократизације земаља некадашњега источноевропског, социјалистичког блока. У том смислу овај појам означава измену геополитичке равнотеже насталу после пада Берлинског зида и окончања Хладног рата. У пракси се овај појам најчешће везује за промене у државно-политичком, економском и безбедносном систему социјалистичких земаља, у источној и централној Европи. Међутим, транзиционе промене нису карактеристичне искључиво за поменуте државе већ могу да се посматрају и много шире. Ови процеси

[482] Armijo, L. E., Biersteker, J. T., Lowenthal, J. A., (1994), *The Problems with Simultaneous Transitions*, Journal of Democracy Vol. 5 No.4, October.

[483] Војнић, Д., (1993), "Економија и политика транзиције и хрватско господарство у транзицији", *Економски преглед*, 44 (1-2): 37-54

захватили су и Русију, азијске земље, а у одређеном облику присутни су и у Африци и Латинској Америци.

Када се ради о транзицији у посткомунистичким земљама, треба имати у виду да се не ради о друштвима стабилне демократије, које у својој традицији имају либералне идеје парламентаризма, правне државе, слободног тржишта и људских права. Та друштва, иако су претходно имала зачетке либералних идеја, свој пут развоја су после II светског рата, под утицајем и доминацијом Совјетског Савеза, усмерила ка социјалистичком државном уређењу. Такав систем подразумевао је државну својину, власт партије, ограничење или чак суспендовање основних људских права, давање предности колективитету и планску привреду.

Овај систем показао се политички и економски инфериорним у односу на западни модел. Разна ограничења, као и политичка и економска затвореност система нису били довољни да буде компатибилан са дешавањима у међународном окружењу. Све то је условило да систем почне да се урушава изнутра. Ограничење инвентивности и строга контрола развоја технологије, били су препрека покретању система. Планирањем и контролом *одозго* разарала се динамична природа економског система. Промене су биле неопходне. Могло би се рећи да је и пре колапса Совјетског Савеза, ланац социјалистичких држава био у озбиљној системској кризи за коју нису постојали адекватни одговори.

Са друге стране, Запад је развијао политичко-економски систем у коме су највише вредности приватна својина, подела власти и плурализам, индивидуализам и људска права и, као незаобилазна одлика Запада − слободно тржиште. У том смислу је једно од суштинских одређења транзиције, управо, трансформација система планске привреде у систем тржишне привреде. У складу са оваквим ужим одређењем, поједини аутори сматрају да је уместо израза транзиција боље користити појам пост-социјалистичка трансформација.[484]

Међутим, ова тумачења не подразумевају суштину промена када су у питању бивше земље реалног социјализма. Чињеница је да су и земље развијене демократије имале и имају своју *транзицију*, која се битно разликује од постсоцијалистичке, како због континуитета политичко-економског система, тако и због саме природе вредности на којима почивају ова друштва.

[484] Stark, D., (1994), "Recombination Property in East Europe Capitalism", *Public Lectures*, No. 8, Collegium Budapest.

Према Семјуелу Хантингтону,[485] процес транзиције бивших социјалистичких земаља укључује три фазе.

Прва фаза је слом социјалистичких система. Та фаза је спроведена у свим европским државама. Она је уследила због нестанка легитимности реалсоцијалистичког типа владавине, у којем сила и принуда нису биле више одрживе. Модерни политички системи према Холмсу своју легитимност могу да заснивају на успешно спроведеној транзицији оствареној на различитим подручјима од економског развоја, грађанских и политичких слобода, слободног тржишта до аутономије моралне, културне и религијске сфере.

Друга транзициона фаза заснива се на приближавању већ готовом моделу развијених друштава тржишне економије и либералне демократије. Ова фаза одвијала се кроз комбинацију континуитета и дисконтинуитета. Континуитет представљају обрасци ауторитативне политичке културе, игнорисање владавине закона, клептократски однос према јавној имовини, нетолеранција итд., док дисконтинуитет чине слободни и демократски избори, институције вишестраначког система, приватизација друштвеног власништва, тржишна екомонија, медијски плурализам итд. Транзиција за бивше социјалистичке земље представља убрзани процес који је у западним земљама пролазио кроз деценијске циклусе и због тога у транзиционим земљама производи изненађујуће, често шокантне друштвене последице.

Трећа фаза је најдужа и да би се остварила консолидација новог система потребно је да се испуни шест међусобно повезаних услова:

1. Успостављање институција вишестраначких, слободних избора и тржишне економије,
2. Обликовање виталног и слободног цивилног друштва,
3. Конституисање релативно аутономног политичког друштва (деловање политичких странака, законодавство, избори и изборна правила, политичко руковођење итд.),
4. Владавина права (заштита индивидуалних слобода и деловања удружења, која се односи на све политичке актере),
5. Државна администрација која служи свим грађанима и у њиховом интересу спроводи интенције демократске власти,

[485] Hantington, S., (2000), *Сукоб цивилизација*, ЦИД Подгорица и Романов Бањалука.

6. Институционално организовано економско друштво (систем социополитичко обликованих и прихваћених норми, институција и прописа који кореспондирају између државе и тржишта).

Појам транзиција у међународним односима користи се и изван овог терминолошког одређења. Семјуел Хантингтон је, на пример, ратове у којима доминирају етнички сукоби и ратови због неодговарајуће границе између група из различитих цивилизација, назвао – транзициони ратови.[486]

Важан елемент транзиције је транзиција вредности која је често праћена шоком и неразумевањем, као што је већ виђено у претходним историјским периодима ренесансе реформације, контрареформације.[487] Шок је финале процеса губљења легитимитета са којим се суочава претходни институционални аранжман. У такве примере транзиције могу да се уброје периоди након Француске или Октобарске револуције.

Транзиција бивших социјалистичких земаља третира се као наставак трећег таласа демократизације чији су део и Грчка, Шпанија, Португал и Јужноафричка Република. Четврти талас би требало да представља демократизација и трансформација економског амбијента азијских земаља.

У теоријско-динамичком приступу транзицији присутно је неколико школа које овај процес третирају са становишта различитих метода и динамике. Најчешће се до сада дебата о транзицији бавила питањем да ли се ради о шок методу или постепеном приступу.

Најпознатија школа шок методе (Big Bang) је *Cambridge Mass*,[488] технократска верзија градуализма коју је развио Ероу (K. J. Arrow), док еволуционистичку школу представљају поборници *јавног избора* (*public choice*), институционалисти и аустријска школа. У основи ових приступа налази се економска димензија транзиције и њихови аутори и поборници сматрају да она доминантно одређује динамику и укупан ток транзиције:

1. Шок терапија подразумева брзу либерализацију, балансирање буџета, конверти-билност валуте, компресију социјалних давања, приватизацију – брзо импле-ментирани социјални инжењеринг који подржавају

[486] Hantington, S., (2000), "*Сукоб цивилизација*", ЦИД Подгорица и Романов Бањалука, стр.273
[487] Kates, R., Leiserowitz, A., and Parris, T., (2006), Great Transition Values Present Attitudes, Future Changes, GTI Paper Series 9, Tellus Institute.
[488] Murrell, P., (1995), "The Transition According to Cambridge, Mass", *Journal of Economic Literature*, Vol. 33, No. 1 (Mar), pp. 164-178

неолибералне институције као што су ММФ или Светска банка где је неопходна њихова помоћ као компензација за болне реформе. Једном речју, основа овог приступа су радикалне реформе и убрзана трансформација.[489] Основни елемент је привати-зација с циљем деколективизације друштва и разбијања система централног планирања, а главни недостаци су занемаривање макроекономских питања и неформалних институција – примена јединственог рецепта.

2. Градуалисти се залажу за интервенционистичку политику постепене либерали-зације у циљу одржавања ниске стопе незапослености и социјално праведне расподеле. Градуализам полази од идеалне државе што је кључна мана. У оба случаја потпуно је занемаривано питање економских слобода у циљу инстала-ције нових институција.
3. У оквиру еволуционистичког приступа, аустријска школа транзиције[490] избегава механички прилаз транзицији истичући да је свака земља прича за себе. Она посматра процес транзиције из угла појединца за кога се након историјског шока отвара низ нових прилика. У анализи институционалиста су транзициони трансакциони трошкови – односно време за развој културе индивидуализма и капитализма. Анализа транзиције обухвата анализу владавине права, носилаца институционалног реструктурирања и неформалних институција. По овом приступу, транзиција је успешна ако се јаз између формалних и неформалних институција смањује уз континуирано креирање подстицајне структуре.

У теоријском приступу се понекад користи и теорија о постепеној конвергенцији капиталистичког и социјалистичког економског система. На основу ових теоријских разматрања приликом транзиције долази до стварања потпуно новог система, који узима најбоље и од једног и од другог система. Транзиција се у овом виђењу третира као двоструки процес трансформације социјализма у капитализам и капитализма у социјализам. Од капитализма се узима приватна својина, профит као мотив и економски стимуланс, и тржишни систем, као и критеријум расподеле роба и услуга. Социјализам са собом доноси већу социјалну једнакост, самоуправљање као

[489] Merlevede, B., Schoors, K., (2004), *Gradualism versus Big Bang: Evidence from Transition Countries*, Ghent University, Belgium, Department of Economics&CERISE, April.

[490] Један од водећих представника је Фридрих Хајек филозоф и економиста, залагао се за либерализам а против социјализма и етатизма.

идеју радничке контроле над условима рада и неопходност данашњице – економско планирање.

Иако је ова теорија третирана као утопистички приступ, пракса је показала да она има реалне основе. Одличан пример ове конвергенције представља Народна Република Кина, која је остварење свог економског интереса видела у економским реформама и отварању према свету, после вишедеценијске *затворености*. Принцип конвергенције може се најбоље препознати у кинеском економском правилу да државна својина чини основу система, а приватна својина се развија као њена допуна. Кинески пример је најбоља потврда да не постоје *чисти* или једнострани идеолошки системи. У циљу опстанка, развоја и стабилности, савремени економски систем интегрисао је позитивне елементе и социјалистичког и капиталистичког економског система.

Транзиција се такође може посматрати и као процес интеграција у ЕУ. За земље које су ушле у ЕУ, транзиционо-интеграциони оквир представљала је примена Копенхагеншких критеријума из 1993. и права ЕУ кроз тзв. европске споразуме, а за земље Западног Балкана то је процес стабилизације и асоцијације. Оно што је спорно код овог програма је брзина спровођења реформи, тј. време трајања транзиције. Истовремено су се земље ЕУ економски развијале у потпуно другачијем амбијенту и са другачијом полазном основом. Очигледно је да се искуства Грчке, Шпаније или Португала са растом БДП, СДИ и субвенцијама тешко могу применити на земље источне и централне Европе.

Транзиција као вишедимензионални процес и успешно спроведене економске трансформације и вишестраначје не чини неку земљу аутоматски демократском. Један од значајних индикатора овог процеса су медији који представљају значајну карактеристику демократског карактера неког друштва.

Процес транзиције у Србији је у почетку био под великим утицајем кризе на простору претходне Југославије. Њега је карактерисао немоћ парламентаризма и доминација политике над економијом, док је процес политичке транзиције, односно остваривања политичких слобода, био оптерећен периодом санкција и међународне изолације, политичким конфликтима унутар СРЈ, НАТО агресијом и разарањем друштвено-економских ресурса, међународним трупама на делу територије, одвајањем Црне Горе, осамостаљењем Србије и косовском кризом, која ни након потписивања споразума још увек не јењава. Политичку транзицију прати и еволуција вредности – становништво је већински опредељено за нове демократске и политичке вредности:

слободу говора, независност медија, независно судство итд., као вредности грађанског друштва. Даљи развој владавине закона и владавине права неопходан је за консолидацију политичких слобода.

Транзиција у Србији је и даље оптерећена бројним изазовима. Демократске институције су још слабе, корупција и организовани криминал су озбиљни друштвени проблеми, политичке коалиције крхке, а доносиоци политичких одлука без стратешке визије. Један од централних проблема је међународни политички процес поводом статуса Косова и његово решавање. Постоје и бројни проблеми везани за примену закона и функционисање правосуђа, финансирање политичких странака, пролиферацију бирократије и висок ниво јавне потрошње, концепт приватизације друштвене својине и малверзације у вези са тим, пораст насиља и нетолеранције. Јавно мњење подељено је око битних питања као што су приступање ЕУ, НАТО, сарадња са Хашким трибуналом, тако да практично српском друштву недостаје минимални политички консензус око основних заједничких вредности.

Поред тога, у Србији се започело са структурним реформама које су обухватиле: пореску реформу, реформу банкарског система, формулисање индустријске политике која прави разлику између успешних и неуспешних предузећа, заустављање еколошког уништавања средине изазваног екстензивним начином производње, спречавање продужавања монополског положаја појединих привредних организација и успостављање правила за слободну конкуренцију на тржишту.

6.2. Фактори угрожавања критичних инфраструктура у земљама у транзицији

У земљама у транзицији постоје бројни проблеми који могу да отежају реформске процесе. Пут интеграције у светску привреду ни у ком случају није лак и може да траје јако дуго. Напредак процеса интеграција није равномеран за све земље. У неким од напреднијих земаља носиоци економске политике се суочавају са брзим порастом улоге тржишта и великим приливом капитала, што је праћено средњорочним фискалним проблемима као у развијеним привредама Европске уније. У другим земљама напредак није био уједначен у важним областима као што су реструктурирање предузећа и банака и реформа правног оквира, уз значајан посао који преостаје да се уради у процесу транзиције ка тржишној привреди."[491]

[491] Ковачевић, Р., (2002), "Транзиција земаља Централне и Источне Европе у тржишну привреду", Институт за спољну трговину, Београд, *Привредна изградња*, вол. 45, бр. 3-4, стр. 149-178

Прелазак из социјалистичког у демократско, отворено друштво подразумевао је за све земље динамично успостављање принципа тржишне економије. С обзиром на полувековну праксу социјалне државе, потпуно препуштање правилима тржишта уништило би економске системе земаља у транзицији. Због тога, било је неопходно да се трансформација система обавља уз очување одређених елемената социјалне државе. Промене су вршене постепено, али нису ретки били примери тзв. шок-терапија. Многе земље су имале доста проблема и било је неопходно да више пута у ходу мењају зацртани курс, док се друштва нису стабилизовала.

Постигнути резултати транзиције у неким земљама нису испунили очекивања која су произилазила из теоријских претпоставки, дефинисаних на почетку транзиције. Инфлација је у већини случајева осетно порасла, као непосредна последица макроекономске неравнотеже. Обим производње је смањен у свим транзицијским земљама, а број незапослених се изразито повећао. Разлике у нивоу дохотка су се проширили, а социјални конфликти заоштрили. Корупција је постала свеприсутна у бившим социјалистичким земљама, а формирао се и нови јаз између села и града будући да су међусобне разлике продубљене.

Највећи проблеми који су оптерећивали реформе односили су се на денационализацију, приватизацију, корупцију, и у вези са њима, спорим доношењем и неодлучном применом системских закона, који су били неопходни за отпочињање ових процеса. У складу са овим проблемима, за грађане у земљама у транзицији, идентификован је читав низ отворених питања за чије решавање је потребан дужи временски период и озбиљна помоћ развијених западних земаља:[492]

- Драстичан пад индустријске и сличне призводње,
- Недовољно подстицање индустријске производње,
- Смањење инвестиционих улагања,
- Споро освајање нових тржишта и укључивање у светске токове робе и услуга,
- Успорен прилив страног капитала,
- Неадекватна афирмација полицентричног развоја,
- Занемаривање проблема пољопривреде и села,
- Преспоро решавање еколошких проблема,
- Пораст незапослености и масовна отпуштања радника,

[492] Ibid

- Драстично повећање социјалних разлика,
- Пад животног стандарда,
- Недовољна брига за пензионере и угрожене социјалне категорије становништва,
- Пад квалитета здравствене заштите,
- Повећана лична несигурност грађана,
- Незаконито богаћење појединаца и
- Ширење мита и корупције.

Највећи проблеми у региону ЈИЕ и даље су политичка нестабилност и велики екстерни дебаланси, посебно дефицити платног биланса. Земље Западног Балкана заостају у спровођењу реформи, па су у наредном периоду у тим земљама нужне интензивније реформске промене у многим областима привреде и друштва.

Карактеристично за све земље Западног Балкана је да су то углавном мале неконкурентне привреде, недовољно усклађене са европским и међународним нормама и стандардима, да све земље имају дефицит трговинског биланса и буџета. Све оне, мање више, имају незадовољавајућу инфраструктуру, недостатак обртног капитала и недовољну и неадекватну кредитну подршку, високо учешће сиве економије и још увек значајно присутну корупцију и криминал.

Кад је реч о класификацији фактора који угрожавају развој и заштиту критичне инфраструктуре у Србији, није увек једноставно приписати неки од проблема који проистичу из транзиције и који директно стварају проблеме критичним инфраструктурама само једном конкретном фактору из разлога међусобне испреплетености политике, економије и свих осталих фактора.

6.2.1. Структурно-организациони фактори

У процесу транзиције неопходно је проћи низ корака и спровести велики број реформи у различитим областима. Један од неопходних корака је и борба са структурно-организационим слабостима државе кроз спровођење реформи у областима у којима су те слабости изражене. Структурне реформе које се по правилу спроводе у свим земљама у транзицији имају за циљ да створе погодне услове за виши ниво улагања који је неопходан за одрживи економски развој и повећање броја запослених, затим да увећају конку-рентност економије, и на крају да створе услове за одрживи

процес транзиције. Главни типови структурних реформи који се морају спровести у свакој земљи која пролази кроз процес транзиције су:[493]

- Реформа правног система,
- Реформа финансијског сектора и
- Реформа предузетничког сектора (укључујући приватизације, промоцију и подршку малим и средњим предузећима и реструктурирање предузећа).

Било какви проблеми који настану током спровођења реформи у овим секторима утичу и на критичне инфраструктуре и директно или индиректно угрожавају њихово нормално функционисање.

За формирање тржишно оријентисане економије у државама у транзицији неопходно је обавити свеобухватну реформу правног система. Добар део земаља у транзицији започео је са реформама правног, правосудног и законодавног система, а велики број њих је и прилично одмакао у процесу спровођења реформи. Први део реформе правосуђа подразумева усвајање закона неопходних за даљи ток транзиције (закони везани за имовину, безбедност, компанијско пословање, слободу тржишта, приватизацију и низ других закона). Иако само доношење закона јесте битно, без ефективне имплементације и примене закона, процес транзиције се доста успорава и настаје велики број проблема у следећим фазама. Тако на пример у неким земљама у транзицији постоје прилично непоуздани системи уноса земљишта у катастар, што даље валидност неких трансакција власништва над земљиштем чини сумњивим и лако може да угрози КИ. Слични проблеми могу да се десе у оквиру било које области која се за потребе ефикасног спровођења транзиције мора законски регулисати, и у којој се након доношења закона тај закон мора и ефикасно примењивати. Тако, на пример, законска и правна регулатива о стечају, која је иначе од кључног је значаја за ефикасну трансформацију земаља у транзицији јесте усвојена у многим државама у транзицији. Међутим, неадекватна судска и административна подршка је изостала, па је стога имплементација закона у многоме отежана, што оставља негативне последице на предузећа, која се врло често потпуно гасе, а са њима одумире и део критичне инфраструктуре.

Транзиција ка тржишној економији захтева драстичне промене улога финансијског сектора, која уз посредовање финансијских институција омогућава каналисање ресурса директно ка предузећима. С обзиром на то да су банке доминантни

[493] Ibid

сегмент финансијског система земаља у транзицији, а и представљају везу између ненаплативих кредита и губитака које остварују предузећа у земљама у транзицији, банкарски сектор је први на удару приликом реформи финансијског сектора у земљама у транзицији. Увођење тржишних реформи приморало је банке да започну сопствену транзицију и да уместо улоге пасивног даваоца кредита почну да обављају све улоге које банке у другим тржишним економијама обављају – да излазе у сусрет потребама својих клијената с једне стране, а да се придржавају критеријума адекватности капитала и нових рачуноводствених правила везаних за наплате дугова, с друге стране. Процес трансформације банака у земљама у транзицији наилази на низ проблема. Први је висока концентрација банкарског тржишта. Тржишни удео пет главних банака у земљама у транзицији обично чини 2/3 или чак 4/5 целокупног тржишта што је директна последица заоставштина из периода пре транзиције и рефлектује континуирану доминацију државних банака или бивших државних банака. Други проблем представља висок удео ненаплативих кредита. Као резултат транзиционог шока, сектор предузећа акумулирао је велике финансијске губитке услед чега се повећао број ненаплативих кредита код банака. Трећи проблем банкарског сектора су високи трошкови трансакција. Велики број ненаплативих кредита присилио је банке да у многим земљама у транзицији задрже прилично велике разлике између активних и пасивних каматних стопа. Још један разлог високих трансакционих трошкова су и високи оперативни трошкови банака. Услед ниже ефикасности банкарског сектора у земљама у транзицији оперативни трошкови су скоро дупло већи него у развијеним државама са тржишним економијама. Четврти проблем са реструктурирањем банака је неадекватан приступ издавању кредита. У земљама у транзицији кредити се издају углавном средњим и великим компанијама, које су врло често и даље у власништву државе. Такав приступ у ком државне фирме имају привилегован статус приликом издавања кредита, ограничава укупан износ који банке могу да усмере на кредите за нове потенцијалне дужнике, посебно на нека мала и средња предузећа и индивидуалне предузетнике. На тај начин приватни сектор се гаси, а он је у свету све значајнији за функционисање и заштиту КИ, јер се управо све већи део КИ налази баш у власништву приватног сектора.

Реформисање предузетничког сектора један је од основних елемената транзицио-ног процеса и у суштини представља транзицију од доминантно јавног ка доминантно приватном власништву предузећа и укључује:[494]

- Увођење финансијске дициплине и конкуренције у предузетничком сектору,
- Развој приватног сектора кроз приватизацију државних (јавних) предузећа, као и кроз промоцију и подстицање развоја нових приватних предузећа и
- Реструктурирање предузећа, како у периоду пре тако и после приватизације.

Почетак транзиције у великом броју земаља у транзицији карактерише велико погоршање ликвидности предузећа, с обзиром на то да се профит предузећа драстично смањује или се своди на нулу услед отварања тржишта за стране конкуренте, док банке истовремено у новом предузетничком окружењу све теже одобравају нове кредите. У таквим околностима (пад ликвидности предузећа уз приоритет плаћања радника) предузећа обично почињу да одлажу своја плаћања снабдевачима. То за резултат има пораст међукомпанијских дугова, као и све већа дуговања у виду пореза и социјалних давања, а што даље води компаније у све већу финансијску пропаст. Поред смањене кредитне способности банака и мањег броја издатих кредита, државе у транзицији жестоко редукују субвенције према фирмама (било да то раде кроз директно или индиректно *резање* буџета или кроз укидање субвенција за електричну енергију или за сировине), што је такође важан сегмент увођења финансијске дисциплине у предузетнички сектор. Тако је, на пример, у Русији укупан ниво државних субвенција пао са 32% БДП-а колико је износио 1992. године на 6% у 1994. години.[495] Упркос смањењу државних субвенција, оне су ипак на почетку транзиције, а и дуго након тога веће од оног што се очекује на крају транзиције. Такође, пракса и истраживања су показала да државне фирме у земљама у транзицији ипак имају привилеговани приступ државним кредитима за финансирање привреде. У просеку, кад се све сабере, земље у транзицији својим инвестицијама покривају 26% издатака државне фирме.[496]

Практично све земље у транзицији настоје да спроведу приватизације на два нивоа истовремено. Државе настоје да обаве *мале приватизације*, што се односи на приватизовање малопродајних радњи, транспортне опреме и предузећа која се баве пружањем услуга. Овај сегмент приватизација није тема политичких контроверзи и доста је подржан и оцењен као транспарентан и са позитивним резултатима који се

[494] Ibid
[495] World Bank, 1996, p. 45
[496] EBRD, Business Environment and Enterprise Performance Survey, 1999, p.137

постижу у релативно кратком временском периоду. Осим *малих приватизација* постоје и *велике приватизације*, као што су приватизације предузећа која су била у државном власништву. За разлику од *малих приватизација* ове друге означене су као много компликованије него што се то исправа мислило, али и мање униформне него што је то био случај са *малим приватизацијама*. Спорији темпо *великих приватизација* у земљама у транзицији обично је последица више ствари: високих захтева за капиталом, неопходности великих реструктурирања, реституционих проблема, регулаторних и управних слабости као и политичке осетљивости или чак политичког отпора.

Мала и средња предузећа су витални, динамични део тржишних економија, који игра важну улогу у свеукупном економском расту држава са развијеном тржишном економијом. Све земље у транзицији пред себе стављају као битан задатак развој сектора малих и средњих предузећа. Законима се формира правни оквир за функционисање МСП, а неке земље које су у поодмаклим фазама транзиције већ су могле да искусе велики раст и развој сектора МСП. Процес транзиције обележавају у почетку оснивања малих фирми у виду старт-ап предузећа, која се углавном баве трговином или пружањем разних услуга.

6.2.2. Политички фактори

У савременом свету политички фактори утичу на креирање економске политике, у нешто ширем контексту утичу на укупан економски амбијент, а најшире на све друштвене делатности, па у том контексту и на критичне инфраструктуре. Клацкалица *држава – тржиште* на којој су се привреде налазиле током двадесетог века, некада би превагнула на страну државе, а некада на страну тржишта. Са променама у начину вођења економије током двадесетог века дошло је и до значајних политичких промена.[497] Сматра се да су се у прошлом веку десила три таласа демократизације: први – пре Првог светског рата, други – након Другог светског рата и трећи – деведесетих година XX века. Ови таласи су се односили на проширење бирачког права и укључивање свих структура становништва у изборни процес, затим на настанак нових држава – укидање колонијалног система, што је подразумевало и ослобађање политичке воље великог дела човечанства, а на крају и повратак тржишта и парламентарне демократије у земље које су више деценија имале ауторитарне режиме

[497] Зец, М., Церовић, Б., (2008), *Куда иде Србија? – остварење и домети реформи*, Научно друштво економиста и Економски факултет у Београду, (Александра Прашчевић, 3. поглавље − Политички фактори макроекономске нестабилности у Србији), Београд, стр.1

под совјетском доминацијом. Сваки од ових догађаја имао је вишеструки утицај на економска кретања, као и на процес транзиције.

Развој парламентарне демократије постао је у бившим социјалистичким земљама незаобилазан елемент самог процеса транзиције. Економске реформе које је требало спровести ишле су паралелно са процесом демократизације, а често су биле и условљене њоме. Али, на једној страни су се налазиле политичке промене које су подразумевале развој вишепартијског система, укључивање јавности у доношење свих политичких одлука, развој цивилног друштва, изградњу институција и слично, које су у великој мери имале подршку јавности. Одговор на ова питање подразумева стварање друштвеног консензуса између најзначајнијих структура друштва око поделе терета транзиције, као и око веома важног питања брзине реформи.

Ако се земља у економској транзицији определила за развој парламентарне демократије, неопходно је да економске реформе буду вођене и у циљу консолидовања демократског система. Неке земље су у склопу економске транзиције отпочињале развој демократије и демократских институција, а онда су се поново враћале у недемократски систем због великих економских проблема који су се посебно огледали у повећаном раслојавању и сиромаштву.[498] Такав повратак у недемократски систем у великом броју случајева довео је до још већих политичких нестабилности које су увек повезане са даљим погоршањем економских услова у овим земљама. Консолидовање демократије подразу-мева изградњу, имплементацију и развој одређених демократских институција и развој цивилног друштва, а читав тај процес јако је болан по велики део друштва.[499]

Основно правило демократије је да политичари морају да обезбеде подршку гласача како би победили на изборима. Полазећи од тога, у условима парламентарне демократије, креатори економске политике могу да искористе економску политику ради повећања сопствених шанси да победе на изборима, чиме се дефинише још један фактор угрожавања друштвених процеса и посредно критичних инфраструктура – обмањивање јавности. То је кључни правац којим политика утиче на економију и на друштво.[500] Истовремено, идеолошка оријентација креатора економске политике може бити одлучују-ћа за формулисање економске политике, тако да није

[498] Тако је нпр. било у земљама Латинске Америке попут Аргентине, Бразила, Чилеа, Перуа, Гватемале, Венецуеле, Уругваја.
[499] Acemoglu, D. and Robinson, J., (2006), *Economic Origins of Dictatorship and Democracy*, CUP, Cambridge
[500] Akhmedov, A. and Zhuravskaya E., (2004), *Oportunistic Political Cycles: Test in Young Democracy Settings*, Quaterly Journal of Economics, Vol. 11, No. 4, pp. 1301-1338

могуће утврдити исто понашање свих креатора економске политике, без обзира на њихову страначку припадност.[501]

Битно је споменути још један од водећих изазова савремених демократских промена свих земаља у транзицији − корупцију. Врло је опасно кад се она јавља у политичком и друштвеном животу и да се ствара уверење у јавности како без корупције друштво не би могло да функционише, односно да је то сасвим нормална и прихватљива појава. Познато је да корупција долази до изражаја у политички нестабилним системима, односно у временима политичких трвења и турбуленција. Тада долази до осиромашивања јавних службеника, али и слабљења политичких, правних и економских контролних механизама државе и друштва у целини. Корупцију није лако стабилизовати на одређеном ниском нивоу, посебно када она почне да напада и осваја оне делове друштва који би требало да буду брана против корупције, као што су судска власт и полиција.

Најзначајнији разлози који доводе до корупције могу се означити:[502]

- Влада својом политиком, путем уговора, приватизације и давања концесија, обезбеђује велике финансијске користи појединцима и предузећима, а субјекти ближи или *одабрани* од Владе стичу највеће користи,
- Избегавање плаћања пореза, нарочито када порески систем дестимулише привредне активности,
- Мале плате државних и јавних службеника,
- Подмићивање политичара у циљу добрих изборних резултата,
- Судство не поштује законе, већ их селективно примењује у зависности од припадности владајућој државној и политичкој структури и
- Прање новца уз свестрану помоћ државе.

Под политичком компонентом корупције подразумевају се разни видови злоупотребе службеног положаја и угледа у обављању јавних функција, које немају карактер чисто државних функција (народни посланици, лидери политичких странака, руководиоци друштвених, односно добротворних установа или удружења, и слично), али имају друштвени утицај.[503] Дакле, политичка компонента корупције

[501] Alessina, A., Roubini, N., Cohen, G., (1997), *Political Cycles and the Macroeconomy*, The MIT Press, Cambridge, MA.
[502] Ibid
[503] Весић, Д., (2008), *Економска и политичка компонента корупције*, Пројекат Министарства науке Републике Србије и Института за међународну политику и привреду, пројекат бр. 149002, децембар, стр. 486

представља основни и најопаснији вид корупције из које потиче и на коју се ослања, али и помоћу које се шири, коруптивна пракса у свим сегментима привредног а тиме и друштвеног живота. Корупција разара политику, као свесну и планску делатност политичких субјеката, а то су друштво, политичке партије, синдикати и други субјекти законодавне, судске и извршне власти.[504] Политички аспект корупције треба изузетно озбиљно третирати, а то значи да треба да постоји експлицитна, јасно изражена политичка воља на откривању и сузбијању корупције. Анализа узрока корупције, као и њеног обима и раширености, мора поћи од анализе правног система земље, јер се раширеност корупције, пре свега, посматра као један од симптома функционисања правног система, а на то указују:[505]

- Мера у којој се поштују закони од стране законодавне и управне власти,
- Мера у којој закони важе за вршиоце власти,
- Мера у којој је присутан притисак власти на правосуђе,
- Перцепција грађана и економских субјеката о обиму и величини корупције у кључним друштвеним сферама па и правосуђу,
- Начин на који грађани доживљавају функционисање правне државе и
- Легитимност институција власти мерено поверењем грађана у њих.

На основу ових мерила може се увидети у ком је степену корупција ушла у политику. У сваком случају, колико год да је заступљена корупција треба се борити против ње због нормализовања друштва и друштвених процеса, који се из већ наведених разлога не могу одвијати нормално све док корупција постоји.

Кризне и ванредне ситуације у највећем броју случајева проузрокују оштећења на инфраструктурним системима, чиме ремете устаљене начине и методе снабдевања становништва, привреде и других корисника који су директно зависни од њиховог функционисања. С друге стране, застој у свакодневном функционисању инфраструктур-них капацитета може проузроковати стање кризне и ванредне ситуације. Због тога је у земљама у транзицији приоритет на заштити критичних инфраструктурних система. На ефикасно функционисање критичне инфраструктуре у условима кризних и ванредних ситуација знатно утиче на адекватна искоришћеност ресурса система, који могу помоћи да се успешно одговори на безбедносне изазове, ризике и претње.

[504] Ibid, 487
[505] Ibid

6.2.3. Економски фактори

У свим транзиционим земљама под транзицијом у економском смислу подразумева се имплементација реформи везаних за: макроекономску стабилност (смањење и елиминисање буџетског дефицита и вођење одговарајуће неинфлаторне монетарне политике), либерализацију (унутрашњу, али и спољну која се манифестује укидањем трговинских и инвестиционих баријера и променом режима девизног курса) као и трансформацију власничких права кроз приватизацију и нове власничке аранжмане.

Низ економских показатеља даје основ за закључак да ли је земља у процесу транзиције на добром путу у спровођењу економских реформи или је запала у још веће економске проблеме чиме су додатно угрожене критичне инфраструктуре. Неки од егзактних показатеља су: бруто друштвени производ (БДП), извозни коефицијенти у % БДП-а, извоз по становнику, спољнотрговински дефицит, покривеност увоза извозом, однос спољнотрговинског дефицита и робног извоза и стопа незапослености. Уколико се сви ови подаци анализирају за случај Србије, или пак свих земаља у региону, не долази се охрабрујућих података. Наиме, према конкурентности привреда Србије се налази у другој половини табеле од 139 земаља, око 85. места, што никако не може да се сматра добрим резултатим имајући у виду да постоје и много сиромашније земље, па и оне у транзицији.[506] Извозни коефицијент Србије је врло низак (30% у 2008.), али тек се права слика добија кад се то упореди са Словачком која је повећала извозни коефицијент са 58% 1995. године на чак 83%, Мађарска са 45% на 81%, Чешка Република са 51% на 77%, а Словенија са 50% на 70%. Србија је 1995. године имала извозни коефицијент 17% што значи да је раст српског извоза драстично мањи у односу на многе земље које су прошле транзицију;[507] да су цифре о извозу робе и услуга по становнику у Србији веома ниске (1.031 евро/по глави становника), постаје јасније ако се оне пореде са малим високоразвијеним земљама. На пример, извоз по глави становника у 2009. години износио је у Белгији чак 24.349 евра;[508] релативне величине спољнотрговинског дефицита, односно покривеност увоза извозом и однос тог дефицита према робном извозу, у Србији су се драстично погоршавале у периоду 2000−2008. године, да би се од 2008. године осетно смањиле, али су још увек високе.[509]

[506] Ковачевић, М., (2011), *Димензије и узроци неуспешне транзиције Србије*, Нин, 08. јун.
[507] www.weforum.org 17.11.2012
[508] www.Trademap.org (у поглављу *export per capita*) 17.11.2012
[509] Ibid

Један од показатеља недовољно ефикасне транзиције земаља јесте драматичан раст дефицита текућег рачуна платног биланса закључно са 2008, а у неким случајевима и 2009. годином, па је његова релативна величина, тј. његов квантитативни однос према БДП, знатно прешао толерантну границу. Захваљујући светској економској кризи, која је имала за последицу драстичан пад цена низа најважнијих увозних сировина и репродукционих материјала, апсолутне величине њиховог увоза, апсолутне и релативне величине текућег рачуна платног биланса, у Србији су, а и у већини земаља у региону 2009. године осетно смањене, али су и даље остале на врло високом нивоу.[510] Слика незапослености у Србији, а и у земљама у окружењу би била још неповољнија да многи, пре свега, млади људи нису напустили своје земље и запослили се у иностранству. Сама чињеница да је на ранг листи из 2010. године Светског економског форума по интензитету одлива мозгова Албанија била на 32., Хрватска на 17., Македонија на 13., Србија на 4., а Босна и Херцеговина чак на другом месту (од 139 земаља), даје довољно разлога да се закључи да је велики број грађана из ових земаља последњих година нашао посао у иностранству и да се више не јавља на листама незапослених. Када се говори о стопи незапослености у Србији, требало би нагласити да је при том обрачуну искључено Косово у коме је стопа незапослености енормно висока, па би стопа незапослености у Србији са Косовом била још неповољнија. Приче које су биле актуелне почетком последње деценије прошлог века да ће тзв. *транзициона рецесија*, а тиме проблем и незапослености кратко трајати – показала се потпуно нетачном. Врло озбиљан проблем у свакој земљи где је стопа незапослености врло висока, као што је случај са Србијом и земљама у окружењу – јесте чињеница да је врло висок удео младих људи дуго без посла, па многи од њих трајно одлазе у иностранство, а они који остају, временом губе стечено знање, али и самопоуздање и самопоштовање, па се због свега тога знатно смањује њихов радни капацитет.

Спајање економских и политичких функција, односно управљање јавним предузе-ћима и државним фондовима од стране високих државних функционера, довело је до тога да се државна (друштвена) имовина користи у страначке сврхе. У сваком друштву инсајдери и олигарси највише профитирају у неизграђеном институционалном оквиру, а њихова моћ се смањује једино ако су либерализација и

[510] Извор: EBRD *Transition Report* 2005 и *Transition Report* 2010.

приватизација праћене јачањем дисциплине (дакле судства и владавине права) и креирањем повољне инвестиционе климе.[511]

Спремност да се понуди мито је директно пропорционална моћи потенцијалног коруптора, што за последицу има две кључне појаве:[512]

1. Уништавају се средњи и мали предузетници и
2. Затвара се тржиште и отежава улазак у посао заинтересованим привредницима.

Уопштено, корупција тада генерише стање у којем се сви учесници у тржишној утакмици осећају несигурним. У условима такве, пре свега правне несигурности, тешко се могу процењивати потези својих потенцијалних конкурената и не могу се планирати будући потези. На тај начин ствара се економска несигурност која даље проузрокује или поспешује неравноправност актера у тржишним трансакцијама. Познато је и да је у неравноправним условима свака добит нелегитимна, па самим тим и она остварена на тако монополистичком тржишту.

Први услов за елиминисање корупције, с економског аспекта, јесте присуство економских слобода, односно постојање могућности што шире неспутане активности појединаца на тржишту. Даље то значи, у позитивном смислу, најширу слободу избора, а у негативном, одсуство сваке принуде и присиле у економским активностима, уз обавезно поштовање закона. У том смислу економске слободе зависе од сигурности власничких права, економске политике, слободе уговора, обима државне интервенције у привреди, царинских и пореских оптерећења, квалитета и степена регулације, државне потрошње, слободе уласка у посао, па све до општег стања у друштву, односно привредне и друштвене климе. Овако схваћене слободе економисти називају и економским или тржишним слободама. Од степена економских слобода у великој мери зависи развијеност тржишта, односно краткорочни и дугорочни раст националне привреде.[513]

---

[511] Поповић, Д., (2003), "Добитници и губитници у транзицији", *Политика*, Економетар, бр. 16 од 23. септембар, стр. 3

[512] Ibid

[513] Весић, Д., (2008), *Економска и политичка компонента корупције*, Пројекат Министарства науке Републике Србије и Института за међународну политику и привреду, пројекат бр. 149002, децембар, стр. 484 и 485

6.2.4. Културално-перцептуални фактори

У друштвима и срединама које су доживеле темељан распад скупа вредности на којима су почивале, као и распад функционисања унутрашње друштвене и политичке организације, државних и културних институција, свака расправа о месту и правцу развоја културе веома је тешка и мора узети у обзир ове специфичне околности.

Карактеристика друштава у транзицији јесте снажно уплитање политике у све сфере живота, укључујући и културу. Ипак, политика културе у овим земљама није увек јасно профилисана и конзистентна.

У земљама бившег источног блока и Европи уопште важан део културне продукције и стимулације потиче из државног сектора, који већином финансира производњу готово свих садржаја тзв. елитне културе. У Америци, као једној од најмоћнијих држава на планети, која је заједно са Британијом много уложила у свој културни империјализам, културу финансира држава приватни сектор. Америчка теоретичарка културе Дајана Крејн (Diana Crain) разликује две врсте културе: културу коју производе националне културне индустрије и културу која настаје у оквиру урбаних поткултура, укључујући ту и различите уметничке светове и етничке поткултуре.[514] Ово је битно због тога што се амерички културни модел процесом глобализације и америчком економском надмоћи снажно преноси на многа друга друштва, укључујући и српско. У Србији приватне културне индустрије су тек у повоју, док су уметничке поткултуре тешко маргинализоване, а многе етничке поткултуре – нпр. ромска као најбројнија се налази на самој ивици егзистенције. Културне индустрије чини *разнолика група испреплетених сектора у привреди*; то су активности повезане са културом смештене унутар разних сектора приватне индустрије, тј. *музичка индустрија*, *књижевност и тржиште књига*, *уметничко тржиште*, *филмска и телевизијска индустрија* и *извођачка уметност и забављачка уметност*. Стога је веома важно схватити да термин *културне индустрије* не укључује културне активности које пружа јавни сектор нити друге културне институције које су потпомогнуте јавним фондовима.[515]

Генерално, ситуацију на српској културној сцени обележавају сиромашна и девастирана држава која нема средстава за културу; с друге стране не постоји доследна

[514] Crane, D., (1992), *The Production of Culture*, Sage Publ., p.50
[515] Wiesand, A., (2002), "Шта су то културне индустрије и зашто су оне толико интересантне за урбани, регионални и државни развој", у: *Културна политика – развојни аспекти културних индустрија*, Балкан Култ, Београд.

и на дуги рок програмирана политика културног развоја и подршке аутентичним уметничким пројектима. Смернице националног културног развитка којим би се пажња посветила националном културном наслеђу и којима би се одредиле стратегије како уклапања у светске културне токове, тако и заштите националне културе од негативних трендова глобализације, уопште нису постављене.[516] Ако се велика средства улажу у културу, онда се у то уплићу лични интереси, непотизам и корупција, мање него професионални критеријуми.

Из изнетог види се да култура није само погодан оквир за сарадњу и развој, већ је и позадина и плодно тло за различите проблеме у државама у транзицији, који се даље преносе на све системе друштва и државе, па и на КИ. Као таква, култура даје слику света мање или више заједничку за све припаднике културног колективитета. Културне теме се појачавају свесно створеним идеологијама, а управо кроз те идеологије политичке странке и покрети настоје да користе културно наслеђене представе и стереотипе. Тако се култура и идеологија често међусобно потхрањују. С друге стране, и мас-медији на сличан начин црпе своју моћ из представа и стереотипа уврежених у културној матрици и на тај начин их појачавају ради распламсавања најразличитијих типова конфликата, који ни по ком основу не могу бити добри по критичну инфраструктуру. При том, медији могу додатно да погоршају већ лошу ситуацију у свим сегментима друштва.

Природне катастрофе	Македонија	Црна Гора	БиХ	Албанија
Број догађаја	15	4	18	23
Број настрадалих	34	0	16	163
Просечно настрадалих по години	1	---///---	1	5
Број погођених	1,121,805	7,886	403,208	3,877,557
Просечно погођених по години	36,187	254	13,007	125,082
Економска штета (у хиљадама $)	262,163	0	298,000	24,673
Економска штета по години (у хиљадама $)	8,457	0	9,613	796

Табела 6.1. – Преглед природних катастрофа за земље у региону (1980-2010)[517]

У табели 6.1. приказан је преглед природних катастрофа за земље у региону из којег се може закључити да је најмање, по тим питањима, угрожена Црна Гора, како

[516] Кроња, И., (2007), "Култура и политички екстремизам", часопис *Hereticus*, фебруар.
[517] Видети на интернет адреси: *Disaster Statistics*, http://www.preventionweb.net 20.02.2015.

због своје величине и броја становника, тако и због мање изложености природним непогодама. Највише економске штете трпе Албанија, па БиХ и Македонија.

7. КРИЗНИ МЕНАЏМЕНТ У ФУНКЦИЈИ ЗАШТИТЕ КРИТИЧНИХ ИНФРАСТРУКТУРА – ИСКУСТВА ТРАНЗИЦИОНИХ ЗЕМАЉА

7.1. Бугарска

7.1.1. Дефинисање критичне инфраструктуре

Према бугарском Закону о кризном менаџменту "критична инфраструктура представља скуп добара, служби и информационих система, чије би отказивање, спречавање нормалног функционисања или уништење имало озбиљан негативан утицај на јавно здравље, безбедност грађана, животну средину, националну економију или на функционисање државних институција и Владе".[518]

Иако се овом дефиницијом објашњава шта је критична инфраструктура, она не даје неки конкретан критеријум на основу кога би се вршила евалуација *критичности* одређених инфраструктура. Сама дефиниција није довољна ни када се жели утврдити да ли одређено добро, систем или служба могу да се третирају као *критични*. Дефиниција није од велике помоћи ни у процесу идентификовања и анализирања ефективности мера заштите инфраструктуре. Такође, дефиниција се не може искористити ни за утврђивање приоритетних инфраструктура. У суштини, актуелна законска регулатива у Бугарској не пружа одговарајуће основе за квалитетну дистрибуцију јавних и приватних ресурса ради унапређења безбедности критичне инфраструктуре. Стога се улажу напори како би се те основе створиле и како би се установили модели одлучивања приликом државних и приватних улагања у мере безбедности и мере заштите критичне инфраструктуре, а све у сврху тога да се на крају оствари највиши могући ниво безбедности критичне инфраструктуре, уз постојеће ограничене ресурсе.

Бугарска је чланица Европске уније од 2007. године и као таква мора да прати активности и регулативу ЕУ у области заштите критичне инфраструктуре. Према директиви ЕУ "критична инфраструктура дефинише се као скуп добара или одређених елемената инфраструктуре који су критични за функционисање друштва, за нормално функционисање ланаца снабдевања, за здравље и безбедност људи, и за економско и

[518] Дефиниција је донета на основу документа који је издала Комисија ЕУ: Green Paper on a European Programme for Critical Infrastructure Protection (COM 576 final), Brusels, 17. November 2005.

социјално благостање људи".[519] У директиви се даље наводи 11 сектора који се на нивоу ЕУ дефинишу као критични:[520]

1. Енергетика,
2. Нуклеарна индустрија,
3. Информационе и комуникационе технологије,
4. Вода,
5. Храна,
6. Здравство,
7. Финансијске институције,
8. Саобраћај и транспорт,
9. Хемијска индустрија,
10. Истраживање свемира и
11. Научно-истраживачке институције.

У оквиру ЕУ стално је отворена дебата о увођењу нових сектора критичне инфраструктуре, који би тиме постали предмет квалитетније заштите и анализе.[521] Три инфраструктурна сектора сматрају се кандидатима за добијање статуса *критичним*:

1. Отпад и управљање отпадом,
2. Јавне службе за кризни менаџмент,
3. Национални симболи.

На основу ове поделе, која је донета на нивоу Европске уније, могуће је дефинисати и критичне инфраструктурне секторе у Бугарској, како је то наведено у директиви ЕУ.[522]

Снабдевање електричном енергијом и комуникациони системи могу се сматрати круцијалним међу критичним инфраструктурама, с обзиром на то да функционисање свих осталих инфраструктурних сектора зависи управо од њих.

Иако су раније инфраструктурни системи били углавном међусобно раздвојени, након наглог технолошког развоја и промена у динамици тржишта током '70-их година прошлог века, критичне инфраструктуре су у већој мери постале зависне од информационих структура какве су јавне телефонске мреже, интернет, земаљске и

[519] Proposal for a Directive of the Council on the Identification and Designation of European Critical infrastructure, and the Assessment of the Need to Improve their Protection, Comission proposal COM (2006), Decembar 2006.
[520] Ibid
[521] Dunn, M., and Mauer, V., (2006), International Critical Information Infrastructure Protection Handbook, ETH Center for Conflict Studies 2006, vol I Zurich
[522] Nickolov, E., (2005), Critical information infrastructure protection: Analysis, evaluation, and expectations of CII in Bulgaria, INFORMATION & SECURITY. An International Journal, Vol.17, p. 106

сателитске бежичне мреже. Технолошки развој утицао је на аутоматизацију и на увођење компјутера у контролу критичне инфраструктуре, као и на формирање посебне информационе инфраструктуре. Током последње деценије критична информациона инфраструктура се све више истиче као најбитнији (*најкритичнији*) сектор, јер представља основу за управљање и интегрисање свих осталих инфраструктура, а кључан је и за комуникацију, размену података и трговину. Ова симбиоза критичних инфраструктура представља приоритет националне безбедности у Бугарској, јер је информациона инфраструктура основа економског прогреса, а од круцијалног је значаја и за функционисање војске и за функционисање цивилног друштва. Све већа заступљеност информационе инфраструктуре у свим сегментима друштва учинила је информациону инфраструктуру драгоценим добром и врло могућом метом напада. Баш зато велики број земаља развија моделе одбране критичне информационе инфраструктуре, као и моделе одбране од сајбер-напада.[523]

7.1.2 Степен рањивости критичне инфраструктуре

Повећана међузависност критичних инфраструктура и већа операциона комплексност учиниле су критичне инфраструктуре посебно рањивим на природне катастрофе и природне хазарде, људске грешке и техничке проблеме, као и на нове облике сајбер-криминала, тероризам и сајбер-ратове. Сваки од ових догађаја може да доведе до озбиљних последица по критичну инфраструктуру, па чак и до потпуног уништења критичне инфраструктуре. Технолошки развој и кретање ка комплетној аутоматизацији умањили су способност људи да инкорпорирају неопходне безбедносне мере, укључујући детекцију, превенцију и развијање стандарда за умањење негативних ефеката.[524]

[523] Ibid, 107
[524] Tagarev, T., (2006), The Art of Shaping Defense Policy: Scope, Components, Relationships (but no algorithms), The Quarterly Journal 5 no.1, Spring-Summer, p. 16

Природне катастрофе	Бугарска
Број догађаја	34
Број настрадалих	111
Просечно настрадалих по години	4
Број погођених	23,566
Број погођених по години	760
Економска штета (у хиљадама $)	478,104
Економска штета по години (у хиљадама)	15,423

Табела бр. 7.1. – Преглед природних катастрофа у Бугарској (1980-2010)[525]

Извор: Natural Disaster Occurence Reported, http://www.preventionweb.net 23.02.2015.

Велики број бугарских критичних инфраструктура екстремно су осетљиве на природне катастрофе као што су земљотреси, сурови временски услови, поплаве, олује и сл. Чак и кад је елиминисан физички утицај непогода, нагло повећање потребе за критичним инфраструктурама током криза може да доведе до нпр. нестанака струје, што опет представља један облик отказивања критичне инфраструктуре. Слични сценарио је могућ и услед намерних или случајних људских акција. Критична информациона инфраструктура постала је рањива на активности хакера, криминалаца и терориста. Велику опасност по критичну информациону инфраструктуру

[525] Видети интернет страницу*: Disaster Statistics*, http://www.preventionweb.net 20.02.2015.

представљају малициозни програми и кодови (компјутерски вируси, црви, логичке бомбе, тројанци), који за циљ имају модификовање и уништење информационих система или блокирање компјутерских система. Прислушкивање комуникације и крађа података који се размењују путем компјутерских мрежа, као и модификовање нормалних функција компјутерских мрежа и спречавање приступа разним информационим службама често су коришћени видови напада на критичну информациону инфраструктуру. Већина оваквих и сличних напада могу се реализовати путем интернета за свега неколико секунди, а починиоцима је често тешко ући у траг, па је стога неопходна континуирана и непрекидна заштита критичне информационе инфраструктуре.

7.1.3. Процес формирања политике заштите критичне инфраструктуре

Сагласност о томе који се инфраструктурни сектори сматрају критичним представља неопходан предуслов за даљи развој процеса заштите критичних инфраструктура У оквиру процеса формирања политике заштите критичне инфраструктуре у Бугарској постоји низ активности и процена које заједно чине целину. Најбитније активности везане за формирање политике заштите критичне инфраструктуре су:[526]

1. Идентификација главних сектора, подсектора и осталих елемената критичне инфраструктуре и утврђивање *најкритичнијих* међу њима (путем секторске анализе). Критичност се мери на основу очекиваног негативног утицаја који би имало отказивање или спречавање функционисања неког критичног сектора. Што је већи негативни утицај, већа је и *критичност* инфраструктуре. Критеријуми на основу којих се утврђује потенцијални негативни утицај инцидента и отказивања критичне инфраструктуре су:[527]
   a) Негативан утицај на јавност, тј. на становништво (број грађана који су угрожени отказивањем инфраструктуре − очекивани број погинулих, повређених, оболелих, евакуисаних људи),
   b) Економски утицај (утицај који отказивање инфраструктуре има на БДП, други економски губици, деградација производа и служби),
   c) Утицај на животну средину,

[526] Engelbrekt, K., and Förberg, M., (2005), *Managing Crises in Bulgaria*, Elanders Gotab, Stockholm, p. 27-43
[527] Dunn, M., and Mauer, V., (2006), *International Critical Information Infrastructure*, Protection Handbook, ETH Center for Conflict Studiesvol I, Zurich, p. 347

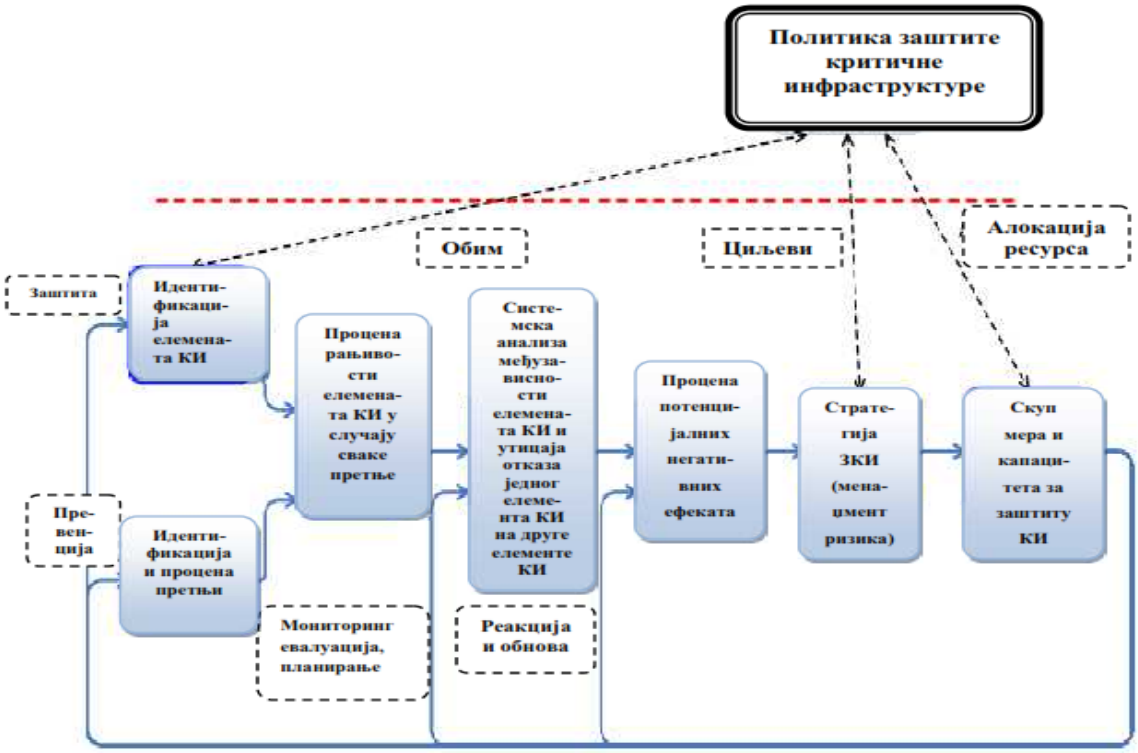
d) Политички и психолошки утицај (нпр. утицај који отказивање инфраструктуре има на смањење поверења које грађани имају у Владу и друге државне институције у погледу решавања оваквих инцидената),

e) Временски аспект (дужина трајања негативног утицаја који изазива отказивање или спречавање нормалног функционисања критичне инфраструктуре – да ли је у питању инцидент чији ефекат се осећа само непосредно након што се догоди, инцидент чији се ефекат осећа дан или два након инцидента, недељу дана или неки дужи временски период).

2. *Идентификација, карактеризација и процена претњи по критичну инфраструктуру*. Претње по критичну инфраструктуру представљају намерни напади, природне катастрофе и људске грешке. У оквиру процене претњи, неопходно је утврдити способност могућих уљеза, нападача, терориста да успешно изврше нападе и извршити процену намера нападача (нападачи могу нпр. да изазову економску (материјалну) штету, да оштете одбрамбене системе или да негативно утичу на друге аспекте националне безбедности).
3. *Процена рањивости главних сектора критичне инфраструктуре у односу на специфичне претње.* Рањивост се може дефинисати као постојање слабости (осетљивих тачака), које могу бити изложене нападима, природним катастрофама и сл. при чему би дошло до отказивања или уништења одређених сегмената критичне инфраструктуре.
4. *Процена међузависности између подсистема и инфраструктура*, уз фокусирање на оним међузависностима које потенцијално доводе до домино ефекта или сличних повезаних отказивања критичних инфраструктурних сектора. Међузависности и повезаност критичних инфраструктура су од суштинског значаја приликом доношења мера заштите критичне инфраструктуре, с обзиром на то да оштећење једног инфраструктурног сектора може последично да има ефекат на један или више других сектора (па чак и да више оштети неке друге секторе, него сектор на који је извршен напад, односно сектор који је први угрожен).
5. *Процена ризика (односно процена последица које се могу очекивати услед одређених напада на критичне инфраструктурне секторе, укључујући све типове негативних утицаја – губитак људских живота, економске губитке итд.)*. Процена ризика односи се на вероватноћу одређених инцидената.

Резултати ових процена се након свега користе за идентификовање и приоритизацију стратегија и мера којима ће се смањити ризици и ублажити претње по критичну инфраструктуру.

6. *Разрада стратегије заштите критичне инфраструктуре*. Ова стратегија за циљ има ублаживање претњи по критичну инфраструктуру, смањење ризика и ублажавање евентуалних последица напада, природних катастрофа и непогода, људских грешака, по критичну инфраструктуру.
7. Формирање скупа мера и капацитета за заштиту критичне инфраструктуре и смањење ризика у оквирима стратегије. [528]



Слика 7.1. – Приказ процеса заштите критичне инфраструктуре у Бугарској[529]

Активности које се предузимају у циљу планирања и анализе заштите критичне инфраструктуре изводе се корак по корак, у оквиру једног јединственог процеса заштите критичне инфраструктуре, који је приказан на слици 7.1.

Формирање политике заштите критичне инфраструктуре (ЗКИ) укључује одлуке о обиму критичних инфраструктура, затим одлуке о циљевима политике ЗКИ, одлуке о

[528] Engelbrekt, K., and Markus Förberg, M., (2005), *Managing Crises in Bulgaria*, Elanders Gotab, Stockholm, p. 27-43

[529] Tagarev, T., Pavlov, N., (2007), *Planning Measures and Capabilities for Protection of Critical Infrastructures – study case of Bulgaria*, p. 42

мерама за идентификовање и приоритизовање критичних инфраструктура и одлуке о алокацији ресурса за ЗКИ.

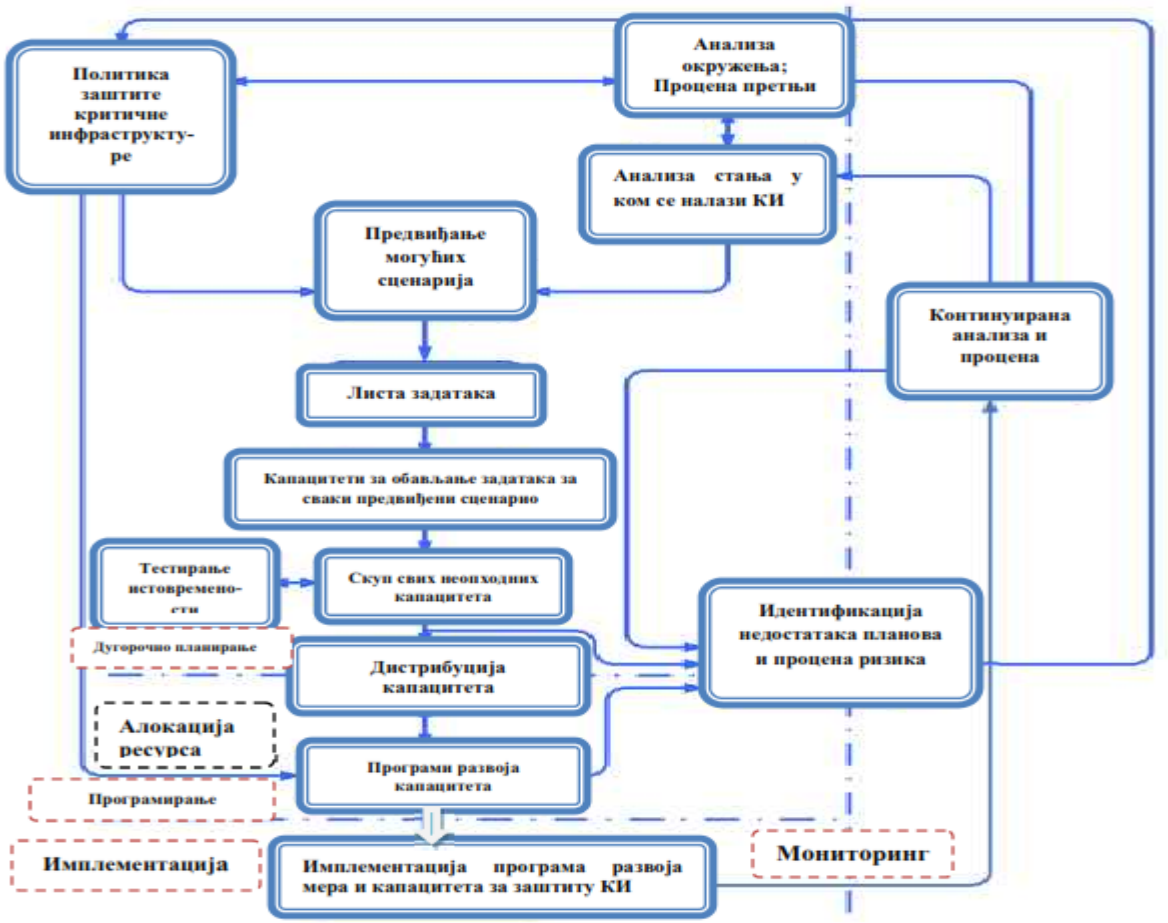
Процес заштите критичне инфраструктуре у Бугарској подразумева имплементацију седам корака приказаних на слици као и повратну информацију о резултатима мера заштите критичне инфраструктуре (дакле представља један интерактиван процес).

Оквири процеса планирања капацитета за заштиту критичне инфраструктуре морају да дефинишу и поставе баланс између четири кључне компоненте: циљева, стратегије и распореда улога између различитих државних и приватних организација, начина имплементирања стратегије и управљања ризицима.[530] Термин *капацитети за заштиту критичне инфраструктуре* се у бугарском Закону о кризном менаџменту дефинише као скуп ресурса којима се постиже мерљиви резултат у области заштите критичне инфраструктуре и остварује одређени квалитет резултата.[531] Сем четири главне компоненте за детаљније описивање процеса планирања заштите критичне инфраструктуре неопходно је дефинисати скуп могућих сценарија, као и скуп задатака који се требају обавити у случају ових сценарија.

Оквир планирања капацитета за заштиту критичне инфраструктуре односи се на различите аспекте процеса планирања, на могућност симултаног деловања различитих елемената који учествују у заштити критичне инфраструктуре, на централизовану природу планирања капацитета и децентрализоване планове и програме финансирања и спровођења мера заштите критичне инфраструкуре, затим на организацију процеса доношења одлука, на имплементацију, надгледање и добијање повратних информација о успешности мера ЗКИ. Слика 7.2. приказује управо описане оквире процеса планирања капацитета за заштиту критичне инфраструктуре.

[530] Bartlett, H., Holman, G., Somes, E. T., (2004), "The Art Strategy and Force Planning", Strategy and Force Planning, Bartlett model, Naval War College Press, Newport, p.17-33

[531] Tagarev, T., (2006), The Art of Shaping Defense Policy: Scope, Components, Relationships (but no algorithms), The Quarterly Journal 5 no.1, Spring-Summer, p. 15-34



Слика 7.2. – Планирање и развој капацитета за заштиту критичне инфраструктуре у Бугарској[532]

7.1.4. Мере заштите критичне информационе инфраструктуре (ЗКИИ) у Бугарској

Заштита критичне информационе инфраструктуре у Бугарској има три стратешка циља:[533]

- Превенцију сајбер-напада на критичне инфраструктуре,
- Смањење националне рањивости на сајбер-нападе,
- Минимизирање штете и времена опоравка од сајбер-напада који се догоде.

Како би се постигли ови циљеви, неопходна је нова стратегија, која укључује следеће елементе:

- Предузимање превентивних мера на свима нивоима,

[532] Tagarev, T., Pavlov, N., (2007), *Planning Measures and Capabilities for Protection of Critical Infrastructures – study case of Bulgaria*, p. 44

[533] Andreas, W., Metzger, J., and Dunn, M., eds., (2004), *International CIIP Handbook* Center for Security Studies at the Swiss Federal Institute of Technology, Zurich.

- Унапређење ране детекције и брзе реакције ради контроле штете и потраге за евентуалним нападачима,
- Лимитирање утицаја различитих напада на КИИ на друштво и државу,
- Брзо враћање угрожених (нападнутих) информационих система на нормалан режим рада.

Претње и рањивости састоје се од физичке, информационе и психолошке компоненте; Стога је неопходан отворени дијалог о новим рањивостима и претњама по КИИ. Такође, неопходно је дефинисање нових физичких, информационих и психолошких заштитних мера.

Спровођење мера заштите КИИ на националном нивоу врши се кроз пет националних приоритета Бугарске у области заштите КИИ, који се могу дефинисати на следећи начин:[534]

- Формирање националног система за сајбер-безбедност,
- Развој националног програма за редуковање претњи и рањивости у области сајбер-безбедности,
- Стварање и јачање свести грађана Бугарске о важности кибер-безбедности и о мерама за очување сајбер-безбедности, као и формирање програма обуке у овој области,
- Обезбеђивање система државне управе,
- Јачање националне безбедности и међународне сарадње у области сајбер-безбедности.

Проблеми заштите КИИ у Бугарској са којима се Бугарска суочава у области заштите КИИ су:[535]

- Недостатак законских оквира – овај проблем у великој мери успорава и отежава сваки судски процес везан за сајбер-криминал,
- Недостатак обученог особља,
- Недостатак неопходних техничких алата за одговор на сајбер-нападе,
- Недостатак поузданих система за интеракцију са специјалним организацијама из других земаља,
- Мањак националних организација на државном нивоу које би се бавиле координацијом активности у области заштите КИИ,

[534] Ibid
[535] Nickolov, E., (2005), Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations – study case of Bulgaria, INFORMATION & SECURITY. An International Journal, Vol.17, p. 116-117

- Недостаци у националној стратегији везани за непостојање одредби на основу којих би се одређени финансијски ресурси државе усмеравали на развој организација које ће се бавити заштитом КИИ и координацијом активности у области заштите КИИ,
- Недостатак националног акционог плана на основу којег би се национални фондови повезивали са међународним пројектима на регионалном нивоу, на основу којих би се развијале организације које ће се бавити заштитом КИИ и координацијом активности у области заштите КИИ.

Бугарска ради на развоју законских оквира којима би се владине агенције овластиле да читају електронску пошту, пресрећу бежичну комуникацију (позиве и интернет комуникацију), да надзиру употребу рачунара, итд. Посебним законом су незаконитим проглашени чинови намерног неовлашћеног упада у рачунаре и намерно изазивање штете на другим рачунарима слањем малициозних програма путем интернета. Пре три године је и хаковање законом означено као кривично дело и уведен је појам сајбер-тероризма.

У области заштите КИИ Бугарска ради на неколико пројеката и унапређује заштиту своје КИИ у неколико сегмената: [536]

1. Ради се на остварењу ефикасније сарадње између судских органа и специјалних служби за ЗКИИ балканских и европских земаља, и уопштено на развоју међународне сарадње,
2. Бугарска ради на унапређењу националне стратегије за превенцију и борбу против сајбер-криминала,
3. Ради се на развоју националне службе за борбу против сајбер-криминала и међународну сарадњу приликом транснационалних сајбер-инцидената,
4. Проширује се међународна сарадња у области правосудне помоћи у борби против сајбер-криминала,
5. Доносе се специјални закони из области телекомуникација и компјутерских мрежа у складу са тренутним међународним стандардима и са Конвенцијом Европске комисије о сајбер-криминалу.

Препорука бугарских стручњака у области заштите КИИ је и да се оформи једна контакт служба у коју би долазиле све релевантне информације везане за заштиту КИИ и за актуелне кризе, и која би након пријема те информације прослеђивала свим

[536] Tagarev, T., Pavlov, N., (2007), Planning Measures and Capabilities for Protection of Critical Infrastructures in Bulgaria, p. 46

релевантним службама. Тиме би се успоставила квалитетнија координација активности свих учесника у заштити критичне информационе инфраструктуре, а као последица боље координације, олакшало би се идентификовање извора напада, као и формирање и спровођење решења за одбрану од напада или за опоравак од сајбер-напада.

7.1.5. Приватно-јавна партнерства у области заштите критичне информационе инфраструктуре

Услед све већег броја приватних учесника који поседују или су корисници критичне инфраструктуре, формирање приватно-јавних партнерстава важан је део процеса заштите критичне информационе инфраструктуре.[537] Ова партнерства у Бугарској имају неколико задатака:[538]

- Баве се проблемима и претњама по националну критичну информациону инфраструктуру,
- Информишу и указују произвођачима хардвера и софтвера на значај безбедности и заштите њихових производа,
- Задужена су за брзу и ефикасну реакцију у случају било каквог инцидента повезаног са функционисањем критичних система,
- Задужена су за формирање система за формалну и неформалну размену информација о криминалним активностима повезаним са коришћењем рачунара и о сајбер-тероризму.

Како би се ови задаци обавили неопходна је сарадња приватног сектора са органима полиције, уз активну размену података о претњама, рањивостима, начинима спречавања напада и успешним оперативним моделима сајбер-безбедности. Како би се унапредила заштита КИИ, приватни сектор мора да информише државне органе о инцидентима и штети који се догоде у оквиру било које компаније, чак и кад изношење тих информација може додатно да нашкоди самој компанији. Сматра се да само потпуно отворена сарадња, без прећуткивања информација, нити од стране државе нити од стране приватног сектора, може да за резултат има ефикаснију заштиту критичне информационе инфраструктуре.

С друге стране, размена информација има неке негативне стране и кад је у питању јавни (државни) интерес и кад је у питању приватни интерес. Размена

[537] US Government, U.S., The National Strategy to Secure Cyberspace, February 2003.
[538] Nickolov, E., (2005), Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations – study case of Bulgaria, INFORMATION & SECURITY. An International Journal, Vol.17, p. 111-112

информације може да доведе до промене цена, до несхватљивих тржишних ограничења или до систематске дискриминације неких корисника. Такође, размена података може да изазове повећани страх од нарушавања приватности, али и да разоткрије добро чуване корпоративне тајне или да открије слабости и рањиве тачке. Трговци и други учесници у малопродаји су често забринути да би обелодањивање било ког проблема везаног за безбедност он-лајн трансакција (нпр. уколико хакери дођу у посед бројева кредитних картица) могло да пољуља поверење јавности у трговину путем интернета, што би нанело штету њиховом пословању. Такође, обелодањивање података о нападима на информационе системе провајдера разних услуга из области телекомуникација може да доведе до губитка корисника, а самим тим и смањења прихода.[539] Уколико би се у контексту отворене размене информација нпр. издала листа најугроженијих и најрањивијих тачака критичне информационе инфраструктуре, с једне стране урадила би се добра ствар, пошто би администратори система и корисници рачунара били информисанији о претњама, али истовремено би се на тај начин и хакерима пружила иста информација и практично би им се тиме помогло у извршењу напада.[540]

Стога је за формирање квалитетне сарадње и у Бугарској, као уосталом и било где другде у свету, апсолутно неопходно поверење и поштовање међу свим странама које учествују. Поверење се гради кроз договор о томе како ће се располагати информацијама које компаније износе, како ће се вршити заштита тих информација и којим ће се све учесницима те информације прослеђивати. Такође, за изградњу поверења битно је и формирање законских регулатива, којима ће се прописати правила сарадње приватног и јавног сектора.

7.1.6. Методолошки и организациони изазови заштите критичне инфраструктуре

Бугарски стручњаци[541] из области заштите критичне инфраструктуре очекују да ће се у блиској будућности у Бугарској и званично (на нивоу државе и Владе) усвојити методологија за процену критичности инфраструктуре, планирање заштитних мера и

[539] Donzelli, P., Goal-Driven, A., and Agent-Based Requirements Engineering Framework, (2004), *Requirements Engineering* 9, no. 1, Springer-Verlag London, February, p. 16-39

[540] Donzelli, P., and Setola, R., (2001), Putting the Customer at the Center of the IT System A Case Study, Euro-Web 2001 Conference – The Web in the Public Administration, Pisa, Italy, 18-20 December, p. 14

[541] Најпознатији признати бугарски стручњаци у области заштите критичне инфраструктуре су између осталих Јуџин Николов, Тодор Тагарев и Николај Павлов.

капацитета и алокацију приватних и јавних ресурса,[542] а које ће се заснивати на управљању ризицима.

Стратегија заштите критичних инфраструктура ће бити имплементирана кроз низ мера и капацитета за заштиту критичне инфраструктуре. Ипак, није препоручљиво формирање планова и програма заштите критичне инфраструктуре независно од других безбедносних захтева. Пошто одређени број организација које учествују у заштити критичне инфраструктуре има много шири спектар активности од рада на заштити критичних инфраструктура, препорука стручњака за ЗКИ у Бугарској је да се процес планирања ЗКИ посматра у контексту "заштите становништва и критичних инфраструктура од терористичких напада, природних катастрофа, индустријских несрећа и катастрофа".[543]

Могуће је, али није препоручљиво да се користи шири контекст планирања ЗКИ, какав је нпр. *планирање капацитета за ЗКИ у контексту "заштите становништва и националне економије од терористичких напада, природних катастрофа, индустријских несрећа и катастрофа*"[544] или пак *планирање капацитета за ЗКИ у контексту планирања капацитета за сектор националне безбедности (која у обзир мора да узме и захтеве које постављају ЕУ и НАТО).*

Са аналитичког становишта, у области даљег развоја и имплементације метода, мера и анализе заштите критичне инфраструктуре, препоручују се следеће активности и ставови:[545]

1. Препоручује се посматрање критичне инфраструктуре као комплексног прилагодљивог система. Све типичне карактеристике оваквих система морају се узети у обзир, укључујући и свеприсутну неизвесност и прилично ограничену могућност предвиђања инцидената која постоји у оквиру оваквих система.

[542] У пролеће 2007. године бугарско Министарство за државну политику везану за катастрофе и несреће започело је пројекат, чији један део представља развој методологије за процену критичности инфраструктуре на општинском нивоу.
[543] Tagarev, T., Pavlov, N., (2007), Planning Measures and Capabilities for Protection of Critical Infrastructures, p. 45
[544] Актуелни званичници државних органа који се баве критичном инфраструктуром и заштитом исте у Бугарској највише су наклоњени оваквом приступу заштити критичне инфраструктуре. О томе сведочи и документ о концепту заштите током природних катастрофа и индустријских несрећа који је донело бугарско Министарство за државну политику везану за катастрофе и несреће. Документ је доступан на бугарском језику на сајту: www.mdpba.government.bg 10.02.2013
[545] Tagarev, T., Pavlov, N., (2007), Planning Measures and Capabilities for Protection of Critical Infrastructures, p. 55

2. Препоручују се различите методологије за проучавање комплексног прилагодљивог система критичне инфраструктуре.
3. Препоручује се да се имплементација ових модела обавља упоредо са експертским проценама, везаним за дефинисање циљева ЗКИ, како би се као резултат генерисала алтернативна решења у процесу заштите критичне инфраструктуре.
4. У одређеним случајевима, како стручњаци процењују, потребно је размотрити одлуке које доносе учесници у компјутерским обукама и симулацијама.
5. Препоручује се и широк спектар метода и приступа којима би се обезбедило обављање одређених задатака везаних за заштиту критичних инфраструктура.

Са организационог становишта, кључни изазов ЗКИ у Бугарској је превазилажење организационих оквира. У било којој другој ситуацији, државна администрација не би могла да добије *целокупну слику*, тј. да изврши процену међузависности између критичних инфраструктура и утицаја инцидената на критичну инфраструктуру. Такође, не би била могућа ни економски ефикасна дистрибуција капацитета за заштиту критичне инфраструктуре међу организацијама које учествују у ЗКИ. Из ових разлога је у Бугарској формирано и Министарство за државну политику везану за катастрофе и несреће.

Зависност пословања, државне управе и друштвених служби од критичних инфраструктурних сектора утиче на настанак рањивости, што може да доведе до значајних губитака у случајевима терористичких и криминалних напада, људских грешака и екстремних природних непогода. Држава и друштво спремни су да плате цену лимитирања рањивости, а самим тим и цену лимитирања губитака, али би притом требало да буду свесни како и колико треба инвестирати у одређене мере и капацитете за заштиту критичне инфраструктуре.[546] То значи да процес заштите критичне инфраструктуре затева *транспарентност*, односно јасна правила и тачно дефинисане одлуке о томе која се инфраструктура сматра критичном, шта би се могло урадити у погледу заштите критичне инфраструктуре, које мере треба имплементирати уз постојеће ресурсе и који ефекат те мере заштите критичне инфраструктуре имају.

[546] Dunn, M., and Mauer, V., (2006), International Critical Information Infrastructure Protection Handbook, ETH Center for Conflict Studies, vol I, Zurich, p. 349

Како би се обезбедила транспарентност, неопходно је утврдити одговарајући методолошки приступ. Уз све методолошке, процедуралне и аналитичке изазове који постоје, главну препреку за ефикасно спровођење мера заштите критичне инфраструктуре представља културолошки модел цетрализованог доношења одлука у оквиру стриктне хијерархије која лимитира могућност координације активности па и комуникације између различитих агенција и организација, као и приватног и јавног сектора.[547]

Као релативно нови концепт за који се у све већој мери интересује читава Европска унија, заштита критичне инфраструктуре има шансу да сломи организационе оквире, унапреди транспарентност доношења одлука и одговорност централне и локалних управа у Бугарској, која је тек од скоро члан ЕУ. Такође, квалитетно спровођење мера ЗКИ требало би да увећа и ниво координације међу владиним организацијама, безбедносним службама, власницима и оператерима критичне инфраструктуре.

7.2. Словенија

Словенија је у погледу доношења и спровођења политике заштите критичне инфраструктуре, добра референтна тачка за поређење са Србијом и за извлачење поука и искустава, која би се касније применила на примеру Србије. Словенија је након стицања независности успела релативно брзо да уђе у састав ЕУ, а уласком у ЕУ обавезана је и да своје законске регулативе усклађује са европским регулативама на свим пољима, па и на пољу ЗКИ. Сем усвајања законске регулативе, Словенија је доста урадила и у области спровођења закона у пракси, што опет може да се користи и за предлагање одређених мера и начина спровођења тих мера у Србији. Из тих разлога ће заштита критичне инфраструктуре у Словенији бити мало детаљније описана.

Територија Словеније[548] подељена је на 58 административних јединица ради лакшег управљања. Ради квалитетнијег функционисања система одбране основано је 8 регионалних канцеларија Министарства одбране, а ради бољег контролисања могућих катастрофа (било ког порекла) основано је 13 регионалних канцеларија, које контролише и координише Управа (дирекција) за цивилну заштиту и помоћ приликом катастрофа.

[547] Ibid
[548] Влада Републике Словеније, http://www.vlada.si/en/about_slovenia/ 10.02.2013

На локалном нивоу, Словенија је подељена на 192 општине. Општине су одговорне за локална питања и проблеме. Градоначелник се налази на челу сваке општинске управе.

7.2.1. Критични инфраструктурни сектори

На основу међусекторске анализе инфраструктуре може се формирати списак критичних инфраструктура Словеније[549] и утврдити који се сектори могу сматрати критичнијим у односу на друге.[550] Нумеричке вредности (прагови за категорисање инфраструктуре) за неке од критеријума одређени су конкретно за случај Словеније. Испитивање критичне инфраструктуре Словеније[551] спроведено је уз учешће око 200 представника релевантних организација. Испитивање је обавила Владина координациона група за ЗКИ заједно са свим релевантним министарствима. Сектори и подсектори КИ идентификовани су на основу компаративне анализе свих битних инфраструктурних сектора других држава ЕУ и поређења те инфраструктуре са секторима и подсекторима у Словенији. Селекција релевантних организација које су се разматрале у контексту идентификовања критичних инфраструктура, обављена је уз консултацију са релевантним министарствима и уз примену критеријума међусекторске анализе. Анализом је идентификовано 9 критичних инфраструктурних сектора, идентификоване су њихове функције и задаци, а формиран је списак министарстава, организација, агенција и других државних и приватних удружења које су одговорне за функционисање и заштиту критичне инфраструктуре.

[549] Словенија се иначе сматра развијеном земљом са индексом развоја друштва од 0.923, што је ставља на 26. место од 179 земаља света. БДП по глави становника за 2008. годину износио је више до 17.000 евра, што јој обезбеђује 30. место у свету. Кључни инфраструктурни сектори су сразмерно развијени. Словенија као држава, као и њена инфраструктура, лакши су за истраживање него веће земље због мале површине (око 20.000 km^2), малог броја становника (нешто изнад 2 милиона људи). Последично држава има и мањи обим инфраструктуре и мање релевантних учесника у процесу заштите критичне инфраструктуре.

[550] Истраживање критичне инфраструктуре Словеније је изнето у раду два словеначка аутора: Prezelj, I., and Kustec Lipicer, S., (2010), Publicand Policy Management of Critcal Infrastructure: Lessons from Integral Nations Cross-Sectoral Scanningin Slovenia, IRSPM Conference, Panel: Risk and Crisis Management in the Public Sector, Berne, pp. 7-17

[551] Ibid

Сектор	Подсектори и њихове активности	Одговорна (прегледана/испитана) тела
1. Енергетика	1. Производња, прерада, складиштење и дистрибуција нафте (Нафта) 2. Производња, складиштење и дистрибуција гаса (Гас) 3. Производња и дистрибуција електричне енергије (Струја)	Министарство за економију, Агенција за робну берзу Словеније, Агенција за трговину нафтом, "Petrol" і "Istrabenz" нафтне компаније, "Геоплин" плиноводи, Плинара Марибор и "Интерна" гасне компаније, Рафинерија "Група НАФТА" Лендава, Словенске електране, ГЕН Енергија, нуклеарно постројење Кршко, ЕЛЕС – Електро Словенија, главне термоелектране у Словенији
2. Нуклеарна индустрија	1. Производња, обрада и складиштење нуклеарних материјала (Нуклеарни материјал)	Управа за нуклеарну безбедност РС, Нуклеарно постројење Кршко, Институт "Јозеф Стефан" – Центар за реакторе, ГЕН Енергија
3. Информациона и комуникациона технологија	1. ИКТ софтвер 2. ИКТ комуникације и хардвер	Агенција за поште и телекомуникације РС, РТВ Словеније, Телеком Словенија, ТУС Телеком, ДАРС центар за саобраћај и комуникације, Железнице Словеније
4. Вода	1. Снабдевање водом за пиће (Вода за пиће) 2. Контрола квалитета воде (Квалитет воде) 3. Контрола залиха воде (Залихе воде)	Министарство за екологију и просторно планирање, неколико највећих агенција за снабдевање водом, Инспекторат за екологију и просторно планирање, Државни здравствени завод, Министарство економије, Агенција за заштиту околине РС, Институт за воду РС, "Сава" Електране – Љубљана, "Драва" Електране – Марибор
5. Здравство	1. Медицинске службе хитне помоћи 2. Медицинска нега	Министарство здравља, Институт за трансфузију РС, Агенција за медицинске производе и опрему Словеније, Државни здравствени завод, Универзитетски медицински центар Љубљана, неколико највећих словенских болница, Удружење

Сектор	Подсектори и њихове активности	Одговорна (прегледана/испитана) тела
	3. Лекови, серуми, вакцине, биолабораторије и биоагенти	самосталних лекара и стоматолога Републике Словеније
7. Финансије	1. Финансијска средства (Финансије)	Министарство финансија, Пореска управа, Народна банка Словеније, Удружење банака Словеније, НЛБ – главна словенска банка
8. Саобраћај	1. Друмски саобраћај 2. Железнички саобраћај 3. Ваздушни саобраћај 4. Водени саобраћај	Министарство саобраћаја, Дирекција за железнице, Дирекција за поморски саобраћај, Дирекција за цивилно ваздухопловство, Дирекција за железнице и жичаре, Железнице РС, Управа за поморски саобраћај Словеније, ДАРС – Управа за ауто-путеве Републике Словеније, Контрола летова Републике Словеније, Аеродром Љубљана, Аеродром Марибор, Аеродром Порторож
9. Хемијска индустрија	1. Производња, складиштење и обрада хемијских супстанци (Хемијска индустрија)	Министарство економије, "Белинка" Петрохемија, КИК Камник група, Рафинеријска група НАФТА Лендава

Табела бр. 7.2. – Преглед инфраструктурних сектора, функција инфраструктурних сектора и подсектора и институција одговорних за функционисање и заштиту критичне инфраструктуре у Словенији[552]

Међу организацијама битним за функционисање система критичних инфраструктура и за њихову заштиту налазе се и сви битни државни органи и институције: Министарство унутрашњих послова Словеније, Министарство одбране (Дирекција за цивилну заштиту и помоћ приликом катастрофа и Дирекција цивилне одбране), као и словеначка обавештајна служба (SOVA).

[552] Prezelj, I., and Kustec Lipicer, S., (2010), Public and Policy Management of Critcal Infrastructure: Lessons from Integral Nations Cross-Sectoral Scanningin Slovenia, IRSPM Conference, Panel: *Risk and Crisis Management in the Public Sector*, Berne, p. 6

Уочени сектори и подсектори критичне инфраструктуре разликују се по структурној сложености и по могућности подсекторског прилагођавања капацитета. У неким секторима прилагођавање капацитета у смислу замене неких система који престану са функционисањем другим системима је могуће у одређеној мери (нпр. у сектору саобраћаја и транспорта када дође до проблема у железничком и ваздушном саобраћају могуће је прилагођавање појачаним коришћењем друмског саобраћаја), док у другим секторима овакво прилагођавање није могуће (нпр. подсектор контроле квалитета воде не може да замени подсектор за снабдевање водом у случају његовог отказивања, као што ни прекид функционисања хитних служби медицинске помоћи и медицинске неге не може да се надокнади радом сектора медицинске индустрије).

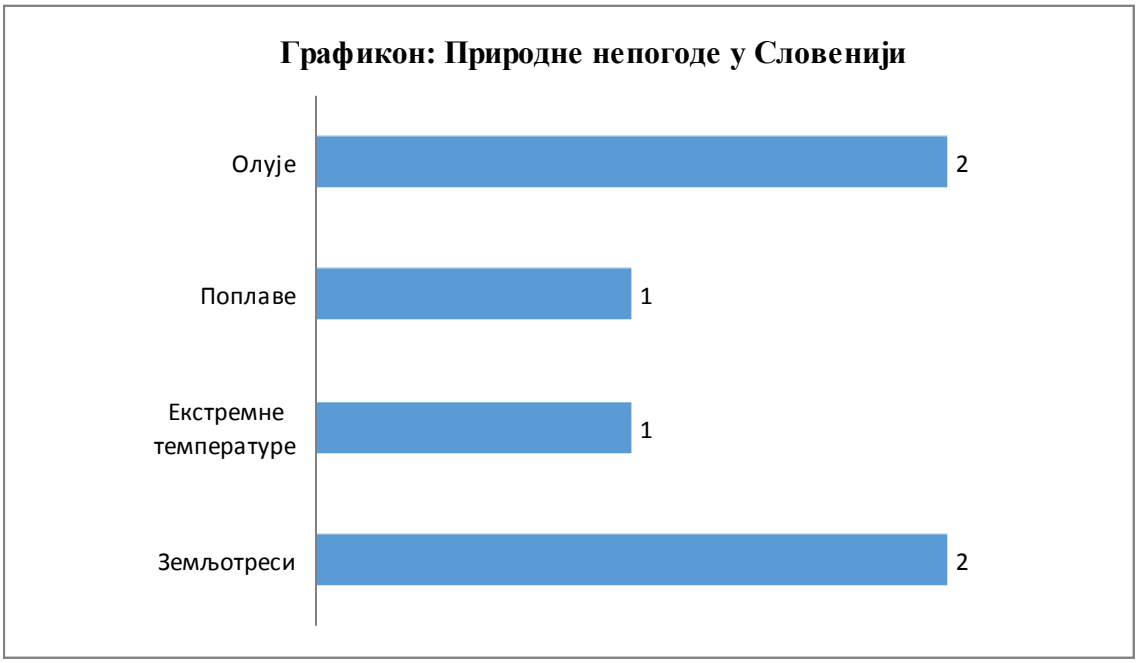
У Словенији постоји интерес и иницијатива за увођењем још неких критичних инфраструктурних сектора као што су затворска инфраструктура (чије увођење предлаже Министарство правде) и инфраструктура културног наслеђа (чије увођење предлаже Министарство културе).

Анализа свих критичних сектора у Словенији јасно указује на њихову велику повезаност. Ово је посебно приметно кад су у питању сектори саобраћаја и транспорта, енергетике, информационих и комуникационих технологија, финансија, воде и хране.

Природне катастрофе	**Словенија**
Број догађаја	6
Број настрадалих	296
Просечно настрадалих по години	10
Број погођених	2,355
Просечно погођених по години	76
Економска штета (у хиљадама $)	487,000
Економска штета по години (у хиљадама $)	15,710

Табела бр. 7.3. – Преглед природних катастрофа у Словенији (1980-2010)[553]

[553] Видети на интернет страници*: Disaster Statistics*, http://www.preventionweb.net 20.02.2015.



Извор: Natural Disaster Occurence Reported, http://www.preventionweb.net 23.02.2015.

Перцепција претњи, рањивости и ризика по критичну инфраструктуру од стране менаџера, власника и оператера КИ указује на то да су неке уочене претње и ризици заједнички за све секторе, а неке су специфичне и везане за конкретне секторе. Заједнички перципирани ризици и претње су: [554]

- Природне катастрофе (поплаве, земљотреси, велики одрони земље),
- Намерни напади на КИ (криминална дела, напади на ИКТ сектор, саботаже итд),
- Ненамерно угрожавања инфраструктуре (технички кварови на КИ, људске грешке приликом коришћења КИ).

Неки подсектори у Словенији имају проблема са усвајањем норми везаних за безбедност. У тим случајевима неопходна је и обука одговорних лица најпре о томе шта све представља претњу и рањивост критичне инфраструктуре, а затим и о мерама заштите КИ. У оквиру великог броја сектора и подсектора КИ у Словенији, претња коју представља тероризам, а која би требало да буде главна покретачка снага која ће утицати на формирање мера заштите КИ доживљава се више као теоретска претња,

[554] The Civil Defense Doctrine of the Republic of Slovenia, 2002, p. 9–13

него као реална.[555] Општи утисак је да се много више пажње *реалној* заштити од терористичких напада поклања у оквиру сектора који су у већој мери међународно оријентисани (нпр. у оквиру сектора ваздушног и поморског саобраћаја). Ови сектори могу лакше да се *отргну* од општег схватања терористичких претњи као теоретских претњи које се у стварности највероватније неће остварити. Разлог је пре свега тај што ове секторе на озбиљније схватање терористичких претњи обавезују међународни безбедносни стандарди. Неки други сектори који нису у тој мери међународно оријентисани, попут сектора вода, не баве се довољно заштитом и превенцијом терористичких напада.

Проблеми са којима се суочавају неки од сектора критичне инфраструктуре су и мањак обучених људи (посебно у ИКТ сектору и у сектору здравства), недовршени пројекти у сектору финансија који могу да доведу до великих проблема у функционисању читавог друштва, погрешна политика снабдевања водом и са њом повезани законски проблеми, преоптерећеност инфраструктуре у ИКТ сектору, сектору финансија и сектору енергетике, што опет може да доведе до колапса мрежа снабдевања различитим услугама. Велики проблем представља и зависност између сектора − зависност ИКТ сектора од електричне струје, зависност сектора производње хране од сектора за снабдевање водом, зависност здравства од енергетике и саобраћајне инфраструктуре, зависност финансија од ИКТ сектора.[556]

Такође, битно је истаћи да један исти узрок може да доведе до поремећаја у функционисању више инфраструктурних сектора.

Предвиђена штета по друштво коју би изазвало отказивање инфраструктурног сектора резултат је процене значаја сваког сектора критичне инфраструктуре за друштво и утврђивање индекса критичности[557] сваке инфраструктуре. Проценом се дошло до закључка да су најкритичнији сектори и подсектори у Словенији производња и дистрибуција хране (са индексом критичности 15 и

[555] Prezelj, I., and Kustec Lipicer, S., (2010), Public and Policy Management of Critcal Infrastructure: Lessons from Integral Nations Cross-Sectoral Scanningin Slovenia, IRSPM Conference, Panel: *Risk and Crisis Management in the Public Sector*, Berne, p. 11-13

[556] Ibid

[557] Индекс критичности рефлектује ниво критичности сваког сектора и подсектора. Индекс критичности настаје на основу процене збирне штете коју би имао евентуални прекид функционисања КИ по становништво, по економију, по јавност и по животну средину. Другим речима, индекс критичности показатељ је значаја критичне инфраструктуре, тј. значаја сваког појединачног сектора. Вредност индекса критичности креће се од 0 до 16 (0 – инфраструктура не утиче на нормално функционисање друштва, 16 – инфраструктура је апсолутно неопходна за нормално функционисање друштва). Како би се омогућило поређење критичности инфраструктура рачуна се нормализовани индекс критичности. Овај индекс рефлектује релативну критичност одређеног инфраструктурног сектора (критичност у односу на друге секторе) и креће се у опсегу од 0 до 100% тј. 0−1

нормализованим индексом критичности 0,93), затим производња лекова и медикамената (са индексом критичности 13 и нормализованим индексом критичности 0,81), резерве воде (са индексом критичности 12 и нормализованим индексом критичности 0,75), здравствена нега (са индексом критичности 12 и нормализованим индексом критичности 0,75) и служба хитне помоћи и предмедицинске неге (са индексом критичности 11 и нормализованим индексом критичности 0,68). Најмање критични сектори и подсектори су три подсектора везана за саобраћај и транспорт: ваздушни саобраћај и транспорт (са индексом критичности 4 и нормализованим индексом критичности 0,25), водни (поморски) саобраћај и транспорт (са индексом критичности 5 и нормализованим индексом критичности 0,31) и железнички саобраћај и транспорт (са индексом критичности 6 и нормализованим индексом критичности 0,37). Овим истраживањем такође је утврђено да би евентуални престанак или отежано функционисање КИ понајвише утицало на поверење грађана и на економију државе, док би понајмање утицало на животну средину.

Временски период који протекне од тренутка кад дође до престанка функционисања инфраструктуре до тренутка избијања кризе није за све КИ исти. Престанак нормалног функционисања неких критичних инфраструктура може моментално да изазове значајне негативне ефекте по друштво, док с друге стране негативни ефекти престанка функционисања неких других КИ настају са извесним закашњењем. Подсектори чије отказивање скоро моментално изазива негативне ефекте по друштво су струја, гас, служба хитне медицинске помоћи и предмедицинска нега, сектор производње лекова и медикамената, друмски саобраћај и транспорт, надзор водних резерви и нуклеарна индустрија. С друге стране, постоје и сектори и подсектори критичне инфраструктуре чије отказивање (прекид функционисања) не изазива моменталне последице већ их изазива са закашњењем које може да буде веће и од недељу дана. Такви су нпр. сектори водног (поморског) саобраћаја и транспорта, ваздушног саобраћаја и транспорта, затим хемијска индустрија и подсектор везан за контролу квалитета вода. Прекид нормалног функционисања сектора за дистрибуцију хране такође не би моментално угрозио становништво, због постојања резерви у радњама. Недостатак хлеба и млека би сигурно били први прехрамбени производи чија би се несташица приметила. Последице прекида и неправилног (отежаног) функционисања финансијског сектора озбиљно би оштетило друштво након неколико дана услед релативно флексибилних рокова плаћања и новчаних резерви.

Прекограничне последице престанка функционисања инфраструктуре могу бити значајне, јер словеначка КИ представља истовремено и саставни део мреже европских критичних инфраструктура. У оквиру словеначке критичне инфраструктуре постоје сектори коју су више и они који су мање међународно оријентисани. Више међународно оријентисани сектори су они који не би могли да функционишу да нису део међународне инфраструктуре. То значи да ови инфраструктурни сектори директно зависе од међународнх инфраструктура, сектора и служби, али и да утичу на те исте међународне инфраструктурне секторе и службе. Инфраструктурни сектори који су у највећој мери међународно оријентисани у случају Словеније су саобраћај и транспорт, информационе и комуникационе технологије и енергетика. Словенија се налази на раскршћу неколико важних коридора друмског, железничког, водног и ваздушног саобраћаја, а словеначка инфраструктура информационих и комуникационих технологија и енергетике такође је саставни део европске инфраструктуре. У случају ових сектора државне границе немају велики значај (тако нпр. државне границе немају велики значај за контролу летења или за слање електронске поште, као ни за ширење нуклеарне радијације).

С обзиром на то да Словенија има малу инфраструктуру у односу на остале европске државе, као и у односу на Европску унију, она углавном зависи од страних инфраструктура, а мање сама утиче стабилношћу своје инфраструктуре на стабилност и нормално функционисање других земаља. Ово се јасно може увидети, како неки експерти из домена финансија тврде, на примеру евентуалног колапса финансијског система Словеније. Наиме, колапс финансијског система Словеније имао би мањи, скоро занемарљив ефекат на европски финансијски систем. Сви системи обављања међународних финансијских трансакција лоцирани су ван Словеније.

Географске области у којима су концетрисани критични објекти могу се разврстати у неколико категорија:[558]

- Критични објекти,
- Критичне везе (повезаности),
- Критична укрштања инфраструктура и
- Критични процеси који се дешавају у критичним објектима или у њиховој близини.

[558] Prezelj, I., and Kustec Lipicer, S., (2010), Public and Policy Management of Critcal Infrastructure: Lessons from Integral Nations Cross-Sectoral Scanningin Slovenia, IRSPM Conference, Panel: Risk and Crisis Management in the Public Sector, Berne, p. 15

Традиционално се објекти критичне инфраструктуре посматрају као материјална категорија (физички објекти). Међутим, сем њих постоје још две категорије које се не могу сматрати материјалним: ваздушне и пловне руте. Ваздушна и поморска навигација заснивају се на коришћењу претходно утврђених рута (које представљају везе узмеђу материјалних инфраструктурних објеката, као што су аеродроми и луке). И поред тога што руте не представљају физичке објекте, опште је прихваћен став да се посматрају као критични објекти, како у оквиру својих сектора тако у оквиру читавог друштва. Руте се сматрају критичним објектима јер њихово ометање може да доведе до проблема, па и криза у ваздушном и водном саобраћају.

Објекти критичне инфраструктуре асиметрично су дистрибуирани у оквиру Словеније. Критичне инфраструктуре у већој мери су смештене у урбаним срединама. Посебно су критичне мулти-инфраструктуралне области тј. области у којима је лоциран већи број различитих типова инфраструктура. Ометање нормалног функционисања једног типа инфраструктуре у оваквим областима брзо би посредно утицало и на функционисање других инфраструктура у тој области. У Словенији постоје два примера таквих области: главни национални аеродром и национална лука. У оквиру главног националног аеродрома смештен је већи број инфраструктура као што су инфраструктура ваздушног саобраћаја, мреже информационих и комуникационих технологија, банке, мењачнице, агенције за шпедицију, пошта, нафтна компанија, војна инфраструктура, инфраструктура спасилачких служби, разни малопродајни објекти. Слична инфраструктура налази се и склопу главне националне луке. Критична инфраструктура је највећим делом смештена у главном граду – Љубљани. Словенија је у извесној мери децентрализована држава у којој осим главног града (у коме живи око 13% становништва Словеније) одређени значај имају и други градови и индустријске зоне. Ипак, главна интернет чворишта, финансијске институције и објекти хемијске индустрије лоцирани су у главном граду. Љубљана се налази на споју два велика европска саобраћајна коридора (Коридор V и коридор X) поред којих је такође смештен велики део инфраструктуре. Највећи део словеначке финансијске инфраструктуре лоциран је у градском центру, а у ширем подручју Љубљане (Љубљанска долина) налази се највећи део критичних објеката словеначке хемијске идустрије. Такође, много других типова инфраструктуре смештено је у главном граду (инфраструктура друмског и железничког саобраћаја, делови система за дистрибуцију воде и хране и инфраструктура службе хитне помоћи и медицинске неге.

С друге стране, велики делови инфраструктуре сектора вода, хране и енергетике смештене су изван урбаних зона (нпр. системи за сакупљање воде, фарме и електране).

Критичне секторске међузависности постоје између критичних сектора и осетљивих подсектора. У утицајне секторе од којих у већој мери зависи функционисање многих других инфраструктурних сектора убрајају се производња и дистрибуција струје, информационе и комуникационе технологије, нафта и гас, друмски саобраћај и транспорт и финансијска инфраструктура. Колапс и прекид функционисања ових инфраструктура имају снажан ефекат на функционисање осталих инфраструктура. С друге стране, у најосетљивије инфраструктуре (оне чије нормално функционисање зависи од великог броја других инфраструктура) убрајају се здравствени сектор, сектор производње и дистрибуције хране, хемијска индустрија, снабдевање водом и контрола квалитета воде.

7.2.2. Кризни менаџмент у функцији заштите критичне инфраструктуре

Основ за функционисање кризног менаџмента у Словенији представља политика националне безбедности. Како је дефинисано у Резолуцији о стратегији националне безбедности Републике Словеније из 2001. године, политику националне безбедности чине различите активности, програми и планови везани за националну безбедност. Спољна политика, одбрамбена политика, политика унутрашње безбедности, економска политика, политика заштите од природних и других непогода (катастрофа) и политика еколошке заштите заједно чине политику националне безбедности.

Према Резолуцији о стратегији националне безбедности Републике Словеније, национални безбедносни систем чине три равноправна, међусобно повезана и међусобно зависна подсистема: безбедносни систем, систем заштите од природних и других непогода (катастрофа) и систем одбране (табела 7.4).

Систем националне безбедности Републике Словеније	Подсистеми		Функције	Управни органи подсистема
	Унутрашња безбедност; Безбедносни систем		Превенција и искорењивање криминалних прекршаја, узурпирања јавног реда и мира и претњи по личну безбедност и имовину; Обезбеђивање државних граница;Обављање послова везаних за унутрашњу безбедност; Обезбеђивање информација; Обављање надзора; Пружање судске заштите	Полиција, државни тужилац, судске агенције, агенције за контролу и инспекторати
	Систем заштите од природних и других непогода (катастрофа)		Унапређивање спремности за реаговање у случају катастрофа, пружање помоћи током катастрофа, осмишљање начина за минимизирање последица и опоравак од катастрофа, обезбеђивање основних услова за живот након катастрофа	Агенције за планирање управљања катастрофама, спасилачке службе, државне и локалне јавне службе, националне и локалне административне агенције, пословне организације, грађани
	Систем одбране	Војна одбрана	Спречавање и борба против војне агресије усмерене према Словенији	Словеначке оружане снаге
		Цивилна одбрана	Мере и активности које се предузимају ради нормалног функционисања читавог друштва – економска одбрана, психолошка одбрана, као и други неоружани облици отпора	Разне агенције државне и локалних управа, пословне организације, институти, друге организације, грађани

Табела бр. 7.4. – Систем националне безбедности Републике Словеније: подсистеми, функције подсистема и службе које су одговорне за обављање функција[559]

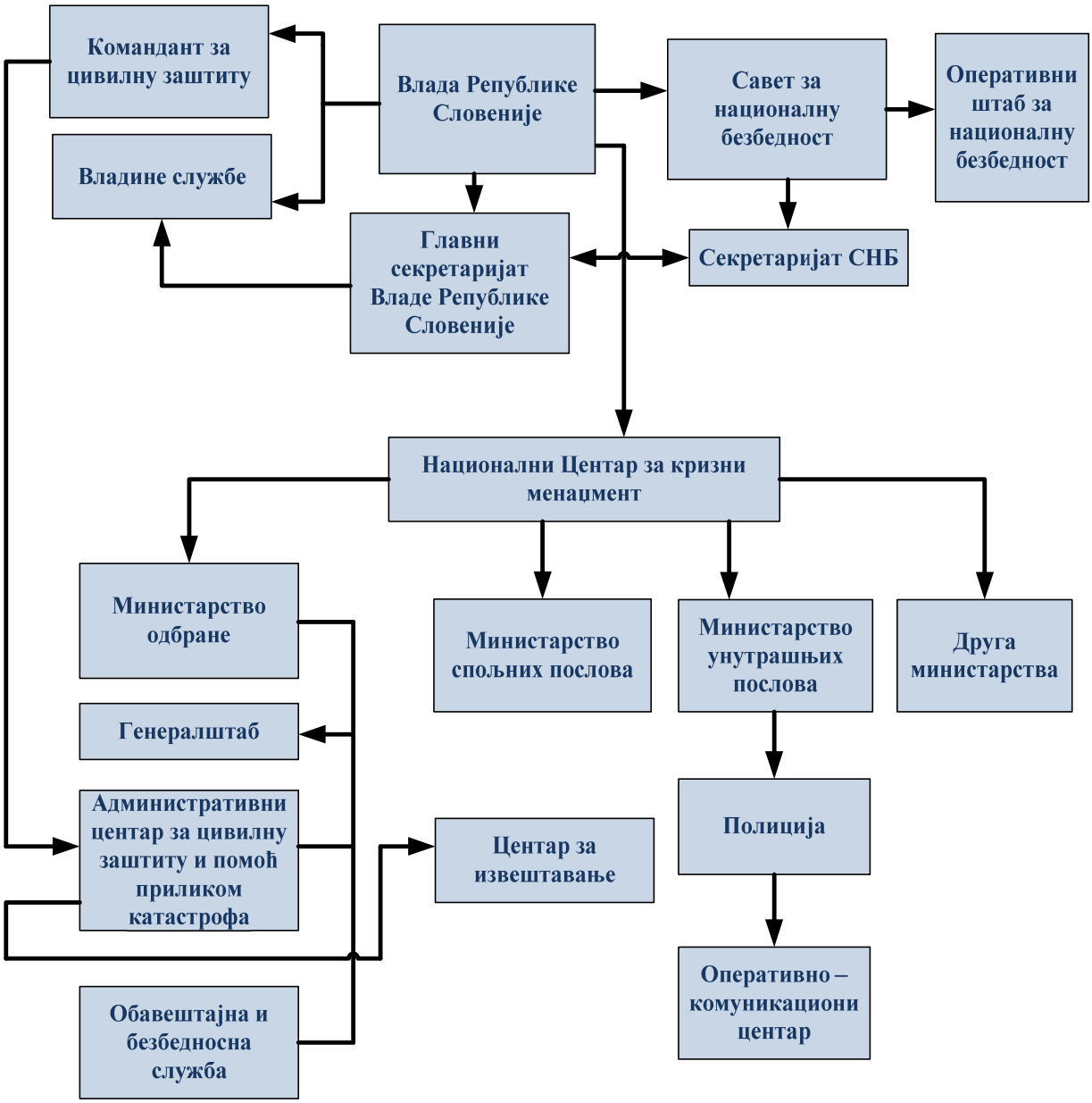
Систем одбране примарно је намењен за одбрану Републике Словеније од страних војних напада (претњи). Систем одбране састоји се од система војне и цивилне одбране. Систем заштите од природних и других непогода (катастрофа), бави се, како уосталом и име каже, заштитом од катастрофа, али и спашавањем и пружањем помоћи током катастрофа, било да се дешавају у мирнодопским или ратним условима.

[559] Jeraj, J., (2003), Civil Protection, the Protection and Rescue System, the System for Protection Against Natural and Other Disasters – Development and Place inthe National Security System (with an emphasis on the case of Slovenia), p. 27

Очување унутрашње стабилности и безбедности представља задатак безбедносног система.

Словенија је током последњих 10−15 година доста пажње поклонила формирању јединственог и свеобухватног система кризног менаџмента, који ће омогућити ефикасну реакцију на модерне комплексне претње, као и ефикасно учествовање у управљању кризама у оквиру граница државе, али и на међународном нивоу. Усвајање стратешких и доктринских докумената поставило је темеље за развој свеобухватног система, који се може поредити са другим међународним системима управљања кризама.[560] Елементи кризног менаџмента развијени су, према оценама стручњака, релатвно добро и подељени на индивидуалне подсистеме националног безбедносног система, али су ипак у доброј мери ограничени на катастрофе, непогоде, ванредне ситуације и ратне околности. Ипак, неопходно је квалитетније интегрисање система кризног менаџмента како би менаџмент комплексним догађајима био успешан.

[560] Међу поменутим законима, стратегијама и другим документима, најбитнији су: Резолуција о стратегији националне безбедности, Стратегија одбране Републике Словеније, Доктрина цивилне одбране Републике Словеније, Доктрина одбране, спашавања и пружања помоћи током криза, Национални програм заштите од природних и других катастрофа.



Слика бр. 7.3.– Координација кризног менаџмента у Словенији

У оквиру система кризног менаџмента, криза се дефинише као ситуација чији је узрок људски фактор, која има ограничено трајање, може да представља озбиљну претњу националној безбедности и не може се решити уобичајеним средствима и активностима; стога је ради очувања националне безбедности неопходно применити механизме кризног менаџмента. Кризни менаџмент представља облик организовања активности, процедура и планова за управљање кризама и за усмеравање даљег развоја.

Саставни део кризног менаџмента, цивилни кризни менаџмент, представља скуп цивилних активности усмерених ка заштити државе од негативних ефеката кризних ситуација, како на националном, тако и на међународном нивоу. Ове активности

олакшавају сарадњу између подсистема цивилне одбране, безбедносних система и система заштите од природних и других непогода (катастрофа). Координација активности кризног менаџмента приказана је на слици 7.3. [561]

Следеће институције у Словенији учествују у кризном менаџменту у наведеним областима делатности:

Заштита економије и финансија	**Министарство економије, Министарство финансија, Банка Словеније, Влада Републике Словеније**
Психолошка одбрана	Влада Словеније, Канцеларија за односе с јавношћу Владе Словеније, министарства и њихови органи и агенције
Војна заштита	Оружане снаге, Министарство унутрашњих послова, Министарство спољних послова, Словеначка обавештајна агенција, друга министарства и владине агенције (у складу са областима надлежности)
Унутрашња безбедност	Министарство унутрашњих послова, Словеначка обавештајна агенција
Међународна безбедност, операције везане за очување мира и подршку миру	Влада Словеније, Министарство одбране, Генералштаб словеначких оружаних снага, Министарство унутрашњих послова, Министарство спољних послова, Словеначка обавештајна агенција, друга министарстава и владине агенције (у складу са њиховим надлежностима)
Заштита и кризни менаџмент у оквиру информационих и комуникационих система	Министарство за информационо друштво, Владин центар за информатику, друга министарства и владине агенције (у складу са надлежностима)
Природне и друге непогоде (катастрофе)	Министарство одбране – Управа Републике Словеније за заштиту и помоћ приликом катастрофа, Министарство здравља, Министарство екологије и просторног планирања, Министарство унутрашњих послова, Министарство одбране, друга министарства и агенције

[561] Напотник, Д., 2003.

	Владе (у складу са надлежностима)
Инфективне болести које остављају значајне последице по становништво и државу	Министарство здравља, Институт за заштиту здравља, Министарство одбране – Управа Републике Словеније за заштиту и и помоћ приликом катастрофа
Заразне болести животиња	Министарство здравља, Министарство пољопривреде, шумарства и хране, Ветеринарска дирекција Министарства здравља, Управа за заштиту и помоћ приликом катастрофа при Министарству одбране

Табела бр. 7.5. – Типови криза и институције које учествују у кризном менаџменту током тих криза у Словенији

Органи који се баве кризним менаџментом одређени су и оформљени у већини области или се њихово оснивање планира приликом појаве првих симптома кризе у тим областима. Оснивање ових органа, у складу са Доктрином цивилне одбране Словеније, разматрано је на нивоу Владе, министарстава и психолошке одбране. Ови органи могу бити оформљени и могу функционисати под окриљем других институција. Органе чине експерти из области науке и економије, као и експерти из државних институција (државна администрација).

Министарства издају обавезне инструкције, упутства и предлоге везане за активности које се предузимају у случају криза органима територијалне организације, јавне администрације и свим организацијама која су под њиховом јурисдикцијом (компаније и сл).

Методе кризног менаџмента тестирају се током обука из области кризног менаџмента на националном, али и на међународном нивоу (НАТО нпр. редовно организује овакве обуке).

Уз приступање међународним безбедносним интеграцијама, Словенија развија систем кризног менаџмента у складу са решењима која имплементирају НАТО и земље чланице Европске уније. У склопу овог развоја основан је ***Национални центар за кризни менаџмент*** јануара 2004. године. Центар се бави контролом и анализом догађаја битних за националну безбедност и одбрану Републике Словеније, као и обавештавањем релевантних органа који се баве кризним менаџментом током рата и кризних ситуација. Центар такође координише активности свих подсистема у оквиру система националне безбедности Словеније и припрема експертску документацију на основу које се касније, у оквиру планирања акција кризног менаџмента, доносе

одговарајуће одлуке. Важно је истаћи да Национални центар за кризни менаџмент представља једини део читавог система подршке током кризне ситуације којим ће се користити Влада Словеније. Као такав, Национални центар за кризни менаџмент је у сталном контакту са осталим центрима у оквиру мреже агенција и организација које се баве кризним менаџментом.

7.2.3. Систем управљања и заштите од природних и других катастрофа

На основу закона о заштити од природних и других катастрофа из 1994. године, систем управљања катастрофама у Словенији има задатак да заштити људе, животиње, имовину, културно наслеђе и животну средину од природних и других катастрофа. Основни циљ система је редуковање броја катастрофа, њихово предупређивање и минимизирање негативних ефеката катастрофа.

Систем цивилне одбране у оквиру некадашње СФРЈ оформљен је крајем '60-их година прошлог века. Иако се систем тада базирао на пружању заштите и спашавању људи у ратним условима, у Словенији се систем цивилне одбране фокусира на заштиту од природних непогода (катастрофа) и катастрофа до којих је довео људски фактор. Нова законска регулатива усвојена након 1991. године, одвојила је систем управљања катастрофама од система одбране. Тиме су створене нове могућности за сарадњу са невладиним организацијама и квалитетнију сарадњу професионалних, истраживачких и других институција.[562]

Данас овај систем обухвата низ интегралних интердисциплинарних активности које имају заједничке циљеве и принципе. Систем управљања катастрофама чине бројне професионалне и волонтерске спасилачке службе, цивилна заштита, хуманитарне организације и друга одговорна тела и организације. Законску основу система управљања катастрофама чини Закон о заштити од природних и других катастрофа из 1994. године. Други закони везани за управљање катастрофама су Закон о заштити од пожара из 1993. године, Закон о ватрогасним службама из исте године, Закон о заштити од поплава из 2000. године, Закон о санацији последица природних катастрофа (непогода) из 2003. године, 2007. године усвојен је и петогодишњи Национални програм заштите од природних и других катастрофа.

Сви нови законски акти који се доносе у Словенији, а који су везани за заштиту од природних и других катастрофа (на пример заштита од индустријских несрећа),

[562] Ušeničnik, B., (1999), *Protection Against Natural and Other Disasters in Slovenia*. Ljubljana: Administration of the Republic of Slovenia for Civil Protection and Disaster Relief, Ministry of Defense, p. 2

увек се усклађују са постојећом законском регулативом Европске уније, због чланства у овој организацији.

Задаци система заштите од природних и других катастрофа су превенција, одржавање степена готовости, заштита од претњи, спашавање, пружање помоћи током катастрофа, обезбеђивање основних услова за живот и санација последица катастрофа.[563]

Управљање системом заштите од природних и других катастрофа и његово функционисање засновано је на подели обавеза између већег броја учесника у процесу заштите од природних и других катастрофа. Одређене обавезе у том смислу имају: држава, општине, компаније и друге пословне организације, власници и корисници стамбених и других грађевина и грађани.[564] Држава и општине одговорне су за превенцију и елиминисање опасности и моментално реаговање у случају катастрофа. Компаније и друге организације одговорне за заштиту својих радника, имовине и животне средине у случају катастрофа. Власници и корисници стамбених и других објеката су одговорни за имплементацију мера заштите у оквиру тих објеката, као и спашавање и пружање помоћи током катастрофа. Грађани, према члану 15 Закона о заштити од природних и других катастрофа, такође имају одређена права, али и дужности током катастрофа. Дужност грађана је да учествују у цивилној заштити, обезбеђивању материјалне подршке, обукама везаним за појединачну и колективну заштиту и имплементацију мера заштите.

Народна скупштина поставља основе за организовање и имплементирање мера заштите од природних и других катастрофа, усваја националне програме у овој области, надзире имплементацију мера заштите и обезбеђује средства за санацију последица природних катастрофа.[565]

Министарство одбране има посебну улогу у оквиру система заштите од природних и других катастрофа. Ову улогу обавља национална агенција за управљање катастрофама, која је функционише у оквиру Министарства одбране. Пуно име агенције је Дирекција за цивилну заштиту и помоћ приликом катастрофа. Дирекција ја задужена за развијање и имплементацију административних и других мера везаних за

[563] Ibid, p. 8
[564] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 5, 1994.
[565] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 92, 1994.

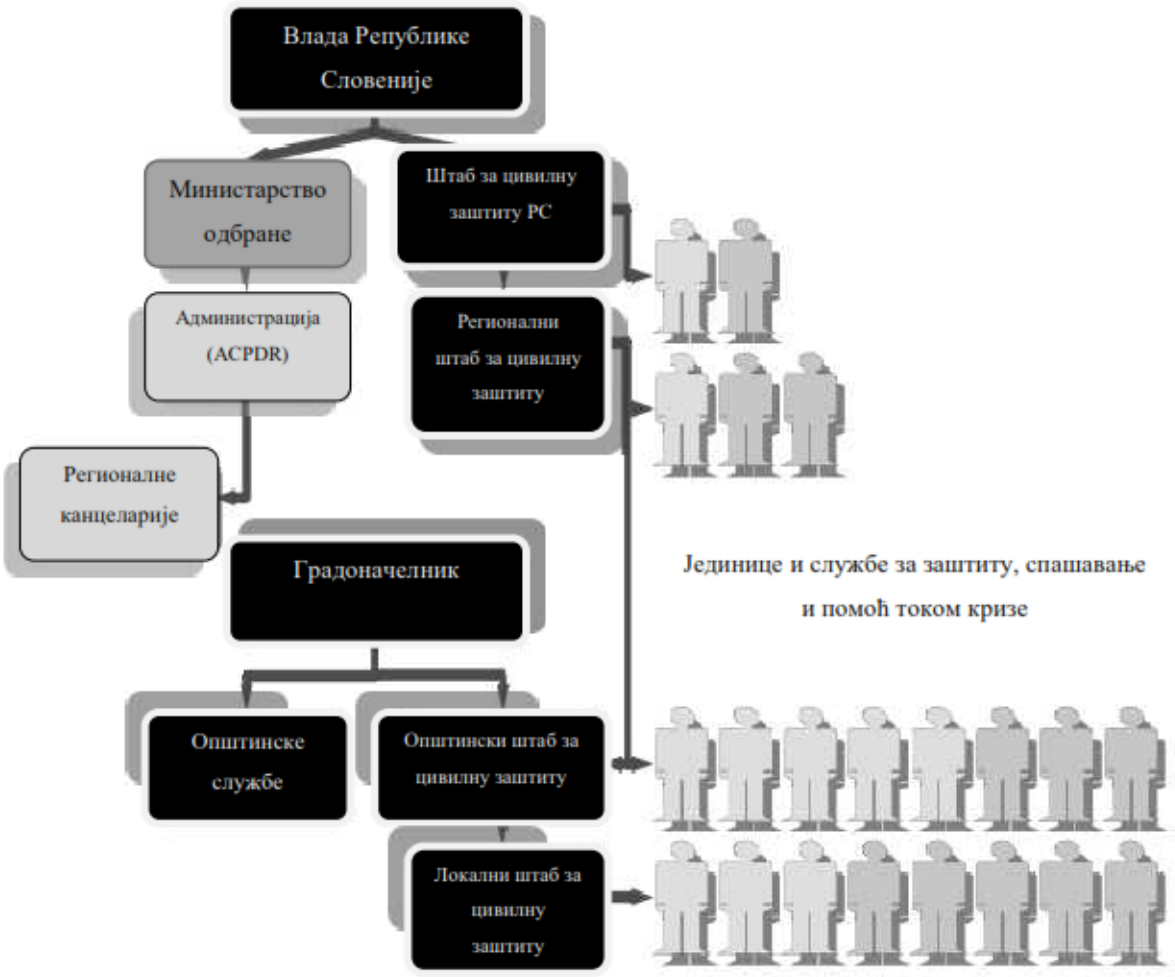
интегрисано реаговање током ванредних ситуација, нарочито оних ванредних ситуација везаних за управљање катастрофама.[566]

Дирекција за цивилну заштиту и помоћ приликом катастрофа је како на националном, тако и на регионалном нивоу задужена за регулисање и контролу система заштите од природних и других катастрофа, планирање развојних пројеката и истраживачких активности, процену ризика и израду нацрта националног плана за реаговање током ванредних ситуација, опремање националних спасилачких служби, организовање и имплементацију обука везаних за заштиту и спасавање током катастрофа, координацију активности током ванредних ситуација, организовање и имплементацију јединственог система надзора и контроле, обавештавање и издавање упозорења о непосредној опасности, процену штете коју проузрокују катастрофе, пружање помоћи локалним заједницама током и након катастрофа, и на крају Дирекција за цивилну заштиту одговорна је и за међународну сарадњу у поменутој области. Дирекција такође пружа подршку у функционисању команданту за цивилну заштиту и његовом штабу.[567]

Службе за заштиту и спасилачке службе у Словенији организоване су на општинском и на националном нивоу. Већина служби постоји већ на локалном нивоу. Грађани учествују у заштити и спашавању током ванредних ситуација кроз следеће организације и активности:[568]

- Волонтерске организације (функционишу по принципима невладиних организација), пре свега хуманитарне организације,
- Професионалне организације (баве се пружањем професионалне помоћи), такви су јавни институти, административне организације и др.,
- Организације чије је постојање обавезно и дефинисано Законом о цивилној заштити.

[566] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 101, 1994.
[567] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 98, 1994.
[568] Влада Словеније, Доктрина заштите, спашавања и помоћи приликом ванредних ситуација, 2002.



Слика бр. 7.4. - Менаџмент система заштите од природних и других катастрофа[569]

У спасилачке службе на општинском нивоу убрајају се: волонтерске организације (ватрогасне службе, извиђачке службе, радио аматери, дресери спасилачких паса, спасилачке ронилачке службе, локални Црвени крст), професионалне организације (општинске ватрогасне службе, службе хитне медицинске помоћи, јавне службе) и организације цивилне заштите (прва помоћ, службе за потрагу у спашавању, службе за одржавање склоништа за случај ваздушних напада, логистичке службе итд).[570]

Менаџмент система заштите од природних и других катастрофа подразумева оперативно управљање процесом цивилне заштите, службама за заштиту и спасилачким службама, и на националном и на локалном нивоу. За менаџмент читавог

[569] Ušeničnik, B., (1999), *Protection Against Natural and Other Disasters in Slovenia*. Ljubljana: Administration of the Republic of Slovenia for Civil Protection and Disaster Relief, Ministry of Defense
[570] Дирекција Републике Словеније за цивилну заштиту и помоћ приликом катастрофа, 11. новембар 2003.

овог система задужени су команданти за цивилну заштиту, штабови и команданти за ванредне ситуације.[571]

Команданти за цивилну заштиту на свим нивоима имају додатна овлашћења у случају већих несрећа. Додатна овлашћења за циљ имају да олакшају активности везане за заштиту људи.[572]

Телекомуникациони, информациони и системи за узбуну функционишу као аутономни, јединствени систем радио комуникације и користе га све спасилачке службе и јединице у земљи. Дирекција за цивилну заштиту и помоћ приликом катастрофа задужена је за техничке аспекте заштите овог система од узурпирања. Комуникациони центри система радиокомуникације налазе се у склопу регионалних центара за извештавање као и у саставу националних центара за извештавање и представљају средство за повезивање корисника са телекомуникационим системима. Регионални центри за извештавање баве се сакупљањем и прослеђивањем података спасилачким службама.

Информациони систем за природне и друге катастрофе може да складишти, обрађује, прослеђује и размењује податке о природним и другим катастрофама, повезујући тиме Дирекцију за цивилну заштиту и помоћ приликом катастрофа, регионалне центре за извештавање, штабове цивилне заштите и друге организације које су укључене у реаговање у ванредним ситуацијама.[573]

Едукација и обука служби за спашавање и других релевантних служби које се ангажују током ванредних ситуација врши се кроз обуку особља које се бави цивилном заштитом кроз програме које одобрава Министарство одбране. Обуке се састоје из три дела: упознавања са проблематиком, основне обуке и напредне обуке.

Едукација јавности о личној и заједничкој заштити у случају катастрофа представља обавезу државе и општине.[574] Едукација се врши на различите начине – објављивањем разних публикација, путем медијских кампања, па чак и путем програма у које су укључени деца предшколског и школског узраста.Такође, организују се и практичне вежбе.

Инспекцију, односно контролу имплементације закона везаних за заштиту од катастрофа обавља орган Министарства одбране – Инспекторат за заштиту од

[571] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 81, 1994.
[572] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 84 и 85, 1994.
[573] Ušeničnik, B., (1999), *Protection Against Natural and Other Disasters in Slovenia*. Ljubljana: Administration of the Republic of Slovenia for Civil Protection and Disaster Relief, Ministry of Defense, p. 28
[574] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 110, 1994.

природних и других катастрофа Републике Словеније,[575] као и његове регионалне канцеларије.

Финансирање се врши углавном из националног и општинских буџета и делом кроз донације и међународну помоћ.[576] Сваке године Република Словенија издваја 0,3% националног буџета за заштиту и спашавање, а општине издвајају још 3% из својих општинских буџета. Ватрогасне службе делом се финансирају од дажбина које грађани уплаћују у сврху осигурања од пожара.

7.2.4. Заштита критичне информационе инфраструктуре

Словенија има прилично развијен систем заштите критичне информационе инфраструктуре, који је великим делом последица усклађивања националне законске регулативе са регулативом Европске уније. У склопу формирања заштите критичне информационе инфраструктуре као и заштите критичне инфраструктуре уопште и националне безбедности, донет је низ закона и стратегија као што су:

- Стратегија развоја Словеније од 2006. до 2013. (у којој се као један од главних циљева будућег развоја утврђује унапређење квалитета живота и благостања грађана кроз увођење образовања и обучавања људи путем ИКТ регионалних и локалних центара; за циљ се поставља и промоција интензивнијег коришћења информационих и комуникационих технологија и служби у оквиру домаћинстава);[577]
- Стратегија[578] и акциони план[579] развоја сервиса е-Владе (оформљена ради побољшања ефикасности јавне администрације);
- Стратегија развоја IT и електронских служби (има за циљ омогућавање балансираног развоја IT јавне администрације и електронских служби, као и интеграцију решења и искустава е-Администрације у другим сферама цивилног друштва. Стратегија настоји да установи оквир за даљи развој IT и електронских служби у оквиру јавне администрације);

[575] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 103, 1994.
[576] Закон о заштити од природних и других катастрофа Републике Словеније, Члан 115, 1994.
[577] Стратегија развоја Словеније (2006-2013) доступна је на интернет адреси: http://www.slovenijajutri.gov.si/fileadmin/urednik/dokumenti/Slovenia_s_Development_Strategy.pdf 10.02.2013
[578] Стратегија развоја сервиса е-Владе доступна је на интернет адреси: http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/mju_dokumenti/english/SEP2010_english_final.doc 10.02.2013
[579] Акциони план развоја сервиса е-Владе доступан је на интернет адреси: http://e-uprava.gov.si/eud/euprava/akcijski_nacrt_e-uprave_2010.doc 10.02.2013

- Стратегија развоја информационог друштва у Републици Словенији (стратегија даје смернице за усклађивање европских циљева са националним приоритетима у области развоја информационог друштва; Неки од циљева стратегије су: формирање јединственог европског информационог система, увођење иновација и инвестирање у развој информационих и комуникационих технологија, истраживање и увођење иновација у електронско пословање, оснивање електронских корисничких служби);
- Закон о основним административним процедурама е-Владе Словеније[580] (усвојен је први пут 1999. године, а измењен 2006. године и пружа опште законске оквире административних процедура и односа);
- Закон о електронским комуникацијама[581] (усвојен је у марту 2004. године, а измењен је 2009. године; Закон настоји да створи и очува конкурентност тржишта електронских комуникација, да очува ефективно коришћење спектра радио фреквенција и да заштити корисничка права);
- Закон о електронској трговини и електронском потпису[582] (прва верзија Закона усвојена 13. јуна 2000. године даје законску основу за коришћење е-потписа и развој е-служби у Словенији; Закон је измењен 2004. године новим одредбама о електронском потпису, којима се прецизније дефинишу одговорности провајдера електронских услуга и постављају основе за реализацију пројекта електронских идентификационих докумената);
- Декрет о административним операцијама у оквиру електронске трговине (усвојен је 2005. године и мењан амандманима више пута; Декрет даје законске основе за увођење службе електронског потписа и службе е-Владе);
- Закон о електронском тржишту (усвојен 2006. године и измењен 2009. године – настоји да регулише пружање услуга у области е-трговине, да утврди одговорности провајдера, да регулише начин вођења спорова везаних за е-трговину, да дефинише обавезе судства у тим процесима);
- Закон о сајбер-криминалу (постоји у склопу словеначког Кривичног закона и идентификује три типа криминалних активности: злоупотребу личних података неопходних за упадање у базе података, неовлашћени упад у

[580] Official Gazette of the Republic of Slovenia, no. 24/2006 - ZUPUPB2
[581] Slovenian Electronic Communications Act (ZEKom-UPB1): http://www.apek.si 10.02.2013
[582] Закон о е-трговини и електронском потпису доступан је на интернет адреси: http://www.uradnilist.si/1/objava.jsp?urlid=200425&stevilka=1066 10.02.2013

компјутерске системе и програме и средстава за остварење претходне две криминалне активности);

- Закон о електронској идентификацији (у склопу припрема за оживљавање система електронске идентификације усвојен је низ других законских и подзаконских аката: Закон о електронској трговини и електронском потпису[583] који пружа законску основу за коришћење е-потписа и електронских служби у Словенији; Декрет о условима спровођења електронске трговине и коришћења електронских потписа;[584] Правила о званичној процедури уписа у регистар сертификационих органа Републике Словеније;[585] Закон о доступности јавних података[586] којим се јавности допушта увид у сва документа која донесу државни органи; Закон о заштити личних података Републике Словеније,[587] којим се дефинишу права, обавезе и мере превенције незаконитог коришћење туђих личних података: Закон о државном регистру становништва;[588]
- Закон о заштити докумената и архива (усвојен је 2006. године, а задатак му је да регулише употребу и чување докумената,како оних у електронској форми тако и опипљивих докумената, као и њихову заштиту);
- Кодекс понашања оператера јавних мобилних електронских комуникација везан за безбедније коришћење мобилне комуникације од стране млађих тинејџера и деце;[589]
- Меморандум о неопходности спречавања говора мржње на интернет порталима (представља саморегулаторни акт, који је потписао низ веб портала и других релевантних организација у оквиру спровођења програма *Сплетно око*; Програм за циљ има редуковање говора мржње на интернет порталима).

Република Словенија ужива доста висок степен безбедности у релативно нестабилном регионалном и међународном окружењу, иако је као и друге развијене

[583] Official Gazette of the RS, No. 57/2000, 25/04.
[584] Official Gazetteof the Republic of Slovenia, No. 77/2000 and 2/2001
[585] Official Gazette of the RS, No. 99-4859/2001
[586] Official Gazette of the RS, No. 51/2006
[587] Slovenian Official Gazette No. 86/2004, Personal Data Protection Act (ZVOP-1)
[588] Official Gazette of the RS, No. 1/1999, 54/2002, 39/2006
[589] Овај кодекс представља саморегулаторни акт са препорукама за операторе мобилних електронских Комуникација и доступан је на интернет адреси: http://www.gsmeurope.org/documents/eu_codes/Slovenian_code_of_conduct.pdf 10.02.2013

земље све више изложена различитим несиметричним невојним безбедносним ризицима и претњама.

Адекватан одговор на такве ризике и претње је формирање високо осетљивог, јединственог и интегрисаног система националне безбедности Републике Словеније, укљученог у систем колективне одбране, као колективне безбедности. Само се такав национално-безбедносни систем може ефикасно прилагођавати честим и интензивним променама стратешког окружења, уз истовремено смањивање могућности за настанак кризе и способност да се одлучно и успешно супротстави њеном негативном развоју.

Према Резолуцији владе Републике Словеније из 2010. године, критична инфраструктура у Словенији од националног значаја укључује сва добра и службе која су од суштинског значаја за државу и чије би нарушавање или уништавање имало велики утицај на националну безбедност, економију, витално функционисање друштва, здравље, безбедност, заштиту, као и на целокупно друштвено благостање.[590]

[590] Resolution of the Government of the Republic of Slovenia, No 80000-2/2010/3 of 19 april 2010.

8. ПРЕДЛОГ МОДЕЛА ЗАШТИТЕ КРИТИЧНИХ ИНФРАСТРУКТУРА У РЕПУБЛИЦИ СРБИЈИ

У савременој науци развијен је велики број истраживачких метода, међу којима је и метод моделовања. Овај метод је данас широко прихваћен како у примењеним, тако и у теоријским наукама.

Циљ сваког моделовања јесте да успостави такав модел који може да замени оригинални објект истраживања. Модел се, као предмет истраживања и истраживачки поступак, карактерише низом одређених предности, што га чини незаменљивим методом у модерним научним истраживањима система. Међутим, и метод моделовања – као, уосталом, сваки метод – има извесних недостатака, па се не може говорити о његовој перфекцији, али је за извесна истраживања најзахвалнији метод.[591]

Ефикасно коришћење метода моделовања захтева много више знања него што је само стручно знање потребно да се модели изаберу, имплементирају и користе, као и да се имплементирају резултати моделовања. Потребно је схватити однос између моделовања и других планских активности, јер се коришћење модела и извршене анализе морају правилно интегрисати са другим планским активностима. За успех научног истраживања такође је битно да се јасно формулише проблем, затим циљеви и задаци, да се поставе критеријуми и осмисли методологија презентовања резултата добијених у поступку моделовања.[592]

Модел је логичка (симболичка) конструкција, која репродукује одређене карактеристике објекта који истражујемо, и која је одређена раније дефинисаним потребама. Можемо га схватити и шире: то је „сваки систем који је представљен у мислима или материјално реализован, који одсликава или репродукује објект истраживања и који је способан да тај објекат замени тако да нам проучавање модела пружи нову информацију о том објекту".[593] Унутар мноштва модела, стварамо теоријске или идеалне моделе (за разлику од модела који представљају физичке, материјалне објекте). Они се могу поделити на очигледне моделе (елементи имају некакву везу с елементима објекта за моделовање) и на формалне, тј. симболичке и логичке моделе за које није обавезна видљива (спољна) веза с објектом који се

[591] Љешевић, Милутин, *Метод моделовања у истраживању животне средине*, СГД, Београд, 1990, стр 12.
[592] Land, Kenneth C., *Models and Indicators*, Social Forces, Vol. 80, No. 2 (Dec. 2001), p. 382
[593] Леонтьев А.А., *Основы психолингвистики*, Институт "Открытое общество", Москва, 1997, стр. 3.

моделује (али је зато обавезна функционална сличност). Некада се, у литератури, знаковни и логички модели називају још и „моделима и конструкцијама из замишљених елемената“.[594]

Моделовање није било какво одражавање објекта у моделу. Правећи модел реалног објекта, ми конструишемо други објекат – реалан или замишљен – изоморфан датом објекту по одређеним важним карактеристикама.

То ново, што сазнајемо о објекту – то су такве његове црте које се „аутоматски“ преносе у модел, када ми сазнајно обезбеђујемо изоморфност објекта при раније одређеним параметрима.

Понекад се схватање објекта непотребно сужава, па се, на пример, научним сматрају само аксиоматски модели, или само математички модели. То је нелегитимно. Свако описивање објекта које је довољно исправно, тј. које одговара одређеним потребама моделовања објекта (које је изоморфно са тим објектом) и које је при томе хеуристички значајно (даје нам нову информацију о том објекту) – јесте његов логички модел и потчињава се општим законима моделовања.

Моделовање објекта је неопходна компонента његовог упознавања, али се оно ту никако не завршава.

Можемо направити безброј модела једног истог објекта, таквих да подједнако одговарају особинама тог објекта, али да се међусобно разликују – сваки модел одражава не само реална, објективна својства, већ и нашу тачку гледишта на тај објекат, као и потребе у погледу сличности модела објекту, које ми сваки пут приказујемо.

Ни један модел није потпун и не исцрпљује сва својства објекта. Таква исцрпност није ни могућа ни потребна. У науци ми сваки пут, при моделовању, рашчлањујемо одређена својства објекта, остављајући неке друге особине ван фокуса нашег истраживања. Чак и моделујући иста својства, одсликавајући их у оквиру једне исте науке под одређеним, врло уским углом посматрања, можемо створити неколико неподударних модела, зависно од система који користимо за разумевање и операције, и зависно од конкретних задатака моделовања.

Апстрактни објекат јесте уопштавање мноштва могућих модела датог конкретног објекта (свеукупност конкретних објеката или, како се често каже,

[594] *Ibid*. стр. 3.

„предметна област“) и, управо, инвариант тих модела.[595] Сви модели, по свом опредељењу (по својој суштини, намени) поседују опште, инваријантне карактеристике, које одражавају суштинска својства објекта и остају без промена при преласку из једног модела у други. Зато те инваријантне карактеристике и могу бити обједињене у појам апстрактног објекта или, као што смо већ рекли, у појам предмета дате науке.

Процес моделовања састоји се у уочавању свих битних чинилаца или момената одређене појаве и њиховом представљању у облику математичких једначина или техничких предмета или система. За процес моделовања везује се принцип универзалности предмета моделовања, принцип разноврсности модела који се изражава и принцип прототипности онога што се изражава. У суштини, улога модела се може схватити као *инструментална*, јер је модел инструмент помоћу кога се истражује објект, и као *сазнајна* зато што се помоћу резултата модела сазнају карактеристике самог објекта истраживања.

У поступку моделовања, понашање система се може пројектовати на основу претходних знања („a priori“ приступ) и на основу сазнања која се стичу у току самог процеса истраживања („post-priori“ приступ).

„A priori“ приступ заступа став да се од постојећих општих теорија може доћи до модела који ће одсликавати све специфичности које су постављене пред модел. Други приступ претпоставља да нема претходних сазнања о процесима који се моделирају, већ се заснива на покушају да се развојем информација добијених емпиријским путем утврде подаци потребни за модел. У почетку је више примењиван први приступ; међутим, развојем науке и технике добијање података је знатно олакшано, те се најчешће прави синтеза ова два приступа у циљу ефикаснијег моделовања.

Поступак моделовања се састоји од више фаза. Универзалну шему овог поступка није могуће дати јер она зависи од самог предмета истраживања. Међутим, као заједничке фазе у различитим научним дисциплинама прихваћене су: *концептуализација*, *избор типа модела*, *верификација* и *потврда модела*.

Да ли и које моделе треба користити процењује се на основу потребе у сваком посебном случају. Приликом одлучивања неопходно је установити да ли већ постоји

[595] Не свих, већ оних који одражавају баш та, дата објективна својства објекта који се моделује, јер он може имати и друга својства, не мање битна, али која су предмет изучавања других наука, под другим углом посматрања.

модел који би одговарао постављеним захтевима, да ли се расположиви модел мора модификовати или је потребно развити посебан модел.

8.1. Избор типа модела заштите критичних инфраструктура

Истраживање проблема кризног менаџмента у функцији заштите критичних инфраструктура у земљама у транзицији, осим истицања организације и функционисања кризног менаџмента у развијеним земљама, ограничен је на транзиционе земље као специфичан културно-историјски контекст. Транзиционе земље су суочене са великим политичким, економским и општим друштвеним тешкоћама, при чему богата искуства других, развијенијих земаља, али и захтеви интеграционих процеса, отварају низ могућности и указују на могућа нормативна и организациона решења. Ипак, могућност имплементације теоријских модела и практичних решења развијених земаља нису аутоматски применљива на транзиционе земље, које не испуњавају потребне политичке, економске и нормативне предуслове.

Република Србија у односу на земље из непосредног окружења ужива доста висок степен безбедности у релативно нестабилном регионалном и међународном окружењу. Стога се систем кризног менаџмента у фукцији заштите КИ земаља из непосредног окружења (БиХ, Црна Гора, БЈР Македнија и Албанија) није могао узети као референтни оквир за избор и предлагање модела заштите КИ у Републици Србији.

С друге стране, Бугарска и Словенија су, због просторно-географских, политичких, друштвено-економских и културолошких сличности, као и у погледу доношења и спровођења политике заштите КИ, добра референтна тачка за извлачење поука из искустава која би се могла применити у Р. Србији.

Словенија и Бугарска су извршиле истраживање критичних инфраструктура уз непосредну стручну и материјалну помоћ Шведске. Истраживања су обавиле владине координационе групе за заштиту КИ заједно са свим релевантним министарствима и уз примену критеријума међусекторске анализе, с циљем идентификације најважнијих критичних инфраструктурних сектора, њихових функција и задатака, као и дефинисања организација, агенција и других државних и приватних удружења која су одговорна за функционисање и заштиту КИ. Следећи поменуту добру праксу, Р. Србија би свој систем кризног менаџмента и заштите КИ могла да осмисли и примени у складу са досадашњим искуствима Словеније и Бугарске. Тим пре, што се Р. Србија, исто као и Р. Словенија и Бугарска, налази на раскршћу неколико важних коридора

друмског, железничког, водног и ваздушног саобраћаја, а инфраструктура информационих и комуникационих технологија и енергетике још увек нису саставни део европске инфраструктуре.

Готови модели Словеније и Бугарски се, са друге стране, не могу преузети и имплементирати у Р. Србији без одређених модификација, јер свака држава има своје специфичне особености. Објекти критичне инфраструктуре асиметрично су дистрибуирани у оквиру Словеније - критичне инфраструктуре у већој мери су смештене у урбаним срединама. Посебно су критичне мулти-инфраструктуралне области тј. области у којима је лоциран већи број различитих типова инфраструктура. Ометање нормалног функционисања једног типа инфраструктуре у оваквим областима брзо би посредно утицало и на функционисање других инфраструктура у тој области. У Србији су, пак, објекти критичне инфраструктуре равномерно дистрибуирани на целој територији државе (по чему је Србија сличнија Бугарској). Осим тога, Србија нема нуклеарну инфраструктуру какву поседују Словенија и Бугарска (Кршко и Козлодуј).

8.2. Анализа проблема и предлог за модификацију изабраних модела

Док су многе развијене државе идентификовале своје критичне инфраструктуре у Србији и региону се о овој теми мало дискутовало.[596] Мисао о кризама, посебно на нашим просторима, је још увек на зачетку, а практично поступање у кризним ситуацијама је на граници неосмишљеног и *ad hoc* реаговања. По мишљењу неких теоретичара личи на инстинктивну реакцију. Практичари у разним областима, почевши од политике, економије до заштите животне средине, и на различитим нивоима, од државног преко регионалног до локалног, на кризе најчешће одговарају реактивно, ситуацијски и исхитрено, без стратешке визије и било каквог краткорочног или дугорочног плана.[597] Потреба динамичког, проактивног и стратешког приступа нарочито је неопходна у процесу планирања заштите критичне инфраструктуре у условима различитих типова кризних и ванредних ситуација.

Република Србија је последњих година учинила значајне напоре у стварању интегрисаног система заштите и спашавања како би се на адекватан начин одговорило

[596] Кљаић, З., (2010), "Примена ИКТ-а у управљању критичном инфраструктуром у транзицијским земљама", *ТЕЛФОР*, Београд.
[597] Funda, D., Majić, T., (2011), Upravljanje krizom, International Conference "Crisis Management Days", Velika Gorica.

у условима угрожавања критичних националних ресурса. Република Србија је децембра 2009 године добила Закон о ванредним ситуацијама[598] и у њему успоставила нормативну основу за један нови – интегрисани систем управљања ванредним ситуацијама.[599] Основним текстом Закона из 2009. године, држава се определила да Министраство унутрашњих послова буде надлежно за израду Процене угрожености од елементарних непогода и других несрећа. Истовремено, Аутономне покрајине и јединице локалне самоуправе, министарства и други органи и организације израђују процену угрожености у делу који се односи на њихов делокруг и достављају је Министарству унутрашњих послова. Влада Републике Србије је на основу чл. 45, став 4. Закона о ванредним ситуацијама донела Уредбу о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама. Овим документом, поред већ наведене Процене угрожености, који су дефинисани у Закону о ванредним ситуацијама, предвиђа се да ће део Процене бити и процена критичне инфраструктуре са гледишта елементарних непогода и других већих несрећа. У Србији се овом уредбом први пут уводи појам критичне инфраструктуре али и даље без јасног дефинисања о којим је елементима или областима инфраструктуре реч. Такође, нису одређени субјекти који би сносили одговорност у заштити критичне инфраструктуре.

После усвајања Закона о ванредним ситуацијама, донет је цео низ подзаконских аката који утврђују права и обавезе појдиних субјеката, док су неки још у фази доношења и/или измена тако да, законски оквир још увек није сасвим заокружен. Поред Закона о ванредним ситуацијама постоји цео низ комплементарних закона који су такође значајни за управљање ванредним ситуацијама и који уређују различите области као што су Закон о заштити од пожара, (2009), Закон о заштити животне средине (2009), Закон о водама (2010), Закон о ваздушној пловидби, (2011), Закон о заштити од јонизујећег зрачења и нуклеарној безбедности (2012), Закон о безбедности и заштити на раду (2005), Закон о приватном обезбеђењу (2013) итд., али веома важни закони као што је Закон о експлозивним материјама, Закон о запаљивим течностима и гасовима и Закон о противградној заштити још увек нису донети. Закон о ванредним ситуацијама је генерално уредио област управљања ванредним ситуацијама на свим

[598] Основни текст закона у Сл. гласнику РС“, бр. 111/09. Измене и допуне закона у Сл. гласнику РС бр 92/2011 и Сл. гласнику РС 93/2012.

[599] Треба нагласити да је поред Закона о ванредним ситуацијама системски правни оквир за управљање ванредним ситуацијама у Србији одређен и Уставом Републике Србије (2006), Законом о државној управи (2010) Законом о министарствима (2011) Законом о локалној самоуправи, (2007) Законом о мерама за случај ванреднос стања (1991), Законом о полицији (2006), Законом о војсци Србије (2007), Законом о одбрани (2009) и стратешким документима: Стратегијом националне безбедности (2009) и Стратегијом одбране Републике Србије (2009).

политичко-административним нивоима, тако да покрајински и општински/градски прописи само операционализују одредбе Закона.

Систем за управљање ванредним ситуацијама постављен је тако да сваки ниво политичко територијалне организације има одговорност и за припрему и за одговор на ванредне ситуације у оквиру свог уставног и законског мандата и оперативних капацитета. Локални ниво има више оперативну улогу, регионални ниво је нека врста медијатора[600] од локалног нивоа ка покрајинској односно републичкој влади. Улога националног/државног нивоа је пре свега бављење стратегијом и укупним дизајнирањем система, као и координација, мониторинг и исправљање грешака и пропуста у функционисању система.[601]

Према Закону о ванредним ситуацијама Република Србија обезбеђује изградњу јединственог система заштите и спасавања у складу са овим законом и другим прописима, као и програмима, плановима и другим документима који се односе на заштиту и спасавање и цивилну заштиту, Народна скупштина усваја Националну стратегију заштите и спасавања у ванредним ситуацијама док је Влада одговорна за све аспекте система за управљање кризним ситуацијама (усвајање планова, процене угрожености и других докумената, наређивање опште мобилизације јединица ЦЗ, надзор над припремама за ванредне ситуације итд.).

У погледу мера заштите критичне инфраструктуре, све државе, укључујући и Републику Србију, морају да утврде и редослед поступака: а) идентификацију критичне инфраструктуре, б) израда мапа критичне инфраструктуре, ц) размена информација, д) оспособљавање особља ангажованог на пословима и задацима у системима критичне инфраструктуре, е) увежбавање система за заштиту критичне инфраструктуре или опоравак у случају кризне или ванредне ситуације.[602]

Област ванредних ситуација свеобухватно је уређена Законом, који је матични за ту област. Поједина питања од значаја за област ванредних ситуација (безбедносна, еколошка и др) уређена су и посебним законима. Нпр. одредбама чл. 15 и 57. Закона о полицији[603] утврђене су посебне мере значајне за заштиту здравља и живота људи и за спречавање угрожавања безбедности изазваног елементарним непогодама или

[600]Улога региона у управљању ванредним ситуацијама није у потпуности јасно дефинисана у Закону о ванредним ситуацијама.
[601] Kešetović Želimir, "Country study Serbia", report within ANVIL project - European Union's Seventh Framework Programme FP7/2007-2013 under grant agreement n°28467, 2013
[602] Национална стратегија заштите и спречавања у ванредним ситуацијама (Усвојена на седници Скупштине Републике Србије 18.11.2011).
[603] "Службени гласник РС", бр. 101/2005, 63/2009 – одлука УС и 92/2011.

епидемијама. Те мере своде се на овлашћење државе да у изузетним случајевима, попут катастрофе 2014. године, ограничи или забрани кретање на одређеним подручјима, забрани настањивање на одређеном подручју, наложи евакуацију – напуштање одређеног подручја или објекта. И у целини посматрано, наведена и слична овлашћења државних и других органа пружају могућност за адекватно супротстављање катастрофи до које је дошло услед незапамћених поплава 2014. године.

Нема сумње да ће се питањима адекватних мера непосредно пре, за време и после катастрофе, многе струке и науке, још дуго бавити и по изучавању ових катастрофалних поплава извести бројне закључке. Било би добро да ти закључци у далеко већој мери послуже будућности и превенцији (предвиђању) него да се по традиционалном приступу ограниче само на објашњење протеклих догађаја и већ установљених феномена.

Доношење једног броја од недостајућих прописа условљено је и претходним стварањем потребних материјалних и других услова за њихову примену, што се може закључити из још увек актуелног приказа стања из области ванредних ситуација, садржаног у "Националној стратегији заштите и спасавања у ванредним ситуацијама.[604] Према том приказу, а и практично, указује се да је неопходно "веће техничко иновирање и опремање, као и унапређење инфраструктурног, информационог и технолошког система уз примену савремених теннологија и стандарда Европске уније". Ваља нагласити да су у овој стратегији и други недостаци постојећег система заштите и спасавања објективно препознати, а нарочито и то да су стратешки циљеви добро постављени. Требало би убрзати њихово остваривање.

Размере катастрофе која је 2014. године задесила Србију захтевају да се узме у обзир и чињеница да се еколошка ситуација на планети Земљи погоршава. Због те чињенице политика је прихватила екологију и настала је еколошка политика, која се развија у многим државама. Два принципа заступљена су у тој политици, и то принцип *еластичности* који се своди на предузимање акција после настанка проблема и принцип *предострожности* који подразумева да се потенцијалне опасности отклањају одмах, пре прерастања у катастрофу. Велике расправе воде се о предностима и недостацима ових принципа. Према једном мишљењу "оба принципа су за креирање еколошке политике апстрактна, пошто су општи. Кључно питање јесте шта

[604] "Слижбени гласник РС", бр. 86/2011.

подразумевају када влада треба да донесе конкретне одлуке у различитим сферама. Ако се деси огромна катастрофа да је мало тога могуће урадити да се побољша *ex post* ситуација, онда је принцип еластичности под великом сумњом. С друге стране, за идеју предострожности велики изазов представља дефинисање нивоа ризика за различите људске пројекте који се не може толерисати. Ако се уско тумачи, онда би уклањање свих ризика могло да значи уклањање свих могућности".[605]

Наведени цитат можда неће бити од помоћи онима који "све знају" о узроцима и последицама катастрофалне поплаве у Србији маја 2014. године, али је чињеница да тек предстоји тежи пут да се до правих сазнања дође и да се она у предстојећем периоду искористе за спречавање нових катастрофалних поплава које би могле да угрозе Републику Србију и њене грађане.

У Србији се критична инфраструктура помиње и у оквиру поглавља 6.2. "*Стратегије развоја информационог друштва у Републици Србији до 2020*"[606] кроз констатацију: "Потребно је развијати и унапређивати заштиту од напада применом информационих технологија на критичне инфраструктурне системе, што поред ИКТ система могу бити и други инфраструктурни системи којима се управља коришћењем ИКТ, попут електро-енергетског система. У вези са тим је потребно додатно уредити критеријуме за утврђивање критичне инфраструктуре са становишта информационе безбедности, критеријуме за карактеризацију напада применом информационих технологија на такву инфраструктуру у односу на класичне облике напада, као и услове заштите у овој области".

Документи који би требало да обрађују питања КИ, сем самог Закона о заштити критичне инфраструктуре, су *Национална стратегија заштите и спасавања у ванредним ситуацијама* и Закон о ванредним ситуацијама. Друга два документа јесу усвојена, међутим, у њима се ни не помиње критична инфраструктура, барем не постоји као термин, мада се закони по својој природи баве питањима који су везани за заштиту КИ.

Треба нагласити да институционални оквири за дефинисање КИ постоје**,** а то су постојање Сектора за ванредне ситуације, надлежних министарстава као и надлежних регулаторних тела. Одређене мере заштите делова инфраструктуре су предузете од

[605] Lane, J. E. (2012), Државно управљање – разматрање модела јавне управе и јавног управљања, Београд, стр. 173.
[606] Влада Републике Србије, "Стратегија развоја информационог друштва у Републици Србији до 2020", 2010

стране оператера, али нису донесене ни стратегија ни политика заштите на нивоу земље.

Потреба разматрања КИ препозната је у оквиру пројекта "Управљање критичном инфраструктуром за одрживи развој у поштанском, комуникационом и железничком сектору Републике Србије". Основни циљ пројекта је идентификација критичних инфраструктурних система чија је ефикасност кључна за неометан развој економије и друштва.

8.3. Критични сектори

Пошто у Србији још увек не постоји закон о критичним инфраструктурама и оне нису јасно дефинисане може се предложити модел заснован на постојећим поделама критичних инфраструктура у суседним земљама, у складу са просторно-географским, привредним, економским и демографским карактеристикама. Издвајањем оних инфраструктура које се појављују у Бугарској и Словенији, земљама са дефинисаном политиком заштите критичне инфраструктуре, добија се следећи предлог критичних инфраструктура у Србији:

- Енергетика (производња дистрибуција и складиштење енергената (гаса и нафте) и електричне енергије),
- Информационе и комуникационе технологије (електронска комуникација, пренос података, информациони системи, пружање аудио и мултимедијалних услуга),
- Саобраћај (друмски, железнички, ваздушни, водни),
- Здравство (болнице, производња лекова),
- Воде (снабдевање пијаћом водом, бране, обрада отпадних вода, заштита вода),
- Храна (производња, снабдевање храном, безбедност хране, робне залихе),
- Финансије (банкарство, берзе, инвестиције, системи осигурања и плаћања) и
- Јавне службе (очување јавног реда и мира, заштита и спасавање, хитна медицинска помоћ).

Наравно, ово је само предлог заснован на искуствима других држава. Да би се са сигурношћу оформила листа критичних инфраструктура неопходно је да се, на основу једног од модела који су претходно описани, кроз сарадњу са свим релевантним

секторима и институцијама (приватним и државним) утврди степен критичности сваке инфраструктуре, па након тога оформи и коначна листа критичних инфраструктура.

8.3.1. Преглед предложених сектора критичне инфраструктуре у Србији

Енергетску привреду Србије[607] у најширем смислу сачињавају нафтна и гасна привреда, рудници угља, електроенергетика и децентрализовани системи градских топлана и индустријске енергетике. У оквиру енергетског система обавља се експлоатација домаће примарне енергије, увоз примарне енергије (пре свега нафте и природног гаса), производња електричне и топлотне енергије, експлоатација и секундарна прерада угља, као и транспорт и дистрибуција енергије и енергената до крајњих потрошача финалне енергије.

Према већ наведеном, енергетску привреду Србије у најширем смислу чине:[608]

Сектор нафте у оквиру којег се врши експлоатација домаћих резерви нафте, обавља увоз, транспорт и прерада сирове нафте и нафтних деривата, као и дистрибуција и продаја/извоз деривата нафте. У области домаћег истражног и екплоатационог простора нафте и гаса присутан је стални пад производње који је последица малог нивоа улагања у одржавање постојеће производње, као и малог интензитета истражних радова због недостатка сопствених средстава. Транспорт нафте се доминантно врши магистралним нафтоводом (Јанаф) од Омишља у Хрватској до рафинерија нафте у Панчеву и Новом Саду. Укупни инсталисани прерађивачки капацитет домаћих рафинерија износи 7,8 милиона тона годишње (4,8 милиона тона у Панчеву и 3 милиона тона у Новом Саду).

Сектор природног гаса у оквиру кога се осим увоза гаса, обавља експлоатација домаћих резерви природног гаса, њихова примарна прерада, сакупљање, транспорт и дистрибуција до крајњих потрошача гаса. На главни магистрални гасовод, укупне дужине око 400 км, који се простире од границе Мађарске до Ниша, повезан је већи број дистрибутивних мрежа преко којих се врши снабдевање потрошача природним гасом. Велика већина ових мрежа изграђена је на територији Војводине.

Сектор угља у оквиру којег се врши експлоатација и прерада угља из рудника са површинском експлоатацијом у три рударска басена: Колубарски, Костолачки и Косовско-Метохијски, који не функционише у саставу енергетског система Србије. Преко 95% укупне производње угља на површинским коповима користи се за

[607] Егзактни подаци преузети су из Стратегије за развој енергетике Републике Србије до 2015.
[608] Ibid

производњу електричне енергије. За финалну потрошњу користи се угаљ из осам рудника са подземном експлоатацијом, у којима се врши експлоатација каменог и мрког угља, као и знатно квалитетнијег лигнита (у односу на лигните из рудника са површинском експлоатацијом угља).

Електроенергетски сектор сачињавају објекти/системи:

- Електроенергетски извори, у које спадају електране (термоелектране на лигнит, термоелектране на мазут и природни гас),
- Системи за пренос електричне енергије, са око 10.200 км далековода и са трафостаницама, преко кога се врши пренос електричне енергије произведене у земљи и обавља размена са суседним системима,
- Електродистрибутивни системи, лоцирани у потрошачким центрима преко којих се врши испорука електричне енергије крајњим потрошачима у секторима потрошње енергије.

Систем градских топлана постоји у 45 градова Србије, чине га децентрализовани топлотни извори и одговарајуће дистрибутивне мреже. Систем се користи за загревање стамбеног и пословног простора, обима од око 450.000 еквивалентних станова (површине 66 м^2).

Основна карактеристика свих наведених делова енергетског система је у великом броју случајева технолошка застарелост и ниска енергетска ефикасност, као и тренутно забрињавајуће и дугорочно неприхватљиво технолошко стање са становишта заштите животне средине.

Сектор информационе и комуникационе технологије, односно ИКТ сектор чине *предузећа којима су ИКТ доминантна делатност* и која су по својој структури претежно мала и средња приватна предузећа. Ту су информациони центри у великим привредним системима са израженом развојном функцијом у области информационо комуникационих технологија. У прошлости су управо ти велики информациони центри у великим системима били ослонац информатизације у Србији. Касније, у процесу транзиције дошло је до стварања низа других малих и средњих приватних предузећа у тој области.

Битан елемент ИКТ сектора су и *универзитети и институти, као и научно-истраживачки центри*, *технолошки паркови и инкубатори* итд. који представљају спој универзитета и имплементације у привреди.

Оно што је упечатљиво јесте да је број предузећа, претежно приватних, која се баве софтверским услугама врло велик, што на неки начин разбија уобичајено мишљење о стању ИКТ у Србији. Подаци потписани и уговор о сарадњи са Мајкрософтом, и низ договора са представницима компанија *Cisco*, *IBM*, *Hewlett Packard*, *Oracle*, *Apple* и *Google Enterprise* показују да је ИКТ врло важан сегмент српске привреде. Битан је развој софтвера, развој рачунарских машина, производња рачунарских машина, систем интеграције и хардвера и софтвера. Наравно, телекомуникације такође играју важну улогу у оквиру ИКТ сектора, као и сви сегменти, подгрупе у области телекомуникационих технологија.

Кад је у питању област увоза и извоза, извоз у ИКТ сектору у Србији нагло расте из године у годину још од 2000. године, што значи да је извозни потенцијал ИКТ сектора огроман. Извештај тржишне анализе кретања ИКТ сектора у Србији, извршене од стране компаније *IDC*, говори о врло високој годишњој стопи раста ИКТ сектора од 18,3% и пројектованом петогодишњем расту од 16,8 % годишње.[609]

Интересантна је регионална расподела ИТ сектора у Србији. Концентрација ИТ фирми је пре свега у Београду, Војводина је заступљена са 15% (мада Војводина има јако високу стопу раста броја фирми ИКТ сектора), Ниш − као некада традиционални и основни центар развоја информатике у Србији − заступљен је са 13%, а остали градови са 16%.[610] Предности ИКТ сектора у Србији су, пре свега, квалитетни кадровски ресурси који су још увек присутни у Србији, затим висок технолошки ниво, који не заостаје за светским трендовима, висок степен знања и вештина коришћења ИКТ технологија. Чињеница је и да стране компаније сматрају да су српски кадрови креативни, флексибилни и врло пријемчиви за савремене трендове у информационим технологијама. Оно што је јако важно јесте међународна конкурентност индустрије софтвера: неценовна конкурентност, базирана на квалификованој радној снази, и ценовна конкурентност.

С обзиром на то да у свету више не важи подела на Исток и Запад, него подела на дигитално развијене, односно на информациона друштва и она друга, Србија у овом сегменту не заостаје за светом. Развој и примена информационих технологија је у пуној експанзији и ефекти и сви елементи глобализације директно се осликавају, а можда и бивају потпомогнути применом информационо-телекомуникационих

[609] http://www.idc.com 10.02.2013
[610] Медаковић, Р., (2007), (ИТ сектор Привредне коморе Србије), *ИКТ индустрија као доминантна привредна грана у Србији*, часопис Е-волуција.

технологија. У свету је нормално да компјутерски писмени људи имају могућност квалитетнијег запошљавања, тј. постоји потреба коришћења технички високообразованог кадра и радне снаге. Чињеница је да мала почетна инвестициона улагања за разлику од других сектора привреде иницирају појаву нових иновативних фирми старт-ап компанија. Ничу мала предузећа која су флексибилна и која могу да одговоре на захтеве једног фрагментираног и разноврсног тржишта. То је тржиште наменског софтвера и услуга које управо омогућава широк спектар могућности за рад малим фирмама односно компанијама. Такође, светске прилике омогућавају да чак и малим предузећима буду доступна страна тржишта управо коришћењем веза, канала и контаката на међународном тржишту посредством интернета и информационих технологија.

С друге стране, велике и мултинационалне компаније имају другу филозофију, која се заснива на томе да одржавају своју конкурентност и рејтинг на тржишту, користећи се решењима која су врло рестриктивна и квалитетна, али по нижој цени. Да би то постигли, фокусирају се на земље у транзицији, као што је Србија,[611] где по релативно нижим ценама могу да *аутсорсују* своју производњу уз постизање жељеног квалитета. Тренутно је у Србији присутан знатан број великих мултинационалних компанија из ИКТ сектора, које врше и значајну улогу трансфера технологије.

ИКТ тржиште у Србији има тренд раста који се може поредити са било којом земљом у региону. Чињеница је да главно ИКТ тржиште у Србији представљају, односно највећа очекивања су од е-Владе, од е-локалне самоуправе и уопште сектора *Владе*. Затим, ту су *инфраструктурни привредни системи, јавна предузећа, успешни привредни системи, али и мала и средња предузећа* која су оријентисана на савремене пословне моделе пословања.

Саобраћај и транспорт у најширем смислу чине:[612]

---

[611] Пример је поменути уговор који је потписан са Мајкрософтом, као и разговори са водећим светским фирмама из ИКТ сектора:
http://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:433144-Dacic-u-SAD-sa-predstavnicima-najvecih-svetskih-IT-kompanija 10.02.2013, као и:
http://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:433290-Dacic-Promenjena-slika-o-Srbiji-u-svetu 10.02.2013

[612] Највећи део нумеричких података преузет је са сајта Министарства саобраћаја (http://www.ms.gov.rs, 10.02.2013) и из званичних докумената (Актуелни Закони о саобраћају и стратегија развоја транспорта до 2015), међутим, документи се врло често позивају на податке који су још из '90-их година (вероватно јер се од тад није озбиљно радило на модернизацији саобраћајне инфраструктуре) па је под великим знаком питања колико и у којим сегментима су подаци релевантни данас (нпр. колико је локомотива, бродова у употреби тренутно, колики је укупни карго саобраћај у лукама у Србији и сл.). Ово се посебно односи на водни и на железнички транспорт, делимично на друмски.

Друмски транспорт са укупном дужином путева од око 38.000 км. Мрежа путева у Републици Србији је добро развијена, мада је њен квалитет врло лош због недостатка инвестиција и недовољног одржавања. На територији Републике Србије се налази 792 км путева Коридора 10 са његовим крацима − 10b и 10c.

Рехабилитација путева започета је 2001. године и процењује се да је за започету реконструкцију мреже потребно још око 600 милиона евра. За рехабилитацију и одржавање мреже државних и локалних путева у наредних десет година биће потребно око 6,2 милијарди евра.[613] Недостатак средстава за модернизацију и одржавање путне мреже уз застарео возни парк утицао је на значајно смањење безбедности саобраћаја на путевима.[614]

Друмски транспорт у Републици Србији представља динамичан и доминантан вид саобраћаја који учествује са око 80% у укупном обиму превезеног терета, односно са око 74% у укупном броју превезених путника. Привредни субјекти који обављају друмски транспорт, а који су били у друштвеној својини, углавном су приватизовани и функционишу у условима слободне конкуренције, а улога државних органа је ограничена на уређивање ове области у смислу издавања лиценци, дозвола за друмски превоз, надзор, итд. Међународни друмски транспорт у Републици Србији, односно приступ међународном транспортном тржишту, већим делом се обавља у режиму квота билатералних и мултилатералних ЦЕМТ дозвола што додатно, у условима постојања значајних административних и физичких препрека (нпр. још увек неоповољан визни режим за професионалне возаче, застоји на граничним прелазима и сл.), има негативан утицај на конкурентност наших превозника на међународном транспортном тржишту.

Управљање мрежом државних путева је претежна делатност Јавног предузећа *Путеви Србије*, док мрежом општинских путева и улица управљају органи јединица локалне самоуправе.

Јавни градски и приградски превоз путника обухвата друмски, железнички и водни превоз. Уређивање јавног градског и приградског превоза путника је у надлежности органа јединице локалне самоуправе.[615]

Јавни превоз путника у градским подручјима је значајно већи у односу на ванградска подручја. Око две трећине путовања обавља се средствима јавног градског

[613] Стратегија развоја друмског, железничког, водног, ваздушног и интермодалног транспорта у Републици Србији 2008–2015.
[614] Ibid
[615] Ibid

и приградског превоза путника док само трећину чине међумесна путовања. Више од трећине становништва Републике Србије живи у шест највећих градских насеља и у њима се реализује око 95% путовања. Значајније учешће у јавном градском и приградском превозу путника железница има само у Београду (Беовоз).

Железнички трансорт преко магистралне железничке пруге пролази кроз све веће градове и укршта се у зонама Београда и Ниша. Од укупне дужине железничке мреже у Републици Србији (3.809 км), 1.768 км представљају магистралне пруге, а електрифицирано је 1.247 км (32,7%).

Само 7% пруга (276 км) има два колосека. Просечно задовољавајућа густина мреже на нивоу Републике Србије веома је неравномерна и осетно опада ка југу.

Недовољно улагање у основно одржавање на железници последица је општег привредног заостатка у претходном периоду, лоше организације, недостатка средстава, социјалне и кадровске политике. Садашње стање железничке инфраструктуре карактерише потреба да се у пројектовано стање врати и модернизује још око 1.000 км магистралних пруга, тј. око 57% главне мреже пруга, односно 26% комплетне железничке мреже. За рехабилитацију и одржавање железничке мреже у наредних десет година према проценама биће потребно око 3,9 милијарди евра.

Управљање јавном железничком инфраструктуром, јавни превоз путника и робе и одржавање железничких возних средстава су претежне делатности ЈП *Железнице Србије*.

Дирекција за железнице је образована као посебна организација ради обављања стручних, регулаторних и других послова у области железничког транспорта утврђених Законом о железници.[616]

Водни транспорт. Република Србија има повољне економске и географске карактеристике за теретни, путнички и туристички водни транспорт. Потенцијали река и канала су значајни, али стање инфраструктуре није задовољавајуће. После 1990. године дошло је до великог застоја у одржавању унутрашњих водних путева и пратеће инфраструктуре.

За рехабилитацију и одржавање система унутрашњег водног транспорта у наредних десет година према проценама биће потребно око 290 милиона евра, а додатних око 220 милиона евра потребно је за развој интермодалног транспорта.

[616] "Службени гласник РС", број 18/05

Превоз путника на унутрашњим пловним путевима у Републици Србији има пре свега туристички карактер. Број путника-туриста који на својим речним крстарењима посећују Републику Србију значајно расте сваке године и представљаће основу за развој значајне привредне активности у областима транспорта, туризма, трговине и других услуга.[617]

Очекује се да ће са обнављањем и повећањем производње у великим индустријским постројењима у Републици Србији (челичане, хемијска индустрија, цемент, нафта) тражња за водним транспортом робе значајније порасти због његових компаративних предности.

Ваздушни транспорт у Републици Србији посматран је у односу на *аеродроме*, *авио-компаније*, *Директорат цивилног ваздухопловства Републике Србије* и *Агенцију за контролу летења.*

Авио-компаније. Јавно предузеће *AIR Serbia*[618] основала је Република Србија, са компанијом *Etihad* из Уједињених арапских емирата, за обављање делатности превоза путника и робе.

Директорат цивилног ваздухопловства државе Србије и државе Црне Горе основан је у октобру 2003. године ради обезбеђивања услова за несметано обављање послова од значаја за остваривање права и дужности у области ваздушног транспорта и примене међународних стандарда и препорука у тој области. Након престанка државне заједнице Србија и Црна Гора, Република Србија је преузела оснивачка права у Директорату и промењен му је назив у Директорат цивилног ваздухопловства Републике Србије.

У току 2005. године Србија и Црна Гора примљена је у чланство EUROCONTROL-а и JAA (*Joint Aviation Authorities*). У току 2006. године потписани су Мултилатерални споразум о успостављању Заједничког европског ваздухопловног подручја и Споразум о одређеним аспектима ваздушног транспорта тзв. *хоризонтални споразум*.

---

[617] Податак је преузет из стратегије развоја транспорта до 2015. године, међутим, оно што противречи логици је чињеница да туризам тешко може да буде "*основ за развој значајне привредне активности у областима транспорта, туризма, трговине и других услуга*", већ би могао да буде само основ за развој туризма, док је за прави развој привреде, транспорта и трговине неопходан развој лука, опремање лука за руковање контејнерима и карго теретом уопште, и развој индустрије (или реиндустријализација како се популарно назива процес улагања у развој конкурентности српске индустрије)

[618] Од 8. августа 2003. име националног авиоревозника није акроним од *Југословенски аеротранспорт* већ заправо пуно име компаније (назив JAT задржан је тада као бренд):
http://www.jat.com/active/sr-latin/home/main_menu/about_us/history.html 10.02.2013

У циљу развоја и унапређења безбедности ваздушног саобраћаја наставља се интензивна сарадња са међународним организацијама у области цивилног ваздухопловства, тј. са ICAO (*International Civil Aviation Organization*), EUROCONTROL, ECAC (*European Civil Aviation Conference*) и JAA.

Агенција за контролу летења Србије и Црне Горе има задатак контроле летења изнад територија Србије и Црне Горе у циљу безбедног, редовног и ефикасног одвијања ваздушног транспорта. У оквиру Агенције послују Центар за обуку контролора летења и другог стручног особља, за сопствене потребе као и за потребе других провајдера, и Служба за калибражу која пружа услуге провере исправности рада навигационих уређаја из ваздуха.

Агенција пружа навигацијско, метеоролошко и техничко обезбеђење ваздушног транспорта у ваздушном простору Републике Србије, Републике Црне Горе, 55% горњег ваздушног простора Босне и Херцеговине, као и међународних вода јужног дела Јадранског мора.

Интермодални транспорт. Поред чињенице да је током деведесетих година интермодални транспорт био у прекиду, постоји делимично изграђена инфраструктура, како на железници − Железнички интегрални транспорт, тако и у лукама (луке у Новом Саду, Београду, Панчеву и Прахову) за претовар контејнера. Код постојећих терминала присутна су значајна ограничења условљена постојећом локацијом, застарелом опремом и расположивим инвестицијама за развој. Такође, више пута дефинисана мрежа терминала и стратешки планови развоја нису реализовани.

Комбиновани друмско-железнички транспорт на железници се последњих година постепено обнавља и у благом је порасту.

Промет интермодалних транспортних јединица у лукама је протеклих година био мали, од четири луке које располажу контенерским терминалима у 2003. години забележен је промет контенера само у луци Београд (2200 TEU[619]) и у луци Дунав Панчево (500 TEU).

Здравство је веома значајно, посебно током ратних конфликата, масовних миграција, политичке и економске нестабилности. Међутим, квалитет здравствене заштите као и инфраструктуре везане за здравство у Републици Србији постао је неадекватан. Ни промена власти 2000. године, као ни све што се након тога издешавало до данас, није довело до неких значајних побољшања ситуације у здравству.

[619] TEU - *twenty-foot equivalent unit*, Јединица еквивалента двадесет стопа - Један ТЕУ представља капацитет робе стандардног ИСО контејнера, 20 стопа (6.1 м) дугачког и 8 стопа (2.44 м) широког.

Здравствени систем у Србији пати од недостатка средстава и инвестиција, али обезбеђује основну услугу грађанима.[620]

Приватни здравствени сектор је развијен, али није и инкорпориран у национални здравствени систем.

Вода. Проблем заштите воде као критичног инфраструктурног сектора у Србији је све већи, а степен загађења речних токова и пијаћих извора се из дана у дан повећава.

Растуће потребе за водом у претходним деценијама допринеле су ставу да ће вода бити ограничавајући фактор развоја човечанства, али и опстанка људи у водом најсиромашнијим деловима света. Већина река у развијеним земљама постале су само канали отпадних вода, које чак и превазилазе капацитете самог воденог тока. Разградња отпадних материја веома је успорена, па је количина кисеоника потребног живим бићима у њој вишеструко смањена. Код нас је све већи број *одумирућих* река, док је на неким токовима стање толико лоше да живота у њима готово и да нема.

Кључни извори загађења река у Србији су непречишћене индустријске и комуналне отпадне воде. Око 50% загађења испуштеног у реке долази од индустријских постројења, а само 13% комуналних отпадних вода се третира пре испуштања.[621]

Велики загађивач вода Србије су и неуређене депоније. Вода и отпад су чврсто повезани, јер сваки отпад доспева и до подземних вода. Последице небриге због неодговарајућег одлагања отпада све се више осећају, а бројни извори су већ загађени. Подземне воде загађује и претерана употреба вештачког ђубрива, а из године у годину број пољопривредика који користе штетне пестициде и супстанце отровне за природу све је већи.

Основни начин да се повећа квалитет вода и да се воде заштите је елиминисање и контролисање њихових загађивача, док би истовремено велики произвођачи морали да поведу рачуна о својим отпадним водама и адекватно их пречисте пре испуштања у природу.

Пошумљавање планинских површина би значајно помогло у очувању здраве воде, а веома ефикасан начин је и изградња површинских акумулација и малих брана.

[620] Списак свих здравствени установа у Србији може се наћи на сајту Републичког фонда за здравствено осигурање: http://www.rfzo.rs/ 10.02.2013

[621] Податак са сајта јавног водопривредног предузећа СРБИЈАВОДЕ, http://www.srbijavode.rs 10.02.2013

Храна и пољопривреда.[622] Србија се налази на површини од укупно 8.840.000 хектара. Површина пољопривредног земљишта обухвата 5.734.000 хектара (0,56 ха по становнику), а на око 4.867.000 хектара те површине простире се обрадиво земљиште (0,46 ха по становнику). Око 70 одсто укупне територије Србије чини пољопривредно земљиште, док је 30 одсто под шумама.

Финансије. Као главни актери у финансијском сектору Републике Србије години означени су: банке, друштва за осигурање, брокерско дилерска друштва, даваоци финансијског лизинга, друштва за управљање добровољним пензијским и инвестиционим фондовима, затворени и приватни инвестициони фондови и друге финансијске институције. Главни носиоци финансијског система су банке, што је, између осталог, последица недовољне развијености сектора осигурања и тржишта капитала, као и оскудног коришћења лизинга као облика финансирања.[623]

Јавне службе. У контексту овог сектора могао се и већи део организација које обављају послове државне управе означити као критичан, што се у неким државама и ради, али се овде због једноставности разматрања узимају само службе које су апсолутно неопходне за функционисање друштва у кризним ситуацијама и које су битан интегрални део кризног менаџмента. Јавна служба је организована делатност у државном или приватном власништву која служи за задовољење важних животних потреба шире социјалне заједнице.[624]

У модерним, развијеним земљама појам јавних услуга обично обухвата:

- образовање,
- дистрибуцију електричне енергије и гаса,
- заштиту од пожара,
- здравство,
- полицију,
- чистоћу и
- производњу и дистрибуцију воде.

---

[622] Пољопривреда је сектор који је по логици ствари директно и нераскидиво везан за храну. У свим земљама са дефинисаном политиком заштите критичне инфраструктуре се као подсектор у оквиру сектора хране појављује и пољопривреда, а у САД-у читав критични инфраструктурни сектор носи назив храна и пољопривреда (*Food and Agriculture*). Подаци у бројкама налазе се на сајту Владе Републике Србије: http://www.srbija.gov.rs/pages/article.php?id=55 10.02.2013

[623] http://www.economy.rs/finansije/9790/Poslovanje-finansijskih-institucija-u-Republici-Srbiji-2012--godine.html
10.02.2013.

[624] Управно право Републике Србије.

У највећем броју случајева јавне услуге су услуге, тј. оне не подразумевају производњу добара (као што су шрафови и матице). Могу их пружати локални или национални монополи и то нарочито у областима у којима постоје природни монополи. Њихови резултати тешко се могу приписати одређеном индивидуалном напору и тешко их је оценити по квалитету. Оне обично подразумевају висок ниво обучености и образовања запослених.

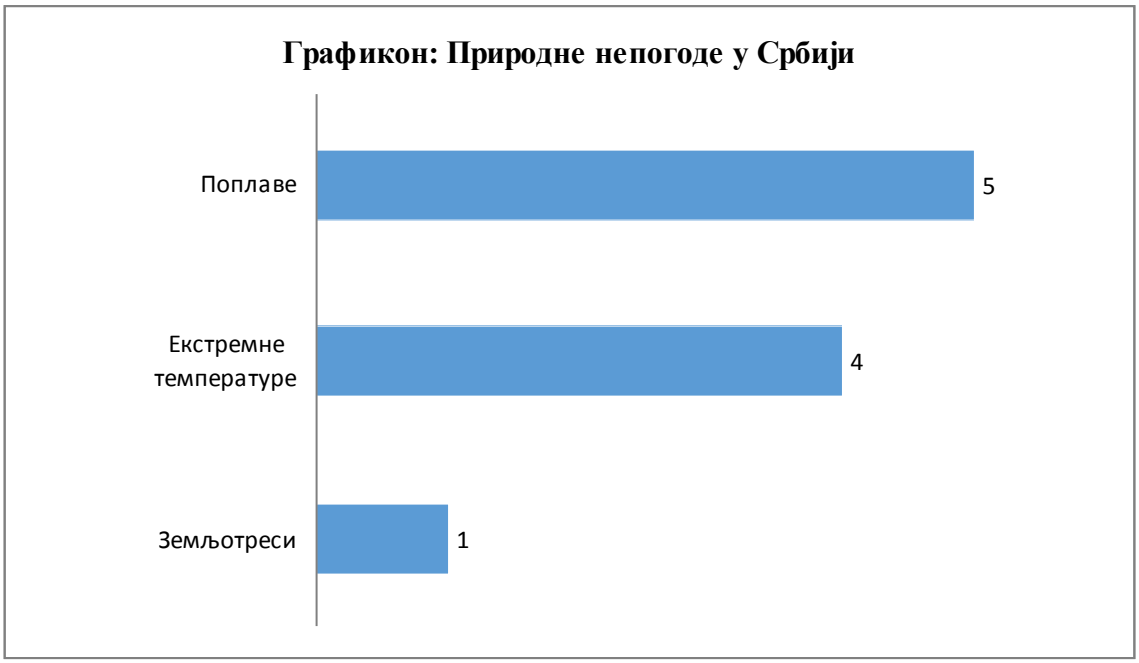
8.4. Доктринарни, стратегијски и законски оквир - идентификација проблема и предлог мера

У ***Стратегији националне безбедности*** Србије из априла 2009. године помињу се у поглављу 2 *изазови, ризици и претње безбедности*. За те *изазове, ризике и претње*, у стратегији се наравно не каже децидирано да су претње по критичне инфраструктуре, али се могу препознати ризици који директно утичу на КИ. Након изнетих ризика ни у ком контексту се у стратегији не помиње заштита критичних инфраструктура. У Стратегији стоји да је "полазни критеријум у разматрању и навођењу изазова ризика и претњи јесте тежина последица по безбедност Републике Србије које би могле да настану у случају њиховог испољавања". То практично значи да ниједан од критеријума који су навођени раније, а који су везани за идентификовање претњи по КИ (главе 3.4.2. и 3.4.3) као и за утврђивање критичности инфраструктура нису узимани у разматрање, па и сам преглед *изазова, претњи и ризика* треба посматрати само као почетак будућег рада на заштити КИ.

Након Стратегије националне безбедности из 2009. године, 2011. су донети Закон о ванредним ситуацијама (донет 2009, а допуњен је амандманима 2011. и 2012. године) и Национална стратегија заштите и спасавања у ванредним ситуацијама.

Природне катастрофе	Србија
Број догађаја	10
Број настрадалих	9
Просечно настрадалих по години	0
Број погођених	48,010
Просечно погођених по години	1,549
Економска штета (у хиљадама $)	132,260
Економска штета по години (у хиљадама $)	4,266

Табела 8.1. - Преглед природних катастрофа у Србији (1980-2010)



Извор: Natural Disaster Occurence Reported,
http://www.preventionweb.net 23.02.2015.

Законом о ванредним ситуацијама[625], као што је претходно речено, регулишу се деловање, проглашавање и управљање ванредним ситуацијама, систем заштите и спасавања људи, материјалних и културних добара и животне средине од елементарних непогода, техничко-технолошких несрећа − удеса и катастрофа, последица тероризма, ратних и других већих несрећа, надлежности државних органа, аутономних покрајина, јединица локалне самоуправе и учешће полиције и Војске Србије у заштити и спасавању, затим права и дужности грађана, привредних друштава, других правних лица и предузетника у вези са ванредним ситуацијама, деловање организација и делатност цивилне заштите на заштити, спасавању и отклањању последица елементарних непогода и других несрећа, регулишу се финансирање, инспекцијски надзор, међународна сарадња и друга питања од значаја за организовање и функционисање система заштите и спасавања. Све горе наведено има за циљ изградњу јединственог система заштите и спасавања у складу са овим Законом и другим прописима, као и програмима, плановима и другим документима који се односе на заштиту и спасавање и цивилну заштиту.

Законом је предвиђено постојање система осматрања, раног упозоравања,

[625] "Службени гласник " Републике Србије, број 111/09, 92/2011 и 93/2012.

обавештавања и узбуњивања. У Закону се наводи да је основни задатак система осматрања, раног упозоравања, обавештавања и узбуњивања откривање, праћење и прикупљање података о свим врстама опасности које могу угрозити људе, животну средину, материјална и културна добра. Имаоци телекомуникационих система и средстава дужни су да служби 112 (112 је законом предвиђени интегрисани број свих хитних служби) омогуће приоритетно коришћење веза у ванредним ситуацијама.

Оно што је такође специфично за овај Закон је и чињеница да има посебно прописане норме и правила деловања у случају криза са прекограничним последицама, где се указује на правила међународне сарадње у разрешењу криза. Овај део Закона подсећа на оно што ЕУ од својих чланица тражи да усвоје кад је у питању заштита европске критичне инфраструктуре, која се може дефинисати и као транснационална инфра-структура, јер су ефекти њеног отказивања такође прекогранични.

Законом се дефинишу (што је јако битно за ефикасно решавање криза) буџетски фондови из којих ће се финансирати све акције везане за ванредне ситуације и за обуку свих релевантних учесника. Тако се на државном нивоу планира да се систем заштите и спасавања финансира из буџета Републике Србије (буџета јединица територијалне аутономије и буџета јединица локалне самоуправе), затим из посебног Фонда за ванредне ситуације, као и преко других прихода у складу са Законом. Законом су, на крају, предвиђене и казнене одредбе, које важе за све оне које на било који начин спрече или ометају ефикасно функционисање механизама реаговања током ванредне ситуације. Казнене одредбе посебно су дефинисане за физичка, а посебно за правна лица.

Закон предвиђа доста ситуација и начина реаговања, уређена је хијерархија у одлучивању, дефинисано (барем оквирно) финансирање акција у ванредним ситуацијама, као и финансирање обука и набавке опреме, дефинисана међународна сарадња у случају криза које имају прекограничне последице, а и у случају локалних криза. Такође, Закон пропагира сарадњу приватног и јавног сектора, што је опет јако битан фактор заштите КИ о чему се раније у овом раду говорило. У Закону се не помиње критична инфраструктура, али сам Закон представља јако добру основу за развој закона о заштити критичне инфраструктуре и свих осталих закона који из њега произилазе. Проблем са којим се Србија, као и све земље у региону, скоро по правилу сваке године сусреће су шумски пожари на планинама и у тешко приступачним зонама.

Национална стратегија заштите и спасавања[626] комплементарна је са Законом

[626] Стратегија је објављена у "Службеном гласнику" Републике Србије, бр. 86/2011 од 18.11.2011.

о ванредним ситуацијама. Као образложење за усвајање и спровођење стратегије наведено је да је регион југоисточне Европе све више угрожен разним врстама природних опасности (поплаве, суше, екстремно високе температуре, земљотреси, клизишта, олујне непогоде, итд.), техничко-технолошким несрећама, дејством опасних материја и другим стањима опасности. Глобалне климатске промене такође доприносе уништавању животне средине, са штетним утицајем на здравље људи, опстанак многих природних врста и културно наслеђе. Национална стратегија заштите и спасавања обухвата системе превенције, ублажавања, заштите и спасавања и обнове. Основ за спровођење Националне стратегије како се наводи у Стратегији "садржан је у Закону о ванредним ситуацијама којим је дефинисано успостављање интегрисаног система заштите и спасавања. Поред законодавног оквира, основ за израду Националне стратегије садржан је и у другим националним и међународним документима, као што су: Национални програм за интеграцију Републике Србије у Европску унију, Национална стратегија одрживог развоја, Стратегија националне безбедности Републике Србије, Миленијумски циљеви развоја, које су дефинисале чланице Уједињених нација и Хјого оквир за деловање 2005−2015: Развој отпорности нација и заједница на катастрофе".

У Стратегији су приказани резултати анализе недостатака постојећег система заштите и спасавања. Уочени недостаци су подељени у неколико категорија:[627]

1. **Институционлано-организациони**:
    - Непостојање услова за доследну примену прописа,
    - Неодговарајућа организација и спровођење превентивних мера,
    - Недоступност специјализованих катастара,
    - Непостојање свеобухватних мапа ризика,
    - Неравномерна расподела капацитета служби за реаговање на територији Републике Србије,
    - Неуспостављен систем 112,
    - Непостојање методологије управљања опасним отпадом.
2. **Материјално-технички**:
    - Незадовољавајући ниво саобраћајне и друге инфраструктуре,
    - Застарела, непоуздана опрема, средства и возила служби за реаговање у ванредним ситуацијама,

[627] Ibid

- Неадекватно финансирање одржавања система заштите и спасавања,
- Непостојање специјализованих возила и опреме за реаговање у хемијским удесима у друмском, железничком и речном саобраћају,
- Недовољан број мобилних еко-токсиколошких јединица.

3. **Сарадња, координација и расположивост информација**:
   - Недовољна координација између субјеката система заштите и спасавања у ванредним ситуацијама,
   - Недовољна сарадња између научних и истраживачких институција и директних корисника истраживања,
   - Недовољна сарадња са невладиним и приватним сектором,
   - Потреба за унапређењем међународне сарадње.
4. **Људски ресурси и едукација**:
   - Неадекватна стручна квалификованост и технолошка дисциплина расположивих људских ресурса,
   - Недостатак специјализованих кадрова,
   - Недовољна обученост професионалног кадра,
   - Неприпремљеност и низак ниво капацитета локалне самоуправе,
   - Неразвијена култура превенције.

У оквиру стратегије наводе се стратешке области, дају се објашњења тих области и циљеви који треба да се остваре:

1. **Обезбедити да смањење ризика од катастрофа постане национални и локални приоритет са јаком институционалном основом** – потребно је постићи свеопшти друштвени консензус који укључује како интеграцију смањења ризика од катастрофа у развојне програме и планове, тако и обезбеђење ресурса (људских и финансијских) неопходних за спровођење тих планова и програма и успостављање интегрисаног система заштите и спасавања.
2. **Идентификовати процењивати и пратити ризике и побољшати системе раног упозоравања** – основа за смањење ризика од катастрофа и повећање културе отпорности на катастрофе састоји се у познавању опасности као и физичких, друштвених, економских и еколошких угрожености са којима се суочавају поједине заједнице и друштво у целини, и начина на које се те

опасности и осетљивости краткорочно и дугорочно мењају, те деловање у складу са тим знањем.

3. **Користити знање, иновације и образовање у циљу изградње културе безбедности и отпорности на свим нивоима** – последице катастрофа могу се знатно смањити уколико су грађани добро и адекватно информисани о ризицима са којима се могу суочити и о могућим опцијама и мерама које могу предузети у циљу смањења угрожености и боље припреме. У том смислу овде је циљ што боље едуковати јавност кроз разне медије.
4. **Умањити факторе ризика** – планирање одрживог развоја, израда и тестирање одговарајућих стратегија, секторских програма и других планско-програмских докумената и важних за ситуације након катастрофе.
5. **Припремити се за случај катастрофе ради ефикасног реаговања на свим нивоима** – у моменту катастрофе, могуће је знатно смањити последице и губитке ако су надлежни органи, појединци и локалне заједнице у областима угроженим опасностима добро обучени, опремљени и спремни да реагују. Припремљеност може да обухвати разне врсте активности, као што су израда планова за реаговање, стварање залиха опреме и материјала, организација хитних служби, склапање *стенд-бај* уговора, припрема циркуларних саопштења и процедура за управљање информацијама, дефинисање механизама координације, обука и заједничке вежбе јединица и становништва.

Сем наведених стратегија и закона везаних за националну безбедност, ванредне ситуације и заштиту и спасавање у Србији постоји још законских оквира који су директно или индиректно везани за законски још недефинисану заштиту критичне инфраструктуре.

Тако у сектору вода постоји **Закон о водама**[628] из 2010, којим се између осталог прописују мере заштите вода, правила прерађивања, правила утврђивања здравствене исправности воде, али и мере заштите од штетног дејства вода.

У сектору хране постоји **Закон о безбедности хране**[629] који је ступио на снагу 1. јануара 2009. године. Законом се регулише производња воћа и поврћа, употреба хемикалија приликом одгоја, гајење стоке, контрола хране и уводи систем брзог

[628] Закон је објављен у "Службеном гласнику" Републике Србије, бр. 30/10, 7.5.2010.
[629] http://www.mpt.gov.rs/postavljen/123/bezbednost1.pdf 10.02.2013

обавештавања и узбуњивања уз примену хитних мера за управљање кризним ситуацијама.

У оквиру сектора информационих и комуникационих технологија постоји највећи напредак када је реч о усклађивању законске регулативе са европским законима. Тако су у оквиру овог сектора, за који је надлежно Министарство спољне и унутрашње трговине и телекомуникација, усвојени следећи закони и стратегије:

- *Закон о електронским комуникацијама*[630] – овим Законом уређују се услови и начин за обављање делатности у области електронских комуникација, надлежности, државних органа у области електронских комуникација, затим, уређује се положај Републичке агенције за електронске комуникације, прописују се начини спровођења јавних консултација у области електронских комуникација, уређује се управљање и коришћење адреса и бројева, управљање и коришћење и контрола радио-фреквенцијског спектра, дистрибуција и емитовање медијског садржаја, заштита права корисника и претплатника, безбедност и интегритет електронских комуникационих мрежа и услуга, тајност електронских података, законито пресретање и задржавање података, даље се уређују мере за поступање супротно одредбама овог Закона, као и друга питања везана за функционисање и развој електронских комуникација у Србији.
- *Стратегија развоја електронских комуникација*[631] у Србији од 2010. до 2020. године – има велики стратешки значај и треба да постави главне правце и циљеве успешног развоја електронских комуникација у Републици Србији. Стратегија представља прагматичан скуп неопходних мера које би требало да Републици Србији обезбеде повољнију позицију у глобалној економији,
- *Стратегија развоја информационог друштва у Републици Србији до 2020. године*[632] – У оквиру Европске уније (у даљем тексту: ЕУ) ИКТ су препознате као главни фактор утицаја на економски раст и иновативност,[633]

[630] Ступио је на снагу 1. јануара 2012.
[631] "Службени гласник" Републике Србије, бр. 68/10, 02.09.2010.
[632] Усвојена 8. јула 2010.
[633] Annual Information Society Report 2007 – Communication from the Commission to the European parlament, the Council, the European Economic and Social Committee and the Committee of the regions, Bruses, 30th March, 2007

а међу седам водећих иницијатива економске стратегије Европа 2020[634] налази се *Дигитална агенда за Европу*, што показује значај који ИКТ имају у развоју модерне економије. Заједно са стратегијом у области телекомуникација, ова стратегија чини Дигиталну агенду за Републику Србију. Циљ Стратегије је да развој информационог друштва усмери ка искоришћењу потенцијала ИКТ за повећање ефикасности рада, економски раст, већу запосленост и подизање квалитета живота свих грађана Републике Србије. Основне идеје развоја информационог друштва чине: отворен, свима доступан и квалитетан приступ интернету, развијено е-пословање, укључујући: е-управу, е-трговину, е-правосуђе, е-здравље и е-образовање.

- *Стратегија развоја електронске управе у Републици Србији за период од 2009. до 2013. године* − стратегија је акт Владе којим се на целовит начин дефинишу основни циљеви, начела и приоритети унапређења стања у овој области и утврђују активности које треба предузети у наредном периоду. Под изразом *електронска управа* (е-управа), у смислу ове Стратегије, подразумева се примена информационо-комуникационих технологија којом се постиже ефикаснији и ефективнији рад органа управе и ималаца јавних овлашћења у функцији вршења власти, економског раста и смањења терета администрације.
- *Закон о електронском документу* - Електронски документ јесте скуп података којим се уређују услови и начин поступања са електронским документом у правном промету, управним, судским и другим поступцима, као и права, обавезе и одговорности привредних друштава и других правних лица, предузетника и физичких лица, државних органа, органа територијалне аутономије и органа јединица локалне самоуправе и органа, предузећа, установа, организација и појединаца којима је поверено вршење послова државне управе, односно јавних овлашћења у вези са овим документом.
- *Законом о електронској трговини*[635] уређују се услови и начин пружања услуга информационог друштва, обавезе информисања корисника услуга, комерцијална порука, правила у вези са закључењем уговора у електронском

[634] Europe 2020 – A strategy for smart sustainable and inclusive growth, Communication from the Commision, Brusels, 03 March, 2010
[635] "Службени гласник" Републике Србије бр. 41/2009.

облику, одговорност пружаоца услуга информационог друштва, надзор и прекршаји.

- *Закон о електронском потпису* − дефинише електронски потпис као скуп података у електронском облику који су придружени или су логички повезани са електронским документом и који служе за идентификацију потписника. Овим Законом уређује се употреба електронског потписа у правним пословима и другим правним радњама, пословању, као и права, обавезе и одговорности у вези са електронским сертификатима, ако посебним законима није другачије одређено.
- *Правилник о издавању временског жига*[636] донет је на основну Закона о електронском документу, у ком се већ помиње коришћење временског жига. Правилником се прописују услови и поступак регистрације издаваоца временског жига, услови које мора да испуњава систем за формирање временског жига, садржина захтева за формирање временског жига, садржај структуре података временског жига, поступак означавања времена које је садржано у њему, као и садржај и начин вођења Регистра издавалаца временског жига у Републици Србији.
- *Закон о заштити података личности*[637] дефинише да је податак о личности свака информација која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и сл.), по чијем налогу, у чије име, односно за чији рачун је информација сачувана, датум настанка информације, место похрањивања информације, начин сазнавања информације (непосредно, путем слушања, гледања и сл., односно посредно, путем увида у документ у којем је информација садржана и сл.), или без обзира на друго својство информације. Овим Законом се уређују услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог закона. Циљ овог Закона је да, у вези са обрадом података

[636] "Службени гласник" Републике Србије бр. 112/2009.
[637] "Службени гласник" РС, бр. 97/08 и 104/09.

о личности, сваком физичком лицу обезбеди остваривање и заштиту права на приватност и осталих права и слобода.

- *Законом о потврђивању Конвенције о високотехнолошком криминалу*[638] се потврђује Конвенција о високотехнолошком криминалу, настала 23. новембра 2001. године у Будимпешти, којом се као кривични чинови класификују дела против поверљивости, целовитости и доступности рачунарских података и система, незаконит приступ, незаконито пресретање, ометање података, ометање система, злоупотреба уређаја и низ других дела из области превара и других криминалних радњи у оквиру ИКТ сектора, а за која се држава потписница обавезује да ће прописати одговарајуће законске казне.

Кључни проблеми везани за доктринарна и стратегијска документа, као и за законску регулативу у области заштите КИ, као и предлог мера за побољшање стања у овој области, дати су у сублимираној форми у Табели 8.2.

Регулатива	Идентификовани проблеми	Предлог мера
Закон о заштити КИ	• Не постоји закон о заштити и списак КИ	• Донети Закон о заштити КИ
Стратегија националне безбедности Р. Србије	• Не постоји појам КИ у Стратегији националне безбедности Р. Србије	• Иновирати Стратегију
Закон о ванредним ситуацијама	• Не постоји појам КИ • Пропагира, а не дефинише, сарадњу приватног и јавног сектора	• Имплементирати Закон о ВС • Иновирати Закон са одредбама о приватно-јавној сарадњи • Консултовати Закон о ванредним ситуацијама приликом израде Закона о ЗКИ
Национална стратегија заштите и спасавања	• Непостојање услова за доследну примену прописа • Неодговарајућа организација и спровођење превентивних мера	Дефинисати кризни менаџмент за заштиту КИ

[638] "Службени гласник" РС, бр. 19/2009.

Регулатива	Идентификовани проблеми	Предлог мера
	• Недоступност специјализованих катастара • Непостојање свеобухватних мапа ризика • Неравномерна расподела капацитета служби за реаговање на територији Републике Србије • Неуспостављен систем 112 • Непостојање методологије управљања опасним отпадом. • Незадовољавајући ниво саобраћајне и друге инфраструктуре • Застарела, непоуздана опрема, средства и возила службе за реаговање у ванредним ситуацијама, посебно за реаговање у хемијским удесима у друмском, железничком и речном саобраћају • Неадекватно финансирање одржавања система заштите и спасавања • Недовољан број мобилних еко-токсиколошких јединица • Недовољна координација између субјеката система заштите и спасавања у ванредним ситуацијама • Недовољна сарадња између научних и истраживачких институција и директних корисника истраживања • Недовољна сарадња са невладиним и приватним сектором	

Регулатива	Идентификовани проблеми	Предлог мера
	• Потреба за унапређењем међународне сарадње	

Табела 8.2. *Доктринарни, стратегијски и законски оквир - идентификација проблема и предлог мера*

8.5. Организационе структуре и надлежности државних институција - актуелно стање, идентификација проблема и предлог мера

Критичне инфраструктуре у Републици Србији су, у највећој мери, у државном власништву – привредна друштва која имају монополски положај на тржишту роба и услуга, док је мало број привредних друштава у приватном власништву (извршен процес приватизације) или постоје приватне компаније као конкуренција државним (какав је пример у области мобилне телефоније, појединих грана индустрије и делимично авио-саобраћаја). Иако процес (свеукупне) транзиције и потпуног преласка на пословање по условима слободног тржишног привређивања налаже прелазак државне у приватну својину (а што је готово неопходно и са буџетског и макроекономског становишта наше земље), ове активности се споро одвијају. Тако у Србији, готово сви облици КИ постоје и послују као јавна предузећа. Јавно предузеће је предузеће које обавља делатност од општег интереса, а које оснива држава, односно јединица локалне самоуправе или аутономна покрајина.[639] Највећи развојни проблеми концентрисани су у следећим нерентабилним јавним предузећима: Електропривреда Србије (ЕПС), "Железнице Србије'" и "Путеви Србије". Ово показују анализе пословања јавних предузећа Сектора за национални развој Министарства финансија Србије.[640]

Светска економска криза додатно је успорила процес транзиционих реформи у Србији што показују и ЕБРД индикатори. Вредност индекса инфраструктурних реформи ЕБРД (2,3) непромењена је у односу на 2009. годину. У односу на земље у окружењу вредност индекса инфраструктурних реформи у Србији на нивоу је вредности у Црној Гори и БиХ, а нижа од оног у Румунији (3,3); Бугарској, Словенији

[639] Закон о јавним предузећима и обављању делатности од општег интереса, "Службени гласник РС" 25/2000, 25/2002, 107/2005, 108/2005

[640] Bošković, M., Ivković, V., Putnik, N., „Risk Management in Public-Private Partnership over Critical Infrastructures“, u: Dimitrijević, I. (editor), *National Critical Infrastructure Protection – Regional Perspective*, Univerzitet u Beogradu - Fakultet bezbednosti i Institut za korporativnu bezbednost - Ljubljana, Beograd, 2013. pp. 231-243

и Хрватској (3,0) и Македонији (2,7). Србија заостаје за већином земаља у окружењу у области приватизације великих система, управљања и реструктурирања предузећа и спровођења политике конкурентности. Велики број јавних предузећа годинама послује са губитком, а разлози томе могу се наћи у постојању монопола ових привредних друштава на српском тржишту, неадекватној управљачкој структури и неспровођењу унутрашњих процеса модернизације и реструктуирања. Пословање са губитком, менаџменту КИ свакако не оставља простора да и у област управљања ризицима и спровођења превентивних мера континуирано улаже све потребне ресурсе (људске, материјалне и финансијске). Са безбедносног аспекта, ово свакако може представљати проблем и изазов како за саме критичне инфраструктуре, тако и за државу.

Доношење одлуке о приватизацији предузећа од стратешког значаја за државу, тј. КИ, попут: телекомуникација, водовода, електропривреде и сличних, захтева нарочиту пажњу свих релевантних фактора одлучивања. Земље у транзицији су, у већини случајева, преписивале моделе који се примењују у капиталистичким земаљама, па је та пракса примењена и у процесу приватизације. Међутим, чини се да се приватизација у бившим социјалистичким државама понекад одвијала без добро осмишљеног плана. Једна од последица, непланског и неконтролисаног процеса приватизације јесте и изостанак такозваних „паметних приватизација“. Наиме, приватизација се неселективно спроводила па је држава често остајала и без власништва и/или без контроле над предузећима од виталног значаја што је управо супротно од циљева приватизације у капиталистичким државама.[641]

Институционално, законски и финансијски "слабе" државе у транзицији, уз лоше обављене приватизације КИ и са незадовољним становништвом, пред изазовом је одабира адекватног начина изградње снажних и стабилних система, државних служби, привреде и повољних социо-економских прилика. Стога, поред строге поделе на државно и приватно власништво, као и професионално и непрофесионално управљање КИ, своје место све више налази облик такозваног "јавно-приватног партнерства".

Јавно-приватно партнерство (Public-private partnerships – PPP) пре свега је уговорни однос јавног и приватног сектора који може укључивати финансирање, пројектовање, градњу, управљање и/или одржавање инфраструктуре и/или пружање услуга од стране приватног сектора, које традиционално набавља или пружа јавни сектор. Сматра се да предност јавно-приватних партнерства у односу на потпуну

[641] *Ibid.* p. 239.

приватизацију лежи у чињеници да овакав модел комбинује предности које поседује јавни сектор, а које се огледају у јавној/друштвеној одговорности са предностима приватног сектора под којима се подразумевају поседовање финансијских средстава, технологије, знања о професионалном управљању.

"Јавно-приватно партнерство се најшире дефинише као кооперативан, институционални аранжман између јавног и приватног сектора, а за који влада заинтересованост широм света".[642] Једна група аутора PPP посматра као нови инструмент државе којим замењује традиционални модел уговарања обавеза путем тендера у сфери јавних послова и радова, док друга група сматра да је реч само о новом виду изражавања у области јавне управе, а чији је циљ да укључивање приватног сектора у јавне послове подведе под старе, већ устаљене процедуре.

Јавно-приватно партнерство свакако није уговорни облик око чије примене постоји општа сагласност, али могућност његовог реализовања, што је позитивно, изазива јавне и стручне дебате, пажњу менаџера јавних предузећа, конкурентност у приватном сектору, а све то чини да се "данас овај тип односа успоставља у много софистицираније и далекосежније облику него икада пре".[643]

У Републици Србији, међутим, овај уговорни облик још није заживео. Као што је већ поменуто, на основу Закона о ванредним ситуацијама највећи део одговорности за спровођење и координацију активности свих релевантних служби током кризе обавља Министарство унутрашњих послова. Релевантне службе чине професионалци из разних области делатности. Велики део ових релевантних служби интегрисан је у састав Министарства унутрашњих послова, ради лакше координације и успостављања јединственог система одговорности и данас представљају Сектор за ванредне ситуације при МУП-у. Без обзира на то што тренутно не постоји Закон о заштити критичних инфраструктура, као ни списак критичних инфраструктура Србије, када се у неком тренутку буде донео и тај закон, систем функционисања већине служби, а посебно Сектора за ванредне ситуације (као и њихова организација и надлежности) у кризним ситуацијама, вероватно се неће драстично мењати, поготово зато што и без поменутог закона Сектор за ванредне ситуације обавља активности, које би такође биле прописане Законом о ЗКИ (судећи по законима о заштити критичне инфраструктуре у другим земљама). Из тог разлога, Сектор за ванредне ситуације данас представља

[642] Hodge Graeme A., Greve Carsten. Public-Private Partnerships: An International Performance Review, Public Administration Review , 2007, стр. 545

[643] Hodge Graeme A., Greve Carsten. Public-Private Partnerships: An International Performance Review, Public Administration Review , 2007, стр. 544

централно тело током свих кризних ситуација, а вероватно ће и у будућности (када се решавање кризних ситуација буде посматрало у контексту заштите критичне инфраструктуре) бити подједнако важан.

Сектор за ванредне ситуације[644] као специјализована организациона јединица Министарства унутрашњих послова Републике Србије координира све активности државних институција и организација цивилног друштва које су укључене у управљање ванредним ситуацијама на свим нивоима политичко-територијалног организовања. Сектор настоји да изгради, одржи и унапреди способност читаве нације како да превентивно делује на ризике, тако и да одговори на изазове и ублажи последице од различитих катастрофа које могу погодити наш регион. Он обједињује све постојеће ресурсе у заштити, спасавању и реаговању у ванредним ситуацијама.

Од 2006. године организована је модерна Служба која поред *ватрогасаца-спасилаца* у свом саставу има и Управе које се баве *превентивном заштитом*, *управљањем ризицима и цивилном заштитом*. Велики труд улаже се у побољшање организације, јачање људских капацитета и снабдевање опремом у циљу подизања безбедности и смањења броја жртава и материјалне штете.

Сектор за ванредне ситуације обавља послове нормативне, организационо-техничке, управне, превентивне, превентивно-техничке, образовне, информативно-васпитне и друге природе за организовње, планирање, спровођење, контролу мера заштите животне средине, здравља и материјалних добара грађана, очување услова неопходних за живот и припремање за превладавање ситуације у условима пожара, елементарних непогода техничких и технолошких несрећа, дејства опасних материја и других стања, опасности већих размера које могу да угрозе здравље и животе људи и животну средину или да проузрокују штету већег обима и пружање помоћи код отклањања последица (смањивање и санацију) проузрокованих у ванредним ситуацијама, а посебно: израде и предлагање закона, норматива и препорука који испуњавају захтеве Европске уније у области заштите и спасавања у ванредним ситуацијама у циљу потпуног правног уређивања за обављање послова; успостављање институционалних, организационих и персоналних услова за спровођење заштите и спасавања у ванредним ситуацијама, и др.

Седиште Сектора за ванредне ситуације у свом саставу има:

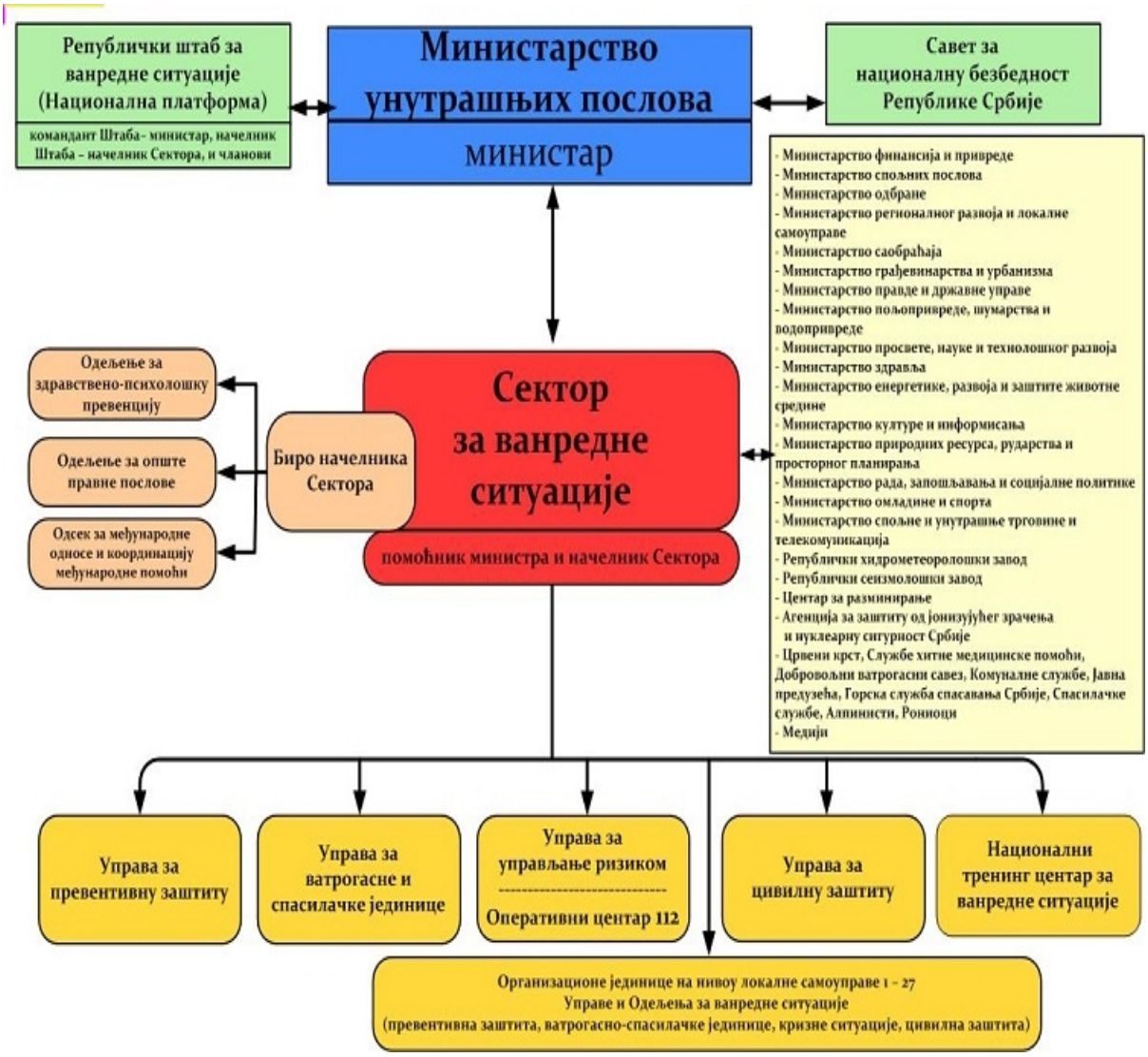
- Биро начелника Сектора,

[644] http://prezentacije.mup.gov.rs/svs/HTML/delatnost.html 10.02.2013

- Управу за превентивну заштиту,
- Управу за ватрогасно-спасилачке јединице,
- Управу за управљање ризиком,
- Управу за цивилну заштиту, и
- Национални центар за ванредне ситуације.

На локалном нивоу, Сектор има 27 организационих јединица:

- четири Управе за ванредне ситуације у Београду, Крагујевцу, Нишу и Новом Саду, и
- 23 Одељења за ванредне ситуације и то у Бору, Ваљеву, Брању, Јагодини, Кикинди, Панчеву, Сремској Митровици, Ужицу, Шапцу, Краљеву, Лесковцу, Новом Пазару, Пироту, Пожаревцу, Прокупљу, Чачку, Пријепољу, Смедереву, Суботици, Сомбору, Зајечару и Зрењанину.



Слика 8.1. – Структура сектора за ванредне ситуације[645]

Биро начелника Сектора у свом саставу има Одељење за опште правне послове, Одељење за здравствено-психолошку превенцију и Одсек за међународне односе и координацију међународне помоћи.

Управа за превентивну заштиту је врло важан функционални део система заштите и спасавања, а формирана је као организациона јединица Сектора за ванредне ситуације у оквиру Министарства унутрашњих послова и има за циљ да обједини све превентивне активности на заштити живота, здравља и имовине грађана.

Управа за ватрогасно-спасилачке јединице учествује у организовању рада Управе и унутрашњих организационих јединица ради благовременог и законитог вршења послова контроле рада ватрогасних и спасилачких једница, индустријских и

[645] http://prezentacije.mup.gov.rs/svs/HTML/organizacija.html 10.02.2013

добровољних ватрогасних јединица, као и њихово координирано деловање у случају већих ванредних догађаја. У свом саставу има: *Одељење за материјално-техничко опремање ватрогасних-спасилачких јединица и Одељење за контролу рада ватрогасно-спасилачких јединица и Одељење за координацију оперативних активности.*

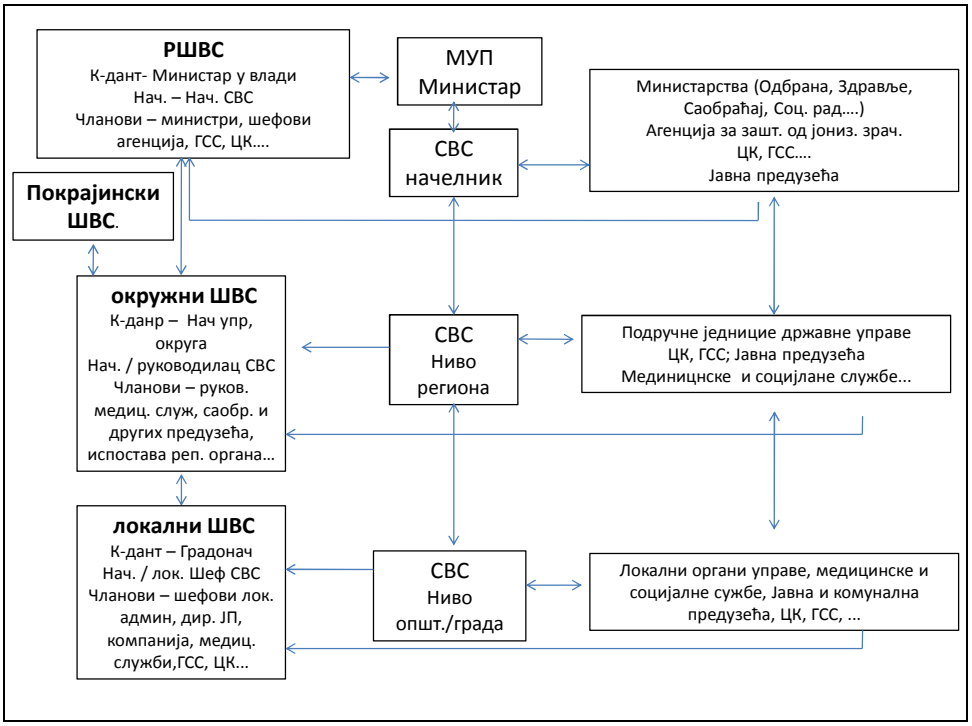
Управа за управљање ризиком у свом саставу има: *Републички центар за обавештавање (112), Одељење за осматрање, обавештавање, узбуњивање и телекомуникације, Одељење за управљање ризиком од технолошких удеса и терористичких напада, Одељење за управљање програмима и пројектима и Одељење противградне заштите.* Неке од дужности Управе за управљање ризиком су: организација изградње и развоја система управљања ризиком од елементарних непогода и других несрећа, организацију система осматрања, обавештавања, раног упозоравања и узбуњивања на територији Републике Србије; затим организација, обезбеђење и имплементација јединственог европског броја за хитне службе 112 на територији Републике Србије; прикупљање, обрада и анализа података о свим елементарним непогодама и другим несрећама и последицама; израда планских докумената из области заштите и спасавања од елементарних непогода и других несрећа.

Управа за цивилну заштиту у свом саставу има *Одељење за оперативно организационе послове цивилне заштите, Одељење за стратешко планирање и координацију, Одељење за техничку подршку и Одељење за НУС (неексплодирана убојна средства).* У задатке Управе за цивилну заштиту спадају: планирање и извршавање оперативних и организационих послова цивилне заштите; планирање, организација, попуна, обучавање, употреба и контрола специјализованих јединица цивилне заштите за територију Републике Србије, управних округа и у привредним друштвима и другим правним лицима која образују специјализоване јединице цивилне заштите.

Национални тренинг центар за ванредне ситуације у свом саставу има *Одељење за специјалистичку обуку и усавршавање припадника Сектора и Одељење за обуку цивилне заштите.* Задатак Центра је обука и оспособљавање припадника система заштите и спасавања и то: обука запослених у Сектору за ванредне ситуације, обука штабова за ванредне ситуације (Републички, покрајински, окружни, градски и општински штаб за ванредне ситуације), обука специјализованих јединица цивилне заштите, органа привредних друштава и обука других правних лица од значаја за заштиту и спасавање, а све у складу са законом и европским стандардима. Такође, у

тренинг центрима обучавају се и грађани, стичу потребна знања из области личне и колективне заштите.

Поред Сектора за ванредне ситуације, различита министарства, друге агенције и специјализоване организације[646] у оквиру своје надлежности и одговорности могу чак да буду и главни играчи у неким врстама ванредних ситуација.[647]



Слика 8.2. – Мрежа штабова за ванредне ситуације[648]

Гледано одозго надоле, Сектор има своје подручне односно територијалне организационе јединице на регионалном нивоу и на нивоу локалне самоуправе које представљају основну подршку раду штабова за ванредне ситуације који су главна оперативно стручна тела за координацију и управљање ванредним ситуацијама. Штабови за ванредне ситуације су стална тела образована за подручје општине/града од стране надлежне скупштине, за подручје региона их образује Републички штаб за ванредне ситуације а за подручје аутономне покрајине и за територију Републике покрајинска, односно републичка влада. Штаб за ванредне ситуације у општинама и градовима чине командант, заменик комаданта, начелник Штава и чланови. Уколико

[646] Ова министарства, агенције и организације приказане су на Органограму десно од СВС.
[647] Тако би у случају пандемије кључни актер свакако било Министарство здравља, а у случају нуклерних и радиолошких опасности Министарство одбране.
[648] http://prezentacije.mup.gov.rs/svs/HTML/organizacija.html 10.02.2013

је потребно штаб може образовати помоћне стручно-оперативне тимове за специфичне задатке заштите и спасавања.

Управа за ванредне ситуације у Београду у свом саставу има: *Одељење за спровођење превентивних мера при изградњи објеката, Одељење за спровођење превентивних мера при коришћењу објеката, Одељење за управљање ризиком и цивилну заштиту, Одсек за управне послове, Одсек за техничку заштиту и увиђаје, Одсек за контролу промета и превоза опасних материја и Ватрогасно спасилачку бригаду.*

Управе за ванредне ситуације у Новом Саду, Крагујевцу и Нишу у свом саставу имају Одељење за превентивну заштиту, Одељење за управљање ризиком и цивилну заштиту и ватрогасно-спасилачку бригаду.

Осим Сектора за ванредне ситуације који је тренутно централно тело за кризне ситуације, а вероватно и будуће централно тело за заштиту критичне инфраструктуре и за координацију активности у процесу заштите критичне инфраструктуре,[649] у оквиру сваког од предложених сектора постоје (или би након доношења Закона о ЗКИ требало да се установе) организације, управе, дирекције, агенције и друге институције, које су директно задужене за заштиту инфраструктуре у оквиру критичних сектора. Такође, на врху (у организационом смислу) сваког од критичних сектора налазе се и одговарајућа министарства, која су задужена за предлагање регулативе везане за заштиту КИ и контролу рада поменутих институција за заштиту КИ.[650]

Такође, Дирекција за воду бави се и заштитом других критичних инфра-структурних сектора од штетних утицаја вода (одбрана од поплава, одбрана од ерозија и уређења бујица, одводњавање земљишта, вађење песка, шљунка и камена ради одржавања и унапређивања водног режима итд). Овај сегмент рада Дирекције за воду такође није занемарљив, с обзиром на то да је било великих проблема приликом поплава у току 2014. године када се показало да систем одбране од поплава не функционише добро, а и да је управљање кризним ситуацјама врло некоординисано и отежано.[651] Сем Министарства пољопривреде и Дирекције за воду, у заштити воде

[649] Ово је само претпоставка овог рада, што дакле не мора да значи да ће се након доношења закона о ЗКИ у будућности, таква организациона структура система заштите задржати, али је за потребе рада корисно одредити централно тело од кога ће се гранати организације које ће се у оквиру посебних критичних сектора бавити заштитом критичне инфраструктуре.

[650] Сајт Дирекције за воде (Србијаводе), http://www.srbijavode.rs/portret-delatnost.htm 10.02.2013

[651] Исто тако, и многе друге, много веће и организованије државе, попут Немачке, имале су велике проблеме приликом изливања река, када се кризни менаџмент није баш снашао, а материјална штета је била огромна. Додуше, брзо после тога Немачка је донела Закон о заштити критичне инфраструктуре у ком се највише пажње придаје елементарним непогодама и тероризму.

учествују и јавна комунална предузећа водовода и канализације. У оквиру ових водопривредних предузећа тренутно се ради (заправо још од 2007. године) на реорганизацији послова и на договорима о делимичном приватизовању неких делатности, али је ситуација у том сегменту недовољно јасна и Закон о приватизацијама у јавним комуналним предузећима још увек није примењен. На предлог Удружења за комуналне делатности Привредне коморе Србије 2011. године 17 највећих ЈКП водовода и канализације Србије су се ујединили и оформили "*Пословно удружење водовода Србије*", што би требало да унапреди и регулише снабдевање водом и доведе до бржег формулисања конкретних критеријума за обим, ефикасност и квалитет услуга које пружају ЈКП.[652]

У сектору хране на највишем нивоу заштиту врше, како је већ речено, Министарство пољопривреде (Управа за ветерину, Управа за заштиту биља, Управа за пољопривредно земљиште) и Министарство здравља (контрола квалитета животних намирница). Наравно, у контроли учествују и произвођачи хране, који морају да имају своје системе контроле. Ово је сегмент који у Србији на врло нејасан начин функционише (нејасан у пракси, без обзира на постојање законских оквира), па зато долази и до проблема попут оног са афлатоксином, а и претходних везаних за квалитет и исправност сухомеснатих, млечних и других производа на српском тржишту.

У сектору енергетике обављена је делимична приватизација, па се сада 51% акција Нафтне индустрије Србије налази у склопу руског *Газпрома*. Компанија је након приватизације почела коначно да послује са позитивним резултатима. Када је у питању заштита енергетског сектора, ово је прави тренутак да се помене начин функционисања заштите инфраструктуре у случајевима кад су критични инфраструктурни сектори приватизовани. Наиме, европска и светска пракса је да се у таквим ситуацијама формирају приватно-јавна партнерства (*Public-private partnership*), чиме би у заштити критичне инфраструктуре једне државе учествовали и државни органи и предузећа која су власници или оператери критичном инфраструктуром. У свету је систем партнерстава врло развијен, постоји низ форума на којима се информације о рањивостима, постојећим претњама и ризицима размењују и доносе заједничке политике заштите КИ. Ово је можда сегмент на коме би Србија након дефинисања КИ и усвајања Закона о заштити критичне инфраструктуре морала

[652] ЈКП водовод и канализација Суботице, http://www.vodovodsu.rs/2-Informacije/131-OSNOVANO-POSLOVNO-UDRUZENJE-VODOVODA-SRBIJE 10.02.2013

понајвише да уради. Сарадња државе са приватним предузећима која су власници и оператери критичном инфраструктуром данас није на задовољавајућем нивоу.

У оквиру сектора саобраћаја (у ком је опет добар део инфраструктуре у државном власништву) највиши ниво на коме се расправља о критичној инфраструктури је Министарство саобраћаја, које предлаже законе и друге регулативе у области саобраћаја, па и заштите критичне инфраструктуре. У оквиру Министарства постоје дирекције (за друмски, за железнички транспорт, директорат цивилног ваздухопловства), а у оквиру њих нове дирекције (у оквиру друмског – Дирекција за путеве, Дирекција за саобраћајну сигнализацију итд.) и свака од тих дирекција требало би да буде задужена за ЗКИ у свом сектору (за предлагање законске регулативе и за спровођење постојеће). У Србији се доста говори о саобраћајној инфраструктури у негативном контексту, практично у свим секторима. Највећи проблеми везани за застарелост инфраструктуре и за инертност (субјективно перципираној од стране корисника инфраструктуре тј. грађана) одговорних дирекција и Министарства.

У оквиру здравства за предлагање закона задужено је Министарство здравља, а за заштиту подсектора одговорно је Министарство унутрашњих послова и Министарство одбране.

У оквиру финансија, законе предлаже и њихово спровођење контролише Министарство финансија и привреде, док заштиту инфраструктуре обавља МУП. У оквиру МУП-а, постоје и одељења која су у оквиру заштите финансијске инфраструктуре баве пословима сузбијања организованог финансијског криминала (одељење у склопу Криминалистичке полиције).

На заштити у области ИКТ сектора се, као и на регулативи, доста урадило. Велики број одељења везаних за заштиту ИКТ налазе се у склопу Министарства унутрашњих послова, а за законску регулативу задужено је (у тренутном сазиву) Министарство спољне и унутрашње трговине и телекомуникација. О регулативи је већ било речи, тако да сад остаје тема организација које се баве заштитом ИКТ у Србији. Дакле, оранизације, агенције и одељења која се баве заштитом ИКТ су:

1. *Сектор за аналитику, телекомуникационе и информационе технологије*[653] у свом саставу има:
   - Управу за аналитику,
   - Управу за информационе технологије (ИТ) и

[653] Информатор о раду МУП-а Србије, март 2012, стр. 41

- Управу за везу и криптозаштиту.

Управа за аналитику непосредно врши аналитичко-информативне послове из оквира послова јавне безбедности и МУП-а у целини, учествује у пословима екстерног и интерног информисања, статистичког истраживања и праћења безбедносних појава и догађаја, стратешког планирања и развоја МУП-а и представља подршку одлучивању министра.

Управа за аналитику у свом саставу има:[654]

- Одељење за аналитику,
- Одељење за оперативно-аналитичко информисање и евиденције и
- Одељење за планирање и развој.

Управа за информационе технологије (ИТ) одговорна је за организовање, функционисање, развој, унапређење и експлоатацију интегрисаног аутоматског информационог система Министарства (ЈИС) и логистичку подршку оперативним пословима из домена примене информационе технологије.

Управа за информационе технологије (ИТ) у свом саставу има:

- Одељење за логистику (које у свом саставу има Одсек за набавку и магацинско пословање, Одсек за координацију и Одсек за корисничке сервисе)
- Одељење за пројектовање и интеграцију (које у свом саставу има: Одсек за пројектовање услуга и Одсек за програмирање услуга.),
- Одељење за интеграцију и апликативну подршку (које у свом саставу има Одсек за интеграцију и увођење нових технологија и Одсек за апликативну подршку),
- Одељење за комуникациону инфраструктуру (које у свом саставу има Одсек за пројектовање инфраструктуре, Одсек за постављање и одржавање и Одсек за сервис),
- Одељење за рачунарску инфраструктуру (које у свом саставу има Одсек за сервере са периферијом и Одсек за базе података и системски софтвер),
- Одељење за коришћење рачунарских система (које у свом саставу има Одсек за интранет и Одсек за интернет),

[654] http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/uprava-za-analitiku.h 10.02.2013

- Одељење за послове заштите (које у свом саставу има Одсек за заштиту коришће-ња система, Одсек за заштиту инфраструктуре и Одсек за сертификацију),
- Одељење за послове припреме података и материјала (које у свом саставу има Одсек за припрему података за персонализацију и Одсек за логистику), и
- Одељење персонализационог центра (које у свом саставу има Одсек за персонализацију идентификационих докумената и Одсек за персонализацију путних исправа)

Управа за везу и криптозаштиту се бави системима техничке и електронске заштите објеката и лица и врши послове одржавања оперативне технике у употреби у организационим јединицама Министарства. Управа такође израђује посебне планове и документа за рад у ванредним ситуацијама, стара се о акцијској резерви средстава везе и врши увид и контролу извршавања послова у подручним полицијским управама из области везе, пружа техничку подршку оперативним линијама рада и учествује у акцијама обезбеђења, акцијама откривања лица која неовлашћено поседују и користе телекомуникациону опрему, акцијама контроле радио-саобраћаја и идентификације ометача радио-веза и другим акцијама.

Управа за везу и криптозаштиту у свом саставу има:

- Одељење за планирање, развој и одржавање комутационих система веза (које у свом саставу има Одсек за ТФ системе, Одсек за системе криптозаштите и Одсек за системе преноса),
- Одељење за оперативно-планске послове, заштиту и експлоатацију веза (које у свом саставу има Одсек за оперативно-планске послове, Одсек за надзор и експлоатацију радио-мрежа и Одсек за криптозаштиту и експедицију телеграма),
- Одељење за планирање, развој и одржавање радио-система веза (које у свом саставу има Одсек за оперативно-планске послове, Одсек за надзор и експлоатацију радио-мрежа и Одсек за криптозаштиту и експедицију телеграма),
- Одељење за електронску заштиту и оперативну технику (које у свом саставу има Одсек за електронску заштиту, Одсек за увођење и експлоатацију оперативне технике).

Криминалистичка полиција – одељење за борбу против високотехнолошког криминала. У области сузбијања високотехнолошког криминала, активности криминалистичке полиције усмерене су на: кривична дела против безбедности рачунарских података, кривична дела у вези са електронским банкарством и електронском трговином (тзв. *phishing*, *pharming* и др), фалсификовање платних картица и њихову злоупотребу на интернету, јер се очекује тренд пораста у извршењу ових кривичних дела, као и активности појединих организованих криминалних група у овој области.

Задаци криминалистичке полиције и одељења за високотехнолошки криминал су и:

- Спречавање злоупотребе података добијених крађом идентитета која доводи до великих финансијских губитака, као и злоупотребе информационих технологија за крађу идентитета, поготово у он-лајн комуникацији.
- Сузбијање неовлашћеног прикупљања података о платним картицама до којих извршиоци кривичних дела долазе преко интернета и то на неколико начина: нежељеним порукама (*Spam*), пецањем (*Phishing*), Фармингом (*Pharming*) и крађом података о платним картицама из базе података електронских продавница.
- Сузбијање активности из области "*CRIMEWARE-AS-A-SERVICE* – CaaS", тј. сузбијање интернет сервиса који пружају *злоћудне* програме као услугу у кривичним делима високотехнолошког криминала на извршењу кривичних дела у виртуелном окружењу.
- Праћење ризика и претњи од високотехнолошког криминала у *CloudComputing* окружењу, с обзиром на то да корисници *CloudComputing* окружења на више начина могу бити угрожени, а најпознатији су: злоупотреба и неовлашћена употреба *CloudComputing* сервиса, небезбедни програмски интерфејс и програми за повезивање софтвера, злонамерни *инсајдери* у систему, губитак података/одлив података и крађа налога, сервиса или неовлашћено преузимање комуникационих сесија. Најчешћи облици напада *CloudComputing* окружења су: преко *бочних канала*, DOS напади, напади на социјалне мреже, као и напади на мобилне телефоне.
- Сузбијање криминалне активности у области ширења незаконитих садржаја на интернету, као што су искоришћавање деце и малолетника за порнографију и његова даља дистрибуција путем интернета (тзв. *интернет*

педофилија или *дечја порнографија*), као и појава ксенофобије, расизма, шовинизма, тероризма и других облика насиља путем интернета (у складу са протоколима Европске конвенције о сајбер криминалу).

- Сузбијање рачунарске преваре, посебно најприсутније облике овог кривичног дела, које се огледају у тзв. нигеријским преварама[655] и коришћењу претходно прибављених података о компромитованим платним картицама и банковним рачунима физичких и правних лица, уз перманентно коришћење техника социјалног инжењеринга.
- Спречавање повреде права интелектуалне својине (подизање нивоа истрага када се крше права интелектуалне својине коришћењем P2P мрежа, FTP сервера, интернет форума, сајтова и сервиса, социјалних мрежа у вршењу кривичних дела везаних за злоупотребе права интелектуалне својине као што су оглашавање и дистрибуција *пиратизованих* рачунарских програма, књига у електронском облику, рачунарских игрица, филмова, музике и других аудио-визуелних садржаја) и других облика извршења кривичних дела из области високотехнолошког криминала који се могу извршити под окриљем наведених кривичних дела против интелектуалне својине. Одељење учествује у иницијативама различитих институција и министарстава Владе Републике Србије за очување права интелектуалне својине, као што је формирање координационог тела за размену података о кршењу права интелектуалне својине.
- Идентификовање садржаја који представљају средство извршења кривичних дела против повреде права индустријске својине, као и предмете настале након злоупотребе (разлике између оригиналних предмета заштите и фалсификата робних марки, жигова и др). Такође, одељење за високотехнолошки криминал поклања пажњу повредама права индустријске својине, односно проналази лица која се оглашавају преко интернета ради продаје роба са фалсификованим ознакама туђих фирми.

[655] Нигеријска превара представља специфичан начин извршења кривичног дела преваре који је настао захваљујући глобалној улози интернета као средства за комуникацију, електронско пословање и сл., као и све већој употреби савремених информационих технологија од стране великог броја крајњих корисника, широм света. Први појавни облици ове преваре подразумевали су лажне пословне понуде које су извршиоци кривичних дела нудили жртвама преваре. Данас начини извршења ових облика превара имају различиту форму, па се тако врше помоћу лажних електронских порука о добицима на играма на срећу, лажних порука везаних за добротворне прилоге, порука у вези са *љубавним понудама*, и др.

- Одељење обавља техничко опремање савременим истражним и форензичким средствима за борбу против високотехнолошког криминала у циљу побољшања прикупљања електронских података (он-лајн и оф-лајн), њихове анализе и аквизиције.
- Одељење је ангажовано и у области сузбијања прања новца које се спроводи коришћењем рачунара и рачунарских мрежа, при чему сарађује са Јединицом за финансијске истраге, као и са Министарством правде и Дирекцијом за управљање одузетом имовином. У том циљу, одељење унапређује сарадњу са другим државним органима који у оквиру своје надлежности располажу информацијама које указују на извршење кривичног дела прања новца (Пореска полиција, Управа за спречавање прања новца, Управа царине и др.).
- С обзиром на нове појавне облике, посебан акценат стављен је на међународну сарадњу у области борбе против високотехнолошког криминала како на нивоу размене података, тако и на нивоу захтева за проверама, заједничких акција, других заједничких активности.
- Одељење подржава иницијативе и активности везане за формирање Националног центра за интернет сигурност (CERT и CIRT) на основу најбољих искустава и праксе ЕУ и земаља у региону. План је да се након оснивања овог Центра, преко њега планирају активности, размена података, искустава и обавља кординација рада различитих институција у овој области. Такође, одељење се залаже за оснивање централног регистра на којем се може вршити пријављивање кривичних дела из области високотехнолошког криминала, а напори се улажу и у развој сопственог рачунарског програма за истраживање, обраду и анализу прикупљених података.

На крају одељење учествује у твининг пројекту "Успостављање ефикасног система за спречавање и сузбијање илегалних миграција на територији Републике Србије" чији су корисници Одељење за борбу против високотехнолошког криминала Службе за борбу против организованог криминала и Управа граничне полиције. *Локална самоуправа.* Након што је 2009. године оформљен интегрални систем за управљање ванредним ситуацијама, у наредне три године је систем успостављен у нормативном и

организационом смислу, али функционише у нестабилним политичким условима. Промене на челним политичким функцијама у локалним самоуправама, као и руководилаца јавних предузећа и установа и других професионалаца отежавају успостављање стабилних радних релација и нормално уходавање и функционисање штабова за управљање ванредним ситуацијама као најзачајних актера. Хронични недостатак финансијских средстава и преовлађујуће схватање да је улагање у превентиву трошак, а не инвестиција, додатни су системски фактори који озбиљно отежавају успостављање ефикасног система за управљање ванредним ситуацијама.

У локалним самоуправама у Републици Србији нису систематизована радна места и одређена лица која би се професионално бавила организацијом и имплементацијом система заштите и спасавања у ванредним ситуацијама. Ово представља озбиљан проблем јер се практично скоро сви послови из ове области пребацују на подручне организационе јединице Сектора за ванредне ситуације.

На локалном нивоу постоје веома велике разлике у броју и врсти формираних стручно оперативних тимова, учесталости састанака штабова за управљање ванредним ситуацијама, односу према одређивању оспособљених правних лица, цивилној заштити итд.

Веома важан елемент система за управљање кризама је цивилна заштита чије је успостављање на самом почетку, и спојено је са бројним нормативно правним, кадровским, организационо техничким и материјалним проблемима.

Поред тога, локалне самоуправе, са ретким изузецима, нису донеле процену угрожености као један од најзначајних докумената који је предуслов за доношење других важних докумената за управљање ванредним ситуацијама.

Осим тога, изражени су и кадровски проблеми, недостатак основне опреме и материјално техничких средстава, недовољно улагање у превентиву, недостатак новца, нестабилни извори финансирања, лоше стање јавних предузећа, недовољна укљученост локалне самоуправе, недостатак свести и др.

Неке од наведених проблема локалне самоуправе би могле да реше бољом организацијом и већом посвећеношћу. чиме би допринеле већој ефикасности система за управљање ванредним ситуацијама и укупној безбедности локалних заједница и њихових грађана.

Кључни проблеми везани за организациону структуру и надлежности државних институција у области заштите КИ, као и предлог мера за побољшање стања у овој области, дати су у сублимираној форми у Табели 8.3.

Институција/орг. структура/надлежност	Идентификовани проблеми	Предлог мера
Сектор за ванредне ситуације	• Надлежност није експлицитно дефинисана у односу на КИ	• Дефинисати надлежност у складу са Словенијом и Бугарском на основу Закона о заштити КИ (који би конкретније дефинисао структуру, обавезе и надлежност институција за ЗКИ, у циљу унапређења ефективности и ефикасности у ванредним ситуацијама)
Јединствен систем комуникације и координације	• Телекомуникациони систем и стање информационо-комуникационе технологије која омогућава и подржава функционисање система за управљање варедним ситуацијама нису задовољавајући. Ова опрема је углавном недовољна и застарела.	• Набавити нову, технолошки напредну опрему у довољној количини.
Приватно-јавно партнерство	• Није дефинисано	• Дефинисати законом.
Дефинисање мера раног упозорења	• Није оформљен CERT	Поступити по препорукама Конвенције о сајбер криминалу.
Едукација становништва	• У целини гледано нема уједначеног, осмишљеног, планског и организованог приступа едукацији становништва за ванредне ситуације.	• Увести перманентну едукацију становништва у свим локалним самоуправама. • Прилагодити школски наставни план и програм овим потребама.

Институција/орг. структура/надлежност	Идентификовани проблеми	Предлог мера
		• Увести менаџера за ванредне ситуације по локалним самоуправама.
Локална самоуправа	• У већини локалних самоуправа није донета процена угрожености у складу са усвојеном Методологијом и недовољна укљученост у процени и заштити КИ. • Кадровски проблеми (непопуњеност, необучен кадар, честе кадровске промене) • Недостатак основне опреме и материјално техничких средстава • Недовољно улагање у превентиву • Недостатак финансијских средстава • Лоше стање јавних предузећа укључених у ЗКИ • Недостатак безбедносне културе • Правни проблеми (неусклађеност Закона о ванредним ситуацијама и Закона о локалној самоуправи)	• Професионализација кадра. • Донети планска документа из области заштите и спасавања (Процену угрожености, План заштите и спасавања, План заштите од удеса), а затим и усагласити мере и задатке са надлежним органима, привредним друштвима и другим правним лицима у суседним јединицама локалне самоуправе. • Анализирати прописе и ускладити нормативну регулативу која се односи на цивилну заштиту

Табела 8.3. *Организационе структуре и надлежности државних институција - актуелно стање, идентификација проблема и предлог мера*

8.6. Смернице за формулисање политике заштите КИ

Као што је већ поменуто, Србија нема кохерентне оквире у области заштите критичне инфраструктуре. Као највећи проблем на овом пољу треба истаћи непостојање закона о критичној инфраструктури, односно закона о заштити критичне инфраструктуре. У том смислу, неопходно је спровести истраживање широког обима које би укључило све секторе друштвене делатности, где би се на основу опсежних тестова (којима би се практично утврђивао значај инфраструктура), дошло до

релевантне листе критичних инфраструктура. Такође, на основу резултата истраживања могао би да се утврди и релативни степен критичности једне инфраструктуре у односу на друге и карактеристичне међузависности, специфичне за територију Србије. До сада нису рађена детаљна истраживања о међузависности КИ у Р. Србији.

Након формулисања листе критичних инфраструктура требало би донети Закон о критичној инфраструктури. Од земаља у региону то су већ урадиле Словенија (2008. године), Хрватска (јануар 2013. године), као и Бугарска и Мађарска. Тек након дефинисања Закона о критичној инфраструктури могло би да се каже шта све Србији још недостаје у погледу законске регулативе. Неки закони, које би требало усвојити, везани су за прецизирање заштите енергетске инфраструктуре, као и електроенергетске инфраструктуре, затим за заштиту инфраструктуре за транспорт енергената (гаса пре свега, због могућег проласка гасовода *Јужни ток* кроз Србију), јер би сви ови подсектори били сматрани европском критичном инфраструктуром. Законодавство би у практично свим критичним секторима морало да се редефинише, односно да се успостави тамо где се појмовно не препознаје критична инфраструктура, и са аспекта заштите инфраструктуре (у пољопривреди, на пример, постоји систем заштитних мера у сточарству, пољопривреди и водопривреди, али су многе теме недовољно обрађене, попут биотероризма, а по питању многих тема које су вишеструко значајне − попут мелиорације, већ дуго се ништа не ради). Основним Законом о заштити критичне инфраструктуре треба да се предвиди и централно тело задужено за заштиту критичне инфраструктуре. У овом истраживању је као централно тело препознат Сектор за ванредне ситуације, с обзиром на то да је на сличан начин решено питање централне одговорности у процесу ЗКИ. Међутим, ту се законски оквир не завршава. Као прво, треба утврдити да ли се опсег делатности Сектора за ванредне делатности треба проширити увођењем закона и да ли ће бити потребно отварање нових одељења, управа, дирекција у оквиру овог сектора. Затим, треба да се утврди један јединствени систем комуникације и координације активности (пошто је координисање кризних ситуација у Србији раније представљало проблем и доводило до преклапања одговорности и на крају до пребацивања одговорности са једног министарства на друго, са једне дирекције на другу), због кога ће евентуално морати да се оформи нови штаб за координисање акција. Велики значај у свету за функционисање система заштите КИ имају приватно-јавна партнерства, у смислу сарадње приватног сектора (власника или оператера критичном инфраструктуром) и државе на регистровању

претњи, ризика и рањивости, те на дефинисању начина на који би се прекид функционисања инфраструктуре спречио упркос претњама. Овакав вид сарадње данас је заснован само на доброј вољи обе стране (што се у пракси ретко дешава). Усвајањем Закона о ЗКИ ово питање би требало да буде решено, будући да би Закон требало да створи атмосферу поверења између приватног и јавног сектора. Закон би такође требало да формулише неопходне услове за оснивање CERT-а (*Central Emergency Response Team*), рачунарског тима за ванредне ситуације који би био још једна тачка задужена за координацију и комуникацију. На националном нивоу Закон би могао и да дефинише обавезе свих приватних власника, односно оператера критичном инфраструктуром, везане за формирање планова за заштиту КИ у оквиру својих компанија, који ће се касније на састанцима представника државе и приватника (чије одржавање − месечно, годишње, ванредно − такође се може законом прописати) тумачити, мењати, или ће се из њих усвајати добра искуства, која би се даље преносила другим компанијама које тек треба да оформе политику заштите своје критичне инфраструктуре). Сем на националном нивоу, Закон би требало да регулише и питање заштите критичне инфраструктуре на локалном нивоу. Тек након усвајања једног овако свеобухватног закона, заједно са стратегијом спровођења политике заштите КИ, која би требало да уследи касније, могло би се говорити о постојању кохерентног законског оквира за спровођење мера и политике ЗКИ.

ЗАКЉУЧНА РАЗМАТРАЊА

У савременом свету суочавамо се са многобројним изазовима, претњама и ризицима који доводе до различитих врста кризних ситуација. Сложеност и отвореност савремених друштава, разни облици економског, друштвеног и политичког деловања, као и катастрофе изазване природним поремећајима, свакодневно стварају изазове и претње којима се морамо супротставити различитим поступцима и инструментима. Појавни облици савремених криза указују на њихову сложеност и захтевност у смислу структурних и организационих одговора. Управљање неком савременом кризом представља врло сложену операцију која траје дуже време и у којој учествују различити актери, од политичких до пословних, као и појединци који су угрожени деловањем кризе. Сложеност и захтевност савремених криза, припреме, организовање одговора кад се криза појави, опоравак после кризе, као и управљање потребним променама које су неопходне за боље функционисање система, захтевају стварање јединствених политика управљања у кризним ситуацијама. Савремене политике се данас ослањају не само на капацитете које има држава, већ су отворене и према партиципацији грађана и других важних актера који учествују у некој заједници. Кризне ситуације су стања у којима морамо деловати, јер свако нечињење може створити још веће последице за појединце, организацију или заједницу. Кризе карактерише висок ниво неизвесности, посебно у условима недостатка информација. Кризно комуницирање је зато важно подручје, јер утиче на смањење неизвесности и ствара претпоставке за функцинисање система одговора на кризе. После завршетка, односно окончања кризних ситуација појединац, организација или заједница приступају опоравку уз извлачење поука које могу послужити за управљање променама у систему с циљем ефикасног деловања у следећим кризним ситуацијама. Све то упућује нас на јачање организованог и свеобухватног приступа управљању савременим кризама у сложеним заједницама какве су данашње, а такав се приступ може обезбедити само обликовањем јавних политика и креирањем познатих и прихватљивих инструмената одговора на кризе.

Крај хладног рата, распад Совјетског Савеза и проширење НАТО-а и Европске уније дубоко су изменили констелацију европске политике и безбедности. Једна од значајнијих последица била је и стављање све већег нагласка на способност држава да се суочавање са не-војним прекограничним претњама и ризицима који могу да изазову комплексне друштвено-политичке кризе. Климатске промене које за последице имају

природне катастрофе, опасности које носе нове технологије, велики друштвено-економски проблеми, масовне миграције, епидемије заразних болести, питања заштите животне средине, тероризам, организовани криминал и трговина дрогом захтевају нове стратегије, те постају све бројнији ургентни позиви за свеобухватне и конзистентне приступе детекцији и превенцији криза, припремљености на њих и адекватном одговору, као и опоравку након кризе. Све ово, као и чињеница да се Европа и даље веома брзо мења, при чему су питања сигурности, ризика и безбедности у самом врху преокупација и држава и јавности, представља велики изазов за владе свих европских земаља.

Одговорност сваке државне власти за једну од њених основних функција – обезбеђивање безбедности грађана – остварује се и успостављањем одговарајућег система за реаговање у ванредним ситуацијама, који ће на најбољи могући начин искористити све расположиве ресурсе државе и друштва како би се пружила максимална могућа заштита цивилном становништву и спречило уништавање добара која грађанима омогућују одређени ниво квалитета живота. Системи за реаговање у ванредним ситуацијама различито су устројени у савременим државама, што зависи од врсте и специфиности угрожавања државне територије, климатских прилика, природних појава, карактеристика тла и др., с једне стране, и постојећег правног система, управних традиција, политичко-територијалне организације и друштвеног уређење, историјских искустава са ванредним ситуацијама, с друге стране. Дакле, ради се о субјективним и објективним могућностима и потребама. С обзиром на начин организовања националних система за реаговање у ванредним ситуацијама и њихову позицију у државној управи, они се могу разврстати у једну од следеће четири групе: 1) посебно министарство или државна управа за заштиту и спасавање (цивилну заштиту), 2) посебна државна агенција за заштиту и спасавање (цивилну заштиту), 3) државна управа заштите и спасавања (цивилне заштите) у оквиру неког министарства, 4) управа заштите и спасавања као организациона јединица министарства.

Истраживање система за управљање ванредним ситуацијама у 22 европске земље и 8 региона у оквиру АНВИЛ пројекта показало је велику разноврсност система у погледу њихове централизације, односно децентрализације, свехазардног приступа, улоге војске у цивилним ванредним ситуација, могућности привремене суспензије појединих права и слобода грађана током кризе итд. Истовремено показано је да нема апсолутно најбољег и општепримењивог система који би био ефикасан у свим земљама, управо због специфичности о којима је било речи. Такође, истраживање је

показало да постоје озбиљни проблеми везани за методологију којом се мери квалитет система за управљање ванредним ситуацијама операционализован кроз димензије ефикасности, ефективности и легитимности.

Оно што је, међутим, несумњиво без обзира на структуру и институционални дизајн система за управљање ванредним ситуацијама је велики значај кризног комуницирања, како у оперативном смислу (комуникације у вези постојећих ризика и опасности, подизање безбедносне свести и културе становништва, давање упутстава за поступање грађана у ванредним ситуацијама итд.) тако и у смислу управљања представама, перцепцијом и симболима. Неблаговремено или технички, односно комуниколошки формулисано и дисеминовано упозорење, савет или наређење (нпр. за евакуацију) неће имати ефекте и додатно ће усложити управљање ванредном ситуацијом. Безбедност грађана је директно зависна од брзине и истинитости обавештења коју надлежни субјекти прикупљају, износе и објављују. Оперативна ефикасност процеса супротстављања кризи, ублажавања њених последица и опоравка је директно зависна од реакције непосредно угрожених лица али и оних који су под посредном опасношћу. Осим тога, добро оперативно управљање ванредном ситуацијом које није праћено адекватном комуникацијом изгледаће у очима јавности мање добро или чак лоше. Истинито је и обрнуто. Наиме неко може објективно учинити низ грешака и пропуста у решавању ванредне ситуације, али добром кризном комуникацијом и управљањем представама односно перцепцијом то може изгледати мање лоше или чак и добро. Кризна комуникације и јесте средство неопходно за опстанак сваке организације, па и државе.

Способност за управљање стресним кризним и ванредним ситуацијама у великој мери зависи од доброг функционисања радних, односно оперативних канала за прикупљање и размену информација на и између свих нивоа, укључујући доносиоце одлука, аналитичаре и оперативни састав. У драматичним кризама комуницирање је такође важно посебно у оним кризама које трају у релативно дугом временском периоду. Управо зато управљање комуникацијама представља важан део кризног плана. Да би се ефективно и ефикасно управљало кризном, односно ванредном ситуацијом важно је циљној јавности у право време упутити праву поруку путем адекватних комуникационих канала.

Одговор на кризе захтева брз проток информација од самога кризног подручја до одлучилаца, међу самим одлучиоцима и између одлучилаца те других учесника (погођени кризом, масовни медији). Пошто су све кризе у задњој фази политички

догађаји за њих се интересују масовни медији. Само извештавање медија о кризи и кризном управљању и вођењу представља тако део, али такође и последицу кризног комуницирања.У том смислу посебно важан сегмент кризне комуникације јесу односи са медијима пре, током и након ванредних ситуација. Истовремено, значајно су порасла очекивања и јавности и политичке елите кад је реч о способности владе да предвиди и управља кризама и ванредним ситуацијама. Медији, јавност и критичари генерално немају више много разумевања када доносиоци одлука на националном нивоу за кризу криве природу или лошу срећу, или покушавају да пребаце кривицу и одговорност на локалне валсти, приватна предузећа или појединце. Чини се да се кризе пре виде као прилика за критику и пропитивање постојећег стања и етаблираних структура и политика. Док су се раније креатори политике концентрисали на прикупљање информација о актуелним догађајима сада се тежиште премешта на перцепцију догађаја, односно управљање истима. На тај начин кризни менаџмент се на неки начин "дематеријализује" у смислу да више није важан само оперативни, технички одговор на кризу већ све више и способност да се управља истом.

Земље у транзицији су се суочиле са свим овим проблемима, при чему су кадровски и технички капацитети њихових система за заштиту и спашавање углавном били мање развијени него у земљама западне Европе. Осим тога ове земље су доживљавале дубоку трансформацију у свим областима, настојећи да уведу демократске институције и превазиђу бреме ауторитарног наслеђа. Поред потпуно измењене глобалне геополитичке констелације и нових безбедносних претњи и изазова, мења се и њихов унутрашњи систем вредности, друштвени и државни приоритети и структуре. Мењају се и схватања саме суштине кризе, њена перцепција, као и концепције везане за поступање у случајевима различитих криза на појединим нивоима друштвеног организовања. Наиме, целокупни наслеђени механизам управљања кризама у овим државама доживљава дубоку траснформацију. Ово добија на значају посебно с обзиром на догађаје као што су терористички напад на САД од 11. септембра, епидемије заразних болести и друге невојне прекограничне претње, изазови и ризици који имају потенцијал да изазову комплексне социо-политичке кризе на националном и на интернационалном нивоу. Поред ових глобаних проблема, земље у транзицји су суочене са бројним проблемима које овај процес сам по себи носи. Наиме, прелазак из једног у други политички систем отвара бројне рањивости које не постоје у стабилним државама. Стварање слободног тржишта, уместо економије регулисане државним планом, реконфигурација социјалних структура и статусних аранжмана

доводе до разочарења и фрустрираности широких слојева становништва. С друге стране доносиоци политичких одлука стављени су пред тешке изборе и дилеме при чему се углавном не могу ослонити на спектар дифузне подршке.

Истраживање проблема кризног менаџмента у функцији заштите критичних инфраструктура у земљама у транзицији, осим истицања организације и функционисања кризног менаџмента у развијеним земљама, ограничен је на транзиционе земље као специфичан културно-историјски контекст. Транзиционе земље су суочене са великим политичким, економским и општим друштвеним тешкоћама, при чему богата искуства других, развијенијих земаља, али и захтеви интеграционих процеса, отварају низ могућности и указују на могућа нормативна и организациона решења. Ипак, могућност имплементације теоријских модела и практичних решења других земаља нису аутоматски применљива на транзиционе земље, које не испуњавају потребне политичке, економске и нормативне предуслове.

Проблемима у управљању кризама у низу транзиционих земаља значајно је допринело лоше кризно комуницирање. Тако се многи слажу да је кризно комуницирање било нарочито лоше у кризном менаџменту у Бугарској, у тој мери да је у одређеним случајевима чак и створило кризу и да се земља нашла на "неуротичном" крају на спектру кризог комуницирања. Слично је и у Румунији у којој је лоше кризно комуницирање допринело ескалацији кризних ситуација. У нашем истраживању смо се определили за четири државе Русију, Словенију, Бугарску и Србију, које деле сличну прошлост и потичу из истог друштвеног контекста, али се данас налазе у различитим фазама транзиционог процеса. Проучавајући различита искуства ових земаља, које немају идентична (у неким елементима чак ни слична) организациона и нормативно-правна решења, као ни једнаку финансијску ситуацију нити истоветан политички контекст, дошли смо до научно утемељених закључака о могућностима унапређења процеса управљања ванредним ситуацијама кроз унапређење кризног менаџмента. Наше истраживање је кроз анализу и упоређење активности релевантних националних тела или агенција задужених за управљање ванредним ситуацијама у Русији (Национални центар за кризни менаџмент у оквиру Министарства за ванредне ситуације), Бугарској (Закон о кризном менаџменту), Словенији (Управа за заштиту и спашавање /Uprava za zaščito in reševanje/ у оквиру Министарства одбране), Србији (Сектор за ванредне ситуације у оквиру МУП-а) у односу на општу јавност, као и поједине циљне групе унутар опште јавности пре свега из перспективе основних поставки савремених теорија кризног менаџмента.

Негативне последице савремених комплексних криза, које истовремено обухватају различита подручја живота заједнице, у бројним европским државама, утичу да се међу научницима, стручњацима и практичарима, који се баве различитим кризама, повећава интерес за теорију и за научне резултате проучавања криза и кризног менаџмента. Резултати таквог вишегодишњег истраживања на пољу управљања и вођења у условима кризе, постају саставни део ширег европског програма *Кризно управљање у Европи*.

Кризни менаџмент остаје ограничен и без ефекта све док се посматра као дисциплина која је негативна, непродуктивна у смислу стварања вредности, временски захтевна, потенцијално опасна и техничка пре него стратешка. Кризе се могу посматрати и као ситуације које нуде необичне могућности за испољавање менаџерске флексибилности, јачање тимског рада, чврстоћу организације и стратешка преподешавања. Кризни менаџмент је у фази настанка, па зато постоји много тога што тек може и треба да се уради, пронађе, открије, и ту има доста послова за креативност и доприносе. Кризни менаџмент може деловати као катализатор за иновације и преузимање ризика, али може представљати и непосредни извор вредности означен као извор компаративне предности (на пример локалне власти у многим земљама у свјим плановима за кризне ситуације посебну пажњу посвећују могућем загађењу воде или прекидима водоснабдевања).

Кризни менаџмент више не би требало посматрати као сет ригидних процедура које је неопходно успоставити уз значајан иницијални напор, спаковати у обиман приручник и то све стално одржавати у стању перманентне готовости што је, практично, неизводљив дугорочни напор. КМ треба гледати као континуирани процес који може бити у сваком тренутку ревидиран или редизајниран у складу са повратним информацијама које долазе из искуства или из кризних симулација. Пошто је кризни менаџмент још увек млада дисциплина све идеје и праксе које се у оквиру њега јављају треба да буду преиспитане и прилагођене специфичној организацији и/или ситуацији која је у питању. Истовремено, веома је мало истраживања о одржавању или, пак, поновном стицању поверења јавности као значајном циљу сваке организације и делу политике менаџмента.

Будуће кризе ће захтевати припреме које ће обухватати како стратегије усмерене на опоравак, тако и оне засноване на антиципацији. Опоравак је кључ за поступање у будућим кризама и зато се за њега мора организовати на одговарајући начин, тј. организовати брз, флексибилан, иновативан и ефективан одговор када

настане будућа криза. Важно је брзо реаговати када се криза појави. Међутим, кризе стварају и такве ситуације које се не могу предвидети и које захтевају одговоре који нису програмирани. Императиви који могу да помогну организацији или заједници да се припреми за непознато су следећи: обезбедити свест највишег руководства за развој одговарајућих оперативних капацитета, као и ангажовање у континуираним припремама (применом повратних искустава из праксе, укључујући и међународна искуства).

Неспорна је чињеница да се друштвени сукоби ни у једном друштву не могу до краја институционализовати, јер у конфликтима постоји низ фактора који су непредвидиви и непоновљиви, и не могу се унапред регулисати никаквим општим правилима, начелима или нормама. Модели разрешавања конфликата и конфликтних ситуација су у теорији бројни и међусобно се разликују у зависности од теоријско-методолошког приступа аутора. Тако се данас у теорији кофликата термини: регулисање, разрешавање, окончање, заменили изразе спречавање, гушење, елиминисање и сл., који су раније били преовлађујући. Тако се и окончање сукоба сматра општим и најширим изразом, док се појам разрешавање користи као најприхватљивији за означавање овог процеса, јер указује на помирење супротстављених страна, док израз решавање подразумева и окончање конфликта, што се у стварности веома ретко дешава.

Појава концепта заштите критичних инфраструктура у развијеним земљама Запада може се објаснити променама које су, најпре, настале у перцепцији претњи и све већој међузависности различитих инфраструктурних елемената, што друштвени систем чини веома рањивим, а ризике и претње критичним инфраструктурама значајнијим. Током последњих година промењио се приступ самом концепту и поглед на рањивост критичних инфраструктура. Она се раније везивала за проблеме који се односе на функционисање *високоризичних* технологија, док данас критична инфраструктура и њена заштита представљају питање од виталног значаја за националну и наднационалну безбедност.

Свесни чињенице да ефикасан систем заштите критичне инфраструктуре ствара предуслове за нормално и несметано функционисање ширег друштвеног система, државе улажу велике напоре у циљу израде адекватних механизама заштите. Оно што представља отежавајућу околност приликом њихове израде јесте широк спектар виталних сектора које обухвата критична инфраструктура, попут саобраћаја, транспорта, производње и дистрибуције енергије, информационих и комуникационих

система, здравствених служби, система за снабдевање водом и храном итд. Делимично или потпуно отказивање ових инфраструктура може нарушити нормално функционисање једног система, угрозити националну безбедност и проузроковати кризе најразличитијих размера.

Развијене земље, а последњих година и оне слабије развијене, као и земље у транзицији, настоје да идентификују и анализирају критичне секторе, подсекторе, процесе и објекте коришћењем различитих методолошких алата. Том приликом, највећи проблем представља комплексност инфраструктурних система и идентификовање специфичних ризика и претњи којима су они изложени. Такође, једно од главних питања тиче се одређивања редоследа спровођења радњи током израде адекватног система заштите критичних инфраструктура. Наиме, најпре треба утврдити ризике, претње и рањивости којима је одређени систем изложен, након чега се приступа идентификовању критичних сектора и изради специфичне класификације. Приликом спровођења поменутих радњи алати кризног менаџмента имају кључну улогу у процесу идентификовања и процене степена изражености одређеног система конкретној врсти ризика и претње. Исправном применом поменутих алата, утврђују се слабе тачке и стварају предуслови за израду ефикасног система заштите критичне инфраструктуре.

Заједнички циљ којем теже све државе када је у питању заштита критичне инфраструктуре јесте израда адекватног механизма који ће спречити стварање услова који могу довести до отказивања одређене инфраструктуре услед несреће или напада на било који елемент система. Сходно томе, политика заштите критичне инфраструктуре представља један веома сложен склоп различитих стратегија, методологија, планова усмерених ка превенцији ризика и претњи, као и спречавању већих последица услед кризних ситуација. Поменути комплексни проблеми захтевају један крајње мултидисциплинарни приступ и примену наменски израђених алата кризног менаџмента ради ефикаснијег идентификовања потенцијалних ризика и претњи.

Што се тиче политике заштите КИ на наднационалном нивоу, Европска унија представља једног од кључних актера, придајући велики значај овом питању. Од 2004. године, након терористичког напада у Мадриду, државе чланице Европске уније су покренуле низ иницијатива и истраживачких програма како би се испитали различити аспекти заштите и претњи по критичну инфраструктуру, као и утицаји који оштећење критичних инфраструктура може имати на образовање, привреду, здравство, систем

комуникација и друге сегменте људске делатности. Функционисање и координација између држава чланица регулисана је Директивом ЕУ о заштити критичних инфраструктура из 2008. године, која представља добар модел и пружа могућност за преузимање одређених решења, посебно у области регулисања јавно-приватног партнерства.

Када је реч о заштити КИ на националном нивоу, највећи напредак на том пољу постигле су САД које улажу велике напоре и издвајају значајна финансијска средства намењена изградњи ефикасног система заштите КИ. Оно што је заједничко у свим стратегијама технолошки развијених земаља, јесу јасно идентификовани извори и облици угрожавања критичних инфраструктура, прецизна класификација критичних сектора, ефикасно регулисано јавно-приватно партнерство и константна модернизација информационе инфраструктуре. Међутим, ове земље суочене су са проблемом комплексности инфраструктура који иницира покретање сложенијих механизама за успостављања њихове ефикасне заштите. Поменути проблем, често може бити узрок грешке у функционисању система, о чему најбоље сведоче догађаји од 9. септембра 2001. године.

Земље у транзицији налазе се у специфичном положају, суочавајући се са дубоком трансформацијом у свим сферама. На основу спроведеног истраживања, дошли смо до резултата који потврђују раније постављене хипотезе о специфичним проблемима са којима је суочена већина транзиционих земаља по питању заштите КИ, као и до података који показују да су поједине транзиционе земље успешно унапредиле системе заштите критичних инфраструктура. Потврђена је претпоставка о неопходности изградње демократских структура као предуслова за ефикасно решавање конфликтних ситуација. Дијалог, усвајање европских система вредности и изградња мира идентификовани су кључним за успешан прелазак на демократски систем уређења.

Приликом преласка из једног друштвено-политичког система у други ове земље суочене су и са бројним проблемима који, такође, не постоје у стабилним демократским државама. Укључивање у слободно тржиште, углавном без адекватне економске државне политике, доводи до ширења сиромаштва и разочарења широких друштвених слојева, што главне доносиоце политичких одлука ставља у веома тешку ситуацију. Лоша економска ситуација често може бити узрок избијања криза, јер нагло отварање доводи до промене макроекономске структуре и пословне културе у националним економијама. Овај процес се одражава на целокупна друштва

транзиционих земаља задирући у све њене слојеве и сегменте. Наведене промене изазивају низ реакција, које се крећу од негативних до позитивних оцена овог процеса, у њиховом економском систему. У светлу процеса стабилизације, преговарања и придруживања Европској унији може се очекивати продубљивање турбулентних процеса и кризних ситуација у свим сегментима и структурама српског друштва. На ово нас упућује укупно стање српског економског и друштвено-политичког система.

Један од проблема са којим су суочене земље у транзицији, а који је повезан са стопом економског развоја, је технолошка заосталост у односу на развијене земље Запада, Европе и света. Нагли и све бржи развој информационо-комуникационе технологије, сателитских комуникација и интернета захтева континуирани технолошки развој као и константну обуку запослених, што изискује значајна финансијска средства. Земље у транзицији најчешће нису у могућности да издвоје потребна новчана средства за унапређење технологије и спровођење нових програма обуке запослених, што се директно одражава на ефикасност система управљања кризама и заштите виталних инфраструктура.

Даље, потврђена је претпоставка да већина земаља у транзицији нема јасно идентификоване изворе и облике угрожавања критичних инфраструктура, као ни прецизну класификацију критичних сектора. Застарели програми заштите критичних инфра-структура, који датирају још из доба социјализма и почивају на хладноратовским поставкама (војни извори и облици угрожавања безбедности су доминантни), не могу стати на пут савременим безбедносним изазовима и обезбедити ефикасно функционисање инфраструктура од виталног значаја. За успостављање ефикасне заштите критичних инфраструктура у земљама у транзицији неопходна је модернизација застарелих инфраструктурних објеката, која захтева високе инвестиције за реконструкцију читавих сектора.

Такође, констатовано је да један од значајнијих проблема са којим се сусрећу земље у транзицији, када је у питању управљање кризама и заштита критичних инфраструктура, представља недовршена трансформација сектора безбедности. Приватна безбедност је уско повезана са заштитом критичних инфраструктура, јер је велики број ових инфраструктурних објеката под заштитом приватних безбедносних компанија. Успешно функционисање сектора приватне безбедности у већини земаља Западног Балкана онемогућено је услед непостојања правних основа и теоријске подршке.

Овај проблем додатно је отежан неефикасним јавно-приватним партнерством (*Private-Public Partnership*). У већини земаља у транзицији значајан део инфраструктуре је у приватном власништву или у процесу приватизације, а сарадња власника инфраструктура са државним институцијама је веома лоша. Један од главних разлога оваквог стања је непостојање законског оквира који би приморао власнике и оператере да учине потребне кораке у циљу ефикасне сарадње са државним институцијама.

Нормативно, аналитичко и интензивно управљање кризом подразумева управљање свим ризицима и опасностима које запрете безбедности Републике Србије, активном применом легислативе из Европске уније и кроз регионалне иницијативе. Уз коришћење организованог и истиуционалног система планирања, управљање кризом кроз опера-тивни систем треба обезбедити услове за континуирано провођење одговарајуће припреме и одржавања потребног нивоа способности за предузимање свих мера и активности усмерених на рано упозорење, превенцију и решавање ризика и опасности које се манифестују кроз: имовину и здравље, живот људи, животиња, биљака и других материјалних добара од већих размера уништења и нормално функционисање државе који су дефинисани Уставом Републике Србије, а за које не постоје услови за објаву рата или ванредног стања. Главни фокус нашег научног истраживања био је да се објасни систем управљања кризом за критичне инфраструктуре у земљама у транзицији, у односу на превенцију, рано упозорење и отклањање последица кризе, као и предлагање новог правног решења за формирање заједничког Центра за кризни менаџмент и заштиту за хитне и кризне ситуације, што је најбоље решење за кризни менаџмент, односно управљање кризом у Републици Србији и за цео регион југоисточне Европе. То јер посебно значајн јер је Балкан осетљив на разне претње и ризике природних катастрофа, што може изазвати велике губитке и штете, како у погледу људских живота и матери-јалних и културно-историјских добара, тако и због могућих ризика и последица на Републику Србију. Систем кризног менаџмнета у Србији је функција која треба да обухвати координисане напоре и средства како би се помогло људима у декларисаним кризним ситуацијама у распону од превентивног деловања до раног упозорења и решавања кризе. Кризни менаџмент за критичне инфраструктуре у Србији још увек није на нивоу и корелацији са савременим друштвеним и глобалним политичким и свим другим збивањима, односно још увек није у складу са међународним нормама и трендовима у том погледу. У том смислу, знајући да у Републици Србији не постоји јединствен приступ за оснивање Кризног

менаџмента, а ни одговарајуће оспособљено особље, неопходно је успоставити националне мреже образовања и оспособљавања одговарајућег особља, које би својим знањем и вештинама могло допринети бољој превенцији и раном упозорење. Истовремено, увођењем информационих и комуни-кационих технологија у систем кризног менаџмента и њиховим међусобним увезивањем, брзо и правовремено би имали одговор на свим нивоима, како би се спречило ширење штете и њене последице. Процес доношења ослука треба да се промовише кроз увођење стандарда ИСО/ПАС 22399 који се односи на организацију институција са одговорностима на подручју за управљање кризним ситуацијама и стандардима на основу најбоље праксе за реализацију процеса управљања кризама.

У Републици Србији највећи проблем представља заостајање за земљама у окружењу, чланицама ЕУ. Државе чланице Европске уније доста тога су урадиле на пољу заштите КИ, између осталог формирале рачунарске тимове за реакцију на инциденте у критичним инфраструктурама – CERT (*Computer Emergenxy Response Team*). Ови тимови имају саветодавну функцију, у смислу превенције и мера заштите од инцидената који могу угрозити критичне инфраструктуре. Поред тога, велики проблем представља непостојање јасне класификације критичних сектора, као ни стратегије и закона који регулишу ову област.

На основу прегледа политика заштите критичних инфраструктура високо развијених земљама и оних које су успешно прошле транзицију (пример Словеније), представљеног у овом раду, могуће је установити модел заштите критичних инфраструктура применљив у Републици Србији. Идентификовањем кључних сектора који су заступљени у стратегијама, у скоро свим земљама са јасно дефинисаном политиком заштите критичних инфраструктура, добија се следећи предлог класификације критичних сектора:

- Енергетика (производња дистрибуција и складиштење енергената и електричне енергије),
- Информационе и комуникационе технологије (електронска комуникација, пренос података, информациони системи, пружање аудио и мултимедијалних услуга),
- Саобраћај (друмски, железнички, ваздушни, водни),
- Здравство (болнице, производња лекова),

- Воде (снабдевање пијаћом водом, бране, обрада отпадних вода, заштита вода),
- Храна (производња, снабдевање храном, безбедност хране, робне залихе),
- Финансије (банкарство, берзе, инвестиције, системи осигурања и плаћања) и
- Јавне службе (очување јавног реда и мира, заштита и спасавање, хитна медицинска помоћ).

Поред усвајања стратегије и прецизне класификације критичних сектора, потребно је унапредити систем размене информација који је неопходан за формирање ефикасне мреже *раног упозорења*. Један од кључних корака у формирању ефикасног модела раног упозорења је оснивање компјутерског тима за ванредне ситуације. У многим развијеним земљама постоје слични тимови који свакодневно блиско сарађују и граде заједничку базу података која поседује све релевантне информације о потенцијалним и стварним претњама критичној инфраструктури. Поменути тимови требало би да раде, како на превенцији, тако и на превазилажењу постојећи криза и заштити интернет окружења у земљи од ногућих сајбер напада. У оквиру модела система за узбуну потребно је идентификовати орган или институцију која би вршила координацију заједничких активности. Та улога би се првенствено односила на надзор, процену ризика, правовремено упозорење и формирање адекватног механизама реаговања уколико дође до угрожавање одређене критичне инфраструктуре. Такође, ефикасан систем раног упозорења мора у свом саставу имати (по угледу на земље са развијеним системима заштите критичних инфраструктура) центре за анализу и размену података. Главна улога ових центара била би пружање информација о претњама, рањивости и инцидентима који могу угрозити критичне инфраструктуре.

Наведеним предлозима, као полазна основа, мора претходити израда и усвајање Закона о заштити критичних инфраструктура и регулисање сарадње између приватног и јавног сектора. Услед непостојања кохерентног законског оквира (што је случај са Србијом), који би регулисао и функционисање приватно-јавног партнерства, није могуће успоставити ефикасан систем заштите критичне инфраструктуре.

Уз предложену и планирану реализацију реформи у систему управљања кризом, у складу са развијеним европским земљама, Република Србија мора изградити сопствени приступ управљања кризним ситуацијама у заштити критичних инфраструктура, узимајући у обзир расположиве капацитете и могућности. Искуства

других треба користити али их увек треба прилагодити сопственим интересима, са крајњим циљем заштите грађана и државе од ризика и опасности.

Из претходно реченог може се закључити да је спроведено истраживање отворило читав низ правних, социолошких, политиколошких питања на која ће се одговори пронаћи у будућности. Са безбедносног аспекта, пак, мишљења смо да је наше истраживање идентификовало кључне проблеме и дало смернице за даље проучавање проблематике корелације кризног менаџмента и заштите критичних инфраструктура у транзиционим земљама.

ЛИТЕРАТУРА

1. Аврамов, С., *Безбедност у 21. веку*, Зборник радова СИМВОН, Београд, 2001.
2. Acemoglu, D., Robinson, J., *Economic Origins of Dictatorship and Democracy*, CUP, Cambridge, 2006.
3. Akhmedov, A., Zhuravskaya, E., *Oportunistic Political Cycles: Testin Young Democracy Settings*, Quaterly Journalof Economics, Vol. 11, No. 4, 2004.
4. Alessina, A., Roubini, N, Cohen, G., (1997), Political Cycles and the Macroeconomy, The MIT Press, Cambridge, MA.
5. Annual Work Programme - Prevention, preparedness and consequencemanagement of terrorism and other security related risks, 2009.
6. Auerswald, P., Branscomb, L., La Porte, T., Michel-Kerjan, E., (2005), *The Challenges of Protecting CI*, Issues in Science and Technology.
7. Боин, А., Харт, П., Штерн, Е., Санделијус, Б., (2010), *Политика управљања кризама*, Факултет безбедности, Службени гласник, Београд.
8. Boin, A, Lagadec, P., Michel-Kerjan, E., Overdijk, W., (2003), *Critical Infrastructures under Threat: Learning from the Anthrax Scare*, Journal of Contingencies and Crisis Management.
9. Baldwin, D., (1997), *The Concept of Security,* Review of International Studies Vol.23, No.1.
10. Baldwin, D., (1971), *Thinking about Threats*, Journal of Conflict Resolution, Vol. 15, no. 1, March.
11. Bartlett, H., Holman, P., Somes, T., (2004), *The Art Strategy and Force Planning*, Naval War College Press, Newport.
12. Baumgartner, R., Jones, B. D., (1993), *Agendas and instability in American politics*, University of Chicago Press, Chicago.
13. Beard, C., (1934), *The Idea of National Interest*, Blue Ribbon Books, New York.
14. Bennett, B., (2007), *Understanding, Assessing and Responding to Terrorism – Protecting Cticical Infrastructure and Personnel*, The Wiley Bicentennial, Canada.
15. Бојовић, Н., Кнежевић, Н., Мацура, Д., Миленковић, М., (2010), *Модел управљања критичном инфраструктуром за одрживи развој поштанског сектора*, Симпозијум о новим технологијама у поштанском и телекомуникационом саобраћају, 18. телекомуникациони форум ТЕЛФОР Србија.
16. Borodzicz, E., (2005), *Risk, Crisis and Security Management*, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester.
17. Bošković, M., Ivković, V., Putnik, N. (2013), „Risk Management in Public-Private Partnership over Critical Infrastructures“, u: Dimitrijević, I. (editor), *National Critical Infrastructure Protection – Regional Perspective*, Univerzitet u Beogradu - Fakultet bezbednosti i Institut za korporativnu bezbednost - Ljubljana, Beograd, pp. 231-243
18. Brändström, A., Malešič, M., (2004), *Crisis Management in Slovenia: Comparative Perspectives*, Stockholm: Crismart, National Defence College.

19. Brunner, M. E., and Manuel, S., (2009), *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich.
20. Buzan, B., (1983), *People, States and Fear: The National Security Problem in International Relations*, Wheatsheaf, Birghton.
21. Bush, G. W., (2001), Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, Вашингтон, 8. октобар.
22. Весић, Д., (2008), *Економска и политичка компонента корупције*, Пројекат Министарства науке Републике Србије и Института за међународну политику и привреду, пројекат бр. 149002, децембар.
23. Вулетић, Д., (2011), *Заштита критичних информационих инфраструктура*, Зборник радова са Конференције о безбедности информација, Универзитет Метрополитан, Београд.
24. Гаћиновић, Р., (2010), *Србија – Изградња националне безбедности*, Зборник радова, Институт за политичке студије, Београд.
25. Gleick, P., (2000), *Water Conflict Chronology*, Pacific Institute, September.
26. Gleick, P.H., (1993), *Water in Crisis: A Guide to the World's Freshwater Resources*, Oxford University Press.
27. Glenny, M., (2011), *The Cyber Arms Race Has Begun*, The Nation, October 31.
28. Gonzalez-Herrero, A, Pratt ,C. B., (1995), *How to manage a crisis before or whenever - it hits*, Public Relations Quarterly, 40(1).
29. Gospic, N., Muric, G., Bogojevic, D., (2012), *Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia*, International Conference on Applied Internet and InformationTechnologies, Zrenjanin, October.
30. Gottschalk, J., (2002), *Crisis Management*, Capstone Publishing, Oxford.
31. Grigg Neil, S., (2002), *Surviving Disasters in Water Utilities: Learning from Experience.* Denver, CO: American Water Works Association.
32. Greenwald, A. G., (1980), *The totalitarian ego: Fabrication and revision of personal history*, American Psychologist 35.
33. Le Grand, G., Springinsfeld, F., Riguidel, M., (2003), *Policy Based Management for Critical Infrastructure Protection*, ACIP Project, Founded by the EU Commission.
34. Daasse, C., Kessler, O., (2007), *Knowns and Unknowns in the War in Terror: uncertainty and the political contruction of danger*, Security Dialogue, vol. 38, December.
35. Decision of the Japanese Advanced Information and Telecommunications Society Promotion Headquarters, 9 November, 1998.
36. Decree of the President of the Russian Federation No. 1013, 7 August, 2004: Issues of the Federal Guard Service of the Russian Federation, with Amendments and Additions of 28 December 2004, 22 March and 1-6 October 2005.
37. Porter, D. G., (2001), *The Who, What, Why, and How of Counterterrorism Issues*, American Water Works Association.

38. Department of Homeland Security, Information Technology: *Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*, Washington, 2007.
39. Didier, P., Macias, F., Harstad, J., Antholine, R., Johnston, S.A., Piyevsky, S., Schillace, M., Wilcox, G., Zaniewski, D., Zuponcic, S., (2011), Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, CISCO Systems and Rockwell Automation, September.
40. Димитријевић, В., (1973), *Појам безбедности у међународним односима*, Савез удружења правника Југославије, Београд.
41. Doctrine of the Information Security of the Russian Federation, approved by the president of the Russian Federation, Vladimir Putin, 2000.
42. Donzelli, P., Setola, R., (2001), Putting the Customer at the Center of the IT System, Case Study, Euro-Web 2001 Conference – The Web in the Public Administration, Pisa, Italy, 18-20 December.
43. Дулић, Д., (2006), *Људска безбедност 1*, Фонд за отворено друштво, Београд.
44. Duffield, R., (2001), *Global Governance and the New Wars: The Merging of Development and Security*, Palgrave Macmillan, New York.
45. Dunn, M., Mauer, V., (2006), *International Critical Information Infrastructure Protection Handbook*, ETH Center for Conflict Studies, vol. I, Zurich.
46. EBRD, Business Environment and Enterprise Performance Survey, 1999.
47. EBRD, *Transition Report* 2005, and *Transition Report* 2010.
48. Edict no. 314 of the president of the Russian Federation of 9 March 2004 on the System and Structure of Federal Executive Bodies.
49. Ејдус, Ф., *Међународна безбедност: теорије, сектори и нивои*, Службени гласник, Београдски центар за безбедносну политику, Београд, 2012.
50. Eriksson P, Barck-Holst S., *Critical Infrastructure Protection policy in the EU and in Sweden – comparative analysis*, FOI, Stockholm, 2005.
51. Alain, E., Ranck, H., and Schmitt, B., (2005), *Information security. A new challenge for the EU*, Chaillo, Paper no. 76, Paris, March.
52. Brunner, E. M., and Suter, M., (2009), *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich.
53. Elliot, W., (1935), *The Idea of National Interes*, Harvard Law Review Vol. 48, No. 4.
54. European Network and Information Security Agency (ENISA), Slovenia Country Report, May 2011.
55. Emercom, administrativeorderno. 2-4-60-10-14, Методические рекомендации по проведению инвентаризации критически важных и потенциально опасных объектов РФ и формированию оеречения критически важных объектов на регинальном уровне, 2008.
56. Ennen, G., (2001), *CERT-Bund – eine neue Aufgabe des BSI*, Bones.
57. Engelbrekt, K., Fröberg, M., (2005), *Managing Political Crises in Bulgaria: Pragmatism and Procrastination*, Elanders Gotab, Stockholm.

58. Erwann, M.K., (2003), *New Challenges in CI: A US Perspective*, Journal of Contingencies and Crisis Management, Vol.11, No.3.

59. EU: *A Secure Europe in a Better World – The European Security Strategy*, 12 December 2003.

60. European Network and Information Security Agency (ENISA). Work Programme 2008: "*Build on Synergies – Achieve Impact*".

61. European Commissions Internal Working Paper, Guidelines for implementation of the Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

62. European Commissions Internal Working Paper (2008) European reference network for critical infrastructure protection.

63. Ezell, C.B., (2007). *Infrastructure Vulnerability Assessment Model (I-VAM)*, Risk Analysis Vol. 27, No.3.

64. Hodge G. A., Greve C. (2007), Public-Private Partnerships: An International Performance Review, Public Administration Review.

65. *Intelligence Warning Terminology*, Joint Military Intelligence College, Washington DC, October 2001.

66. Zakon o osnovnim administrativnim procedurama e-Vlade Slovenije, Official Gazette of the Republic of Slovenia, no. 24/2006 - ZUPUPB2.

67. Zakon Republike Slovenije o elektronskim komunikacijama, Slovenian Electronic Communications Act (ZEKom-UPB1).

68. Зец, М., Церовић, Б., (2008), *Куда иде Србија? – остварење и домети реформи*, Научно друштво економиста и Економски факултет у Београду.

69. Zimmerman, R., (2004), *Decision-making and the Vulnerability of Interdependent Critical Infrastructure*, IEEE Control Systems Magazine.

70. Иванов, М., (2012), Совет федерации занялся цифровым суверенитетом, *Коммерсант*.

71. Jarlsvik, H, Castenfors, K., (2004), Security and Preparedness in the EU, Stockholm.

72. Jeraj, J., (2003), Civil Protection, the Protection and Rescue System, the System for Protection Against Natural and Other Disasters – Development and Place int the National Security System (with an emphasis on the case of Slovenia).

73. Johnson, D, Elizabeth M. P. Madin, (2008), *Paradigm Shifts in Security Strategy, Why Does It Take Disasters to Trigger Change*, in coll. of papers Natural Security.

74. Johnson, D., Tierney, D.R., (2006), *Failing to win: Perceptions of victory and defeat in international politics*, Harvard University Press, Cambridge.

75. Jovanović, B., (1997), *Policija i sigurnost*, Revija, br. 1-2, Zagreb.

76. Kaspersen, A. T., Sending, O. J., (2005), *The United nations and Civilian Crisis Management*, Norwegian Institute of international Affairs, May.

77. Kalser, P, (2012), *Estonia and the Birth of Cyberwar*, Presentation at Aleksanteri Institute.

78. Кегли, Ч., Виткоф, J., (2004), *Светска политика – тренд и трансформација,* Факултет политичких наука, Београд.

79. Kennan, G., (1966), *Realities of American Foreign Policy*, Norton, New York.

80. Кешетовић, Ž, Toth, I., (2012), *Problemi kriznog menadžmenta*, Veleučilište Velika Gorica, Velika Gorica.

81. Кешетовић, Ж.., (2008), *Кризни менаџмент*, Факултет безбедности, Службени гласник, Београд.

82. Кешетовић, Ж., Кековић, З., (2006), *Кризни менаџмент 1, Превенција кризе*, Факултет безбедности, Београд.

83. Kešetović Ž. (2013), "Country study Serbia", report within ANVIL project - European Union's Seventh Framework Programme FP7/2007-2013 under grant agreement n°28467.

84. Engelbrekt, K., and Förberg, M., (2005), *Managing Political Crises in Bulgaria*,

a. Elanders Gotab, Stockholm.

85. Koubatis, A, Schonberger, J.Y., (2005), Risk Management of Complex Planning Framework, Safety Science.

86. Kremer, A., (2004), *Cyber Security in Russia*, Presentation held at ITU-T Cybersecurity Symposium, Florianopolis, Brazil, October.

87. Kuipers, D., Fabro, M., (2006), *Control Systems Cyber Security: Defense in Depth Strategies*, Idaho National Library, May.

88. Kuhn, S.T., (1970), *The Structure of Scientific Revolutions*, Chicago University Press, Chicago.

89. Land, K. C., (2001)., *Models and Indicators*, Social Forces, Vol. 80, No. 2

90. LaPorte, T.R., (2007), *Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise*, Journal of Contingencies and Crisis Management, Volume 15 Number 1, March.

91. Larsson, R., *Tackling Dependency: The EU and its Security Chalenges*, Swedish Defense Research Agency, 2007.

92. Lay, M.G., (1992), *Ways of the World*, Primavera Press, Sydney.

93. Леонтьев А.А., (1997), *Основы психолингвистики*, Институт "Открытое общество", Москва.

94. Lewis, T.**,** (2006), *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Wiley Interscience, New Jersey.

95. Li, Hao et al, (2005), Strategic Power Infrastructure Defense, *Proceedings of the IEEE*.

96. Lindstrom, M., (2008), *A review of four EU member states views on the European programme for critical infrastructure protection*, Swedish Emergency Management Agency- English edition, Stockholm.

97. Lindstrom, M., (2008), *National consequences of the European programme for critical infrastructure protection*, Swedish Emergency Management Agency - English edition.

98. Lomborg, B., (2001), *The Skeptical Environmentalist*, Cambridge University, Cambridge.

99. Љешевић, М. (1990), *Метод моделовања у истраживању животне средине*, СГД, Београд.

100. Macaulay, T., (2008), *Critical Infrastructure - Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies*, CRC Press, London.

101. Making the Nation Safer: the Role of Science and Technology in Countering Terrorism, *the National Research Council*, Washington D.C., 2002.

102. Маринковић, Д., (1998), *Основе прикупљања података и управљања*, Микроелектроника, бр. 1, Београд.

103. МЦХС Росии, Прогноз чрезвичайной обстановки на территории РФ на 2012. год, Центр *Антистихия*, Москва, 2011.

104. Massoud, A., (2002), "Security Challenges for the Electricity Infrastructure (Supplement to Computer Magazine)", *Computer* (IEEE computer society), 2002-04.

105. Медаковић, Р., (2007), *ИКТ индустрија као доминантна привредна грана у Србији*, ИТ сектор Привредне коморе Србије, Магазин Е-волуција.

106. Мијалковски, М., Ђорђевић, И., (2006), *Ризик – специфичан облик угрожавања безбедности*, Универзитет у Београду, Факултет безбедности.

107. Милановић, Г., (2010), *Кризни менаџмент у земљама у транзицији*, Докторска дисертација, Факултет безбедности, Београд.

108. Milburn, W., Watman, H., (1981), *On the Nature of Threat: a Social Psychological Analysis*, New York: Praeger.

109. Милетић, А., (1977), *Национални интерес у америчкој теорији међународних односа*, Докторска дисертација, Факултет политичких наука, Београд.

110. Михаилов, А., (2010), *Критичесская инфраструктура оказалась в кибероп асности*, Business FM, 17 November.

111. Mitroff, I., (2000), *Managing Crises before they happen: What every executive and manager should know about crisis management*, AMACOM, New York.

112. Molden, D., (2007), *Water for food, Water for life: A Comprehensive Assessment of Water Management in Agriculture*, Earthscan/IWMI.

113. Morgenthau, H., (1975), *Politics among Nations*, 5 th edition, Knopf, New York.

114. Московљевић, М., (2006), Речник савременог српског књижевног језика с језичким саветником, Гутенбергова галаксија, Београд.

115. Moteff, D., Parfomak, P., (2004), *Critical Infrastructure and Key Assets: Definition and Identification*, Congressional Research Service, Library of Congress.

116. National Strategy for Critical Infrastructure Protection (CIP Strategy), Federal Republic of Germany, Federal Ministry of the Interior, Berlin, 17. jun, 2009.

117. Nickolov, E., (2005), *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations study, case of Bulgaria,* Information and Security Journal, Vol. 17.

118. Noakes, T., D., Goodwin, N., Rayner, B. L., (1985), *Water intoxication: a possible complication during endurance exercise*, Med Sci Sports Exerc num. 17.

119. Народна скупштина Републике Словеније, *Резолуција о стратегији националне безедности Републике Словеније*, 2001.

120. Народна Скупштина Републике Словеније, *Закон о заштити од природних и других катастрофа Републике Словеније*,1994.

121. Народна скуштина Републике Словеније, *Доктрина цивилне одбране Републике Словеније*, 2002.

122. Народна скупштина Републике Словеније, *Закон о одбрани Републике Словеније*, 1994.

123. National Information Security Center (NISC), Japanese Government's Efforts to Address Information Security Issues – Focusing on the Cabinet Secretariat's Efforts, Chapter 3.1 - Standards for Information Security Measures for the Central Government Computer Systems.

124. Official Journal of the European Union, Commission Decision on establishing the European Research Advisory Board, 22 April 2005.

125. Outline of the First Follow-up of the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society in Japan, May 2000.

126. Papa, M., and Shenoi, S., (2008), *Critical Infrastructure Protection II*, International Federation for Information Processing, New York.

127. Pearson, C., Clair, J., (1998), *Reframing Crisis Management*, *Academy of Management Review*. Vol. 23, No 1.

128. Pereboom, J., (2001), *Infrastructure Interdependencies: Overviews of Concepts and Terminology*, Infrastructure Assurance Center, Argonne.

129. Perrow, C., (1984), *Normal Accidents: Living with High-Risk Technologies*, Basic Books, New York.

130. Prezelj, I., and Kustec Lipicer, S., (2010), *Public and Policy Management of Critcal Infrastructure: Lessons from Integral Nations Cross-Sectoral Scanning in Slovenia*, IRSPM Conference, Panel: Risk and Crisis Management in the Public Sector, Berne.

131. Podbregar, I., Lobnikar, B., Ivanuša, T., Banutai, E., (2012), *Critical Infrastructure and Public-Private Partnership*, Tne Ninth Intenational Conference on Criminal Justice and Security in Central and Eastern Europe – Contemporary Criminal Justice Practice and Research, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, September.

132. Pynnöniemi, K., (2012), *Russian critical infrastructures – vulnerabilities and policies – The evolution of Russian policy on critical infrastructure protection*, The Finish Institute of International Affairs.

133. Поповић, Д., (2003), *Добитници и губитници у транзицији*, Политика, Економетар, бр. 16, септембар.

134. Постановление Правительство РФ, О Федеральной целевой программе снижения рисков и смягчение последствий чрезвичайных ситуаций природного и техногенного характера в Росийскои Федерации до 2010. года, январь 2006.

135. Постановление Правительство РФ, но. 1094., О классификации чрезвичайных ситуаций природного и техногенного характера, сентябрья 1996.

136. Постановление Правительство РФ но. 304, О класификации чрезвичайных ситуаций природного и техногенного характера, май 2007.

137. Постановление Правительство РФ, О Федеральной целевой программе снижения рисков и смягчения последствий чрезвичайных ситуаций природного и техногенного характера в Росийской Федерации до 2015. года, no. 555, июля 2011.

138. Правительство РФ, Концепция Федеральной целевой программы снижения рисков и смягчения последствий чрезвичайных ситуаций природного и техногенного характера в Росийской Федерации до 2015. года, распоряжение но. 534, 2011.

139. Правительство Росийской Федерации, О федеральной целевой программе – Снижение рисков и смягчение последствий чрезвичайных ситуаций природного и техногенного характера в Росийской Федерации до 2005. года, Постановление no. 1098, Сентябрь, 1999.

140. Президент РФ В. Путин, указ Пр-2194. Основы государственной политики в области обеспечения химической и биологической безопасности РФ на период до 2010. года и дальнейшую перспективу, 2003.

141. Президент РФ В. Путин, Основы государственной политики в области обеспечения безопасности населения РФ и защищености критически важных объектов и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов, 2006.

142. Протић, Д., (2012), *Стратегија развоја информационог друштва у Републици Србији до 2020. године: безбедност информација и критична инфраструктура*, Војно-технички гласник, Београд.

143. Поляков, Р., (2003), *Владимир Рушаило обсудил проблеми национальной безопасности Росии*, Коммерсант (Воронеж).

144. Ravindranath, N. H., Sathaye, A. J., (2002), *Climate Change and Developing Countries*, Springer.

145. Radvanovsky, R., McDougall, A., (2010), *Critical Infrastructure, Homeland Security and Emergency Preparedness*, Second edition, CRC Press, Taylor & Francis Group, New York.

146. Reinermann, D., Weber, J., (2003), Analysis of Critical Infrastructures: The ACIS Methodology, Federal Office for Information Security, Bonn, Germany.

147. Report on the implementation of the European security strategy: providing security in a changing world, Brussels, 11 December 2008.

148. Rhoades R.A, Tanner G.A., *Medical Physiology* (2nd ed). Baltimore: Lippincott Williams & Wilkins, 2003.

149. Rodda, J. C., Ubertini, L., (2004), *the Basis of Civilization - Water Science?* International Association of Hydrological Sciences (International Association of Hydrological Sciences Press.

150. Roehrs, P., (2005), *Weak States and Imlications for Regional Security: A case study of Georgian instability and Caspian regional in security*, Research paper No. 97, Research Institute for European and American studies.

151. Simon, S., Benjamin, D., (2000), America and the new terrorism, Survival, Vol. 42, Taylor & Francis.

152. Schacter, D. L., (1995), *Memory distortion: How minds, brains, and societies recontruct the past*, Harvard University Press, Cambridge.

153. Schivelbusch, W., (2004), *The culture of defeat: On national trauma, mourning, and recovery*, Picador Press, New York.

154. Schot, J., (2003), *Transnational Infrastructures and the Rise of Contemporary Europe*, working Doc No.1, January.

155. Симић, Д., (2002), *Наука о безбедности – савремени приступи безбедности,* Службени лист СРЈ, Београд.

156. Стајић, Љ., (2004), *Основи безбедности*, Полицијска академија, Београд.

157. Стајић, Љ., (2008), *Основи система безбедности*, Правни факултет, Нови Сад.

158. Statute on the Federal Security Service of the Russian Federation and Structure of the Federal Security Service Agencies, approved by presidential edict no. 960, 2003.

159. Stern, E. K, Hansen, D., (2004), *The Latvian Experience – Crisis Management in a Transitional Society*, Elanders Gotab Ab, Vallingby.

160. Stoessinger, J. G., (1998), *Why nations go to war*, St. Martin's Press, New York.

161. Tadjibayev, F. A., Sattarova, F. Y., (2009), *Categorization of Critical Infrastructures and Critical Information Infrastructures*, International Journal of Advanced Science and Technology, Volume 8.

162. Tagarev, T., (2006), The Art of Shaping Defense Policy: Scope, Components, Relationships (but no algorithms), The Quarterly Journal 5 no.1, Spring-Summer.

163. Tagarev, T., Pavlov, N., (2007), *Planning Measures and Capabilities for Protection of Critical Infrastructure in Bulgaria*, Information and Security Journal, Vol. 22.

164. The President's Commission on Critical Infrastructure Protection (PCCIP),"Critical Foundations: Protecting America's Infrastructures", Washington, 1997.

165. The White House, "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", Washington, 2003.

166. Timothy, L.T., (2001), Information Security Thinking: A Comparison of U.S, Russian and Chinese Concepts.

167. Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322.

168. Thissen, A. H., Paulien, M. W., and H., (2003), *Critical Infrastructures – State of the Art in Research and Application*, Kluwer's International Series Academic Publishers, Boston.

169. Trostle, R., (2008), *Global Agricultural Supply and Demand: Factors Contributing to the Recent Increase in Food Commodity Prices*, Economic Research Service/USDA.

170. True, J. L., (2002), *The changing focus of national security policy*, Policy Dynamics, Chicago: University of Chicago Press.

171. UNEP International Environment, Environmentally Sound Technology for Waste water and Storm water Management: An International Source Book, 2002.

172. UNESCO, *Water, a shared responsibility*, The United Nations World Water Development Report 2, 2006.

173. UNISYS, Study on the establishment of the critical infrastructure warning information network (CIWIN). Interim report. Approved version. Contract Number: JLS/D1/2006/02 ABA Number: 30-CE-0080088/00-03.

174. Ušeničnik, B., (1999), *Protection Against Natural and Other Disasters in Slovenia*, Ljubljana: Administration of the Republic of Slovenia for Civil Protection and Disaster Relief, Ministry of Defense.

175. Farazmand, A., (2001), *Handbook of Crises and Emergency Management*, Marcel Dekker, Inc, New York.

176. Federal Target Program, "Electronic Russia (2002–2010)", approved by the government of the Russian Federation, Decree No. 65, 28 January 2002.

177. Filippov, S., (2005), *Policy for ICT Adoption in Moscow*, "Electronic Moscow" Programme, Institute of the Information Society.

178. Friedman, T., (2002), *Longitudes and Attitudes: Exploring the World After September 11*, New York: Farrar Straus & Giroux.

179. Федеральный Закон О защите населения и территории от чрезвичайных ситуаций природного и техногенного характера, no 68-ФЗ, Декабря 1994.

180. Haimes, Y.Y, Longstaff, T., (2002), *The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism*, Risk Analysis, Vol. 22, No.3, Oxford.

181. Hadfield, C., (1986), *World Canals (First ed.)*, David & Charles Press, London.

182. Hellstrom, T., (2007), *Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework*, National Emergency Training Center.

183. Homeland Security of the U.S., Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies, October 2009.

184. Hyslop, M., (2007), *Critical Information Infrastructures Resilience and Protection*, Spronger, UK, Springer Science.

185. Цаликов, Р., Акимов, В. А., Козлов, А., (2009), *Оценка природной, техногенной и екологической безопасности Росии*, ФГУ, МЦХС Росии.

186. Clarke, R., Knake, R., (2010), *Cyber War – The next treat to National Security and What to do about it*, Harper Collins e-books.

187. Crane, D., (1992), *The Production of Culture*, Sage Publ.

188. Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576 final, Brussels, 17 November 2005.

189. Commission of the European Communities. Critical Infrastructure Protection in the Fight against Terrorism, COM (2004)702 final, Brussels, 20 October 2004.

190. Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17 November 2005.

191. Commission Report Results of the EPCIP Green Paper consultation responses of them emberstates. JLS/D1/PR/vdb D (2006) 4675, Brussels, 14 March 2006.

192. Communication from the Commission to the Council and the European parliament, Critical infrastructure protection in the fight against terrorism, Brussels, 20 October 2004.

193. Concept of National Security of the RF, approved by Presidential decree no. 24, 10 January 2000.

194. Concept of National Security of the RF, approved by Presidential decree no. 130, 17 December 1997.

195. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

196. Craddock, R. J., (2006), *Crisis Management Models and Timelines*, Thales Research and Technology (UK), White Paper.

197. Crampton, J., Elden S., (2007), *Space, Knowledge and Power: Foucault and Geography*, Ashgate, Hampshire.

198. C., von Hirschhausen, and Meinhart, B., (2001), *Infrastructure Policies and Liberalization in the East European Transition Countries: Would Less Have been More?,* Proposal for the Annual Congress of the European Economic Association Université de Lausanne, Switzerland.

199. Chartres, C., Varma, S., (2010), *Out of water - From Abundance to Scarcity and How to Solve the World's Water Problems*, FT Press, USA.

200. Цукић, Н., Кисић, С., Мандић-Лукић, Ј., (2012), *Безбедност SCADA система*, Извештај са 11. скупа Инфотех Јахорина, март.

201. Van Evera, S., (1998), *Hypothesys on nationalism and war*, International Security 18.

202. Water Governance, Water Issue Brief, Issue 5, 2010.

203. Wenger, A., Metzger, J., Dunn, M., M., (2004), *International CIIP Handbook,* Center for Security Studies at the Swiss Federal Institute of Technology, Zurich.

204. Welle, K., Evans, B., Tucker, J., Nicol, A., (2008), *Is Water Lagging Behind on Aid Effectiveness?* Briefing paper.

205. Wendt, A., (1999), *Social Theory of International Politics*, Cambridge University Press, Cambridge.

206. Wight, M., (1977), *System of States*, Leicester University Press, Leicester.

207. Williams, D. E. & Olaniran, B. A., (1998), *Expanding the Crisis Planning Function: Introducing Elements of Risk Communication to Crisis Communication Practice*, Public Relation Review, 24 (3).

208. Clinton, J. W., (1998), *Protecting America's Critical Infrastructures: Presidential Decision Directives 62 and63*, Washington.

209. Clinton, J. W., (2010), *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0*, An Invitation to a Dialogue, Washington.

210. Winston, B., (1998), The Telegraph in Media Technology and Society, A History: From the Telegraph to the Internet, Routledge Publications, London.

211. World Water Assessment Program, International World Development Report, 2003.

212.9/11 Public Discourse Project, Final report on 9/11 Commission recommendation, 2005.

Интернет извори:

1. Талијан, М., *Менаџмент и безбедност: Прве установе приватне безбедности у Србији.* http://www.gmbusiness.biz/index.php/arhiva/3140/gm_32/prve_ustanove_privatne_bezbednosti_u_srbiji.html 13.05.2011.
2. http://sr.scribd.com/doc/99579355/6025-Odnosi-s-Javnoscu-u-Kriznim-Situacijama 13.05.2011.
3. Каровић, С., Комазец, Н., Ђурић, Н., *Подручје одбрамбене делатности као предмет истраживања кризног менаџмента.* http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2011-leto/25.%20Podrucje%20odbrambene%20delatnosti%20kao%20predmet%20istrazivanja%20kriznog%20menadzmenta;%20Samed%20Karovic,%20Nenad%20Komazec%20i%20Nenad%20Djuric.pdf, 13.05.2011.
4. Global security, https://www-gs.llnl.gov/, 13.05.2011
5. Global Economic Crisis, A Publication of Yale Center for the Study of Globalization, Yale Global Online, http://yaleglobal.yale.edu/content/global-economic-crisis, 11.12.2012
6. Гаћиновић, Р.: *Класификација безбедности*, Зборник радова НБП, Криминалистичко-полицијска академија, Београд, 2007. http://www.kpa.edu.rs/data/akademija/nbp/nbp_2007_2.pdf, 13.05.2011.
7. UNDP, Human Development Report 1994, Oxford University Press, New York, 1994. http://hdr.undp.org/en/media/hdr_1994_en_contents.pdf, 13.05.2011.
8. USA PATRIOT ACT: http://www.epic.org/privacy/terrorism/hr3162.html, 13.05.2011.
9. Department of Homeland Security. "National Infrastructure Protection Plan", Washington, 2006, http://cipp.gmu.edu/archive/NIPP_Plan6-06.pdf, 13.05.2011.
10. The White House, "National Strategy for Homeland Security", Washington, http://www.whitehouse.gov/infocus/homeland/ nshs/NSHS.pdf, 13.05.2011.
11. The White House, "Homeland Security Presidential Directive/HSPD-7", Washington, 2003, http://www.whitehouse.gov/news/releases/2003/12/200312175.html, 13.05.2011.
12. "Department of Homeland Security", http://www.dhs.gov/critical-manufacturing-sector, 13.05.2011.
13. George, W. Bush, "*Executive Order 13231*", *Critical Infrastructure Protection in the Informaion Age* Washington, 2001. http://www.fas.org/irp/offdocs/eo/eo-13231.htm
14. The White House, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

15. Office of Homeland Security, "*National Strategy for Homeland Security*", Washington, 2002. http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf, 13.05.2011
16. The White House, "*National Strategy to Secure Cyberspace*", Washington, 2003. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf, 13.05.2011
17. The White House, "*National Strategy for Information Sharing*", Washington, 2007. http://www.whitehouse.gov/nsc/infosharing /NSIS_book.pdf, 13.05.2011
18. Department of Homeland Security, http://www.dhs.gov, 17.11.2012
19. Official website of the Department of Homeland Security, http://www.dhs.gov/xabout/structure/index.shtm, 17.11.2012
20. Department og Homeland Security, "*About the National Protection and Programs Directorate*", http://www.dhs.gov/xabout/structure/editorial_0794.shtm, 17.11.2012
21. Department of Homeland Security, "*Office of Infrastructure Protection*", http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm, 17.11.2012
22. Department of Homeland Security, "*Office of Cybersecurity and Communications*", http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm, 17.11.2012
23. Department of Homeland Security, National Communications System – "*Background and Hystory of the NCS*", http://www.ncs.gov/about.html, 17.11.2012
24. Department of Homeland Security, http://www.dhs.gov/xabout/structure/editorial_0839.shtm, 17.11.2012
25. Department of Homeland Security, "*About the Office of Emergency and Communications*", http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm, 17.11.2012
26. U.S. House of Representatives, Committee on Land Security, http://homeland.house.gov/about/index.asp, 17.11.2012
27. United States Senate – Committee on the Judiciary, http://judiciary.senate.gov, 17.11.2012
28. United States Senate – Committee on the Judiciary,
29. http://judiciary.senate.gov/subcommittees/110/technology110.cfm, 17.11.2012
30. United States Government Accountability Office (GAO), "*Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sectors*", 2004, http://www.gao.gov/new.items/d04780.pdf, 17.11.2012
31. United States Government Accountability Office (GAO*), "Report to the Congressional Requesters, Information Security. Emerging Cybersecurity Issues Threaten Federal Information Systems*", 2005, http://www.gao.gov/new.items/d05231.pdf, 17.11.2012
32. United States Government Accountability Office (GAO), "*Critical Infrastructure ProtectionDepartment of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*", 2005, http://www.gao.gov/new.items/d05434.pdf, 17.11.2012
33. U. S. Department of Defense, http://www.defenselink.mil/cio-nii/index.shtml, 17.11.2012

34. Information Technology, Information Sharing and Analysis Center (IT-ISAC), https://www.it-isac.org, 17.11.2012
35. U. S. National Coordinating Center for telecommunications (NCC), http://www.ncs.gov/ncc, 17.11.2012
36. U. S. North American Electric Reliability Corporation, http://www.nerc.com/cip.html, 17.11.2012
37. Financial Services, Information, Sharing and Analysis center, http://www.fsisac.com, 17.11.2012
38. National Cyber Security Alliance, http://www.staysafeonline.org, 17.11.2012
39. National Cyber Security Partnership, http://www.cyberpartnership.org, 17.11.2012
40. On Guard Online, http://onguardonline.gov/index.html, 17.11.2012
41. Federal Bureau of Investigation, http://www.fbi.gov/hq/lab/org/cart.htm, 17.11.2012
42. Okinawa Charter on Global Information Society, Okinawa, 22 July 2000, http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm, 17.11.2012
43. Сајт државног информатичко-статистичког система Русије, одељак са подацима о ванреднимситуацијама, http://www.fedstat.ru/indicator/data.do?id=41317&referrerType=0&referrerId=947198, 23.01.2013
44. Министарство за ванредне ситуације Русије, http://www.mchs.gov.ru/stats/index.php?SectIoN_Id=253, 23.01.2013
45. "Doctrine of the Information Security of the Russian Federation". approved by the president of the Russian Federation, Vladimir Putin, 2000, http://www.medialaw.ru/e_pages/laws/project/d2-4.htm, 29.11.2012
46. Official portal of the President of Russian Federation, "Security Council", http://www.kremlin.ru/eng/articles/institut04.shtml, 23.01.2013
47. Помоћни сајт владе Русије са електронским сервисима и елктронском аминистрацијом, http://www.e-rus.ru, 23.01.2013
48. Оффициальная Интернет страница Совета Безопасности РФ, http://www.scrf.gov.ru, 23.01.2013
49. Оффициальная Интернет страница Федеральной службы безопасности РФ, http://www.fsb.ru, 23.01.2013
50. Оффициальная Интернет страница Партнерства для развития информационного общества в России, http://prior.russia-gateway.ru, 23.01.2013
51. Центр Права и средства массовой информации, http://new.medialaw.ru, 23.01.2013
52. Gleick, Peter, "Water Conflict Chronology (September 2000 Version)". Pacific Institute. http://www.worldwater.org/conflict.htm, 29.11.2012
53. Denileon, Gay Porter, "The Who, What, Why, and How of Counterterrorism Issues". American Water Works Association, 2001. http://www.awwa.org/Advocacy/public_ep/may.pdf, 29.11.2012

54. Hickman, Donald, "A Chemical And Biological Warfare Threat: USAF Water Systems at Risk". Maxwell Air Force Base, Air University (U.S. Airforce). http://www.au.af.mil/au/awc/awcgate/cpc-pubs/hickman.htm, 29.11.2012
55. MDG Report 2008, http://mdgs.un.org, 29.11.2012
56. G8 Action plan decided upon at the 2003 Evian Summit, http://www.g8.fr/evian/english/navigation/2003_g8_summit/summit_documents/water_-_a_g8_action_plan.html, 29.11.2012
57. World Health Organization, Safe Water and Global Health, http://www.who.int/features/qa/70/en, 29.11.2012
58. WBCSD Water Facts & Trends, http://www.wbcsd.org/includesgetTarget.asp?type?=d&id=MTYyNTA, 29.11.2012
59. Water Use in the US, National Atlas.gov, http://www.nationalatlas.gov/articles/water/a_wateruse.html, 29.11.2012
60. Get Safe Online, Free epert advice, http://www.getsafeonline.org, 29.11.2012
61. Information Security Policy Council of Japan, Action Plan on Information Security Measures for Critical Infrastructures, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf, 29.11.2012
62. Strategy of Information Security of Japan, http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf, 29.11.2012
63. The First National Strategy on Information Security "Toward the realization of a trustworthy society", http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf, 29.11.2012
64. Secure Japan 2006, First Step Towards a Trustworthy Society, http://www.nisc.go.jp/eng/pdf/sj2006_eng.pdf, 23.01.2013
65. Special Action Plan on Countermeasures to Cyber-terrorism of critical infrastructure in Japan, 2000, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN009986.pdf, 23.01.2013
66. Commission of the European Communities, Critical Infrastructure Protection in the Fightagainst Terrorism (Brussels, 20 October 2004), COM(2004)702 final, http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf, 23.01.2013
67. Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM(2005) 576 final, http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf, 23.01.2013
68. European Commission, "Communications Networks, Content and Technology", http://ec.europa.eu/dgs/information_society/index_en.htm, 23.01.2013
69. European Commission, "Justice – Building a European Area of Justice", http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infra- struct_en.htm, 23.01.2013

70. European Union Law**,** Proposal for a DIRECTIVE OF THE Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0787:EN:NOT23.01.2013

71. EU Council Resolution on the protection of critical information infrastructure, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf, 23.01.2013

72. European Commission, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm, 23.01.2013

73. European Network and Information Security Agency (ENISA), 2006:http://www.enisa.europa.eu/doc/pdf/deliverables/wiw_v2_2006.pdf, 23.01.2013

74. European Network and Information Security Agency (ENISA), ENISA Inventory of CERTActivities in Europe - Version 1.5, September 2007, http://www.enisa.europa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf, 23.01.2013

75. European Commission, "Research and Innovation", http://ec.europa.eu/research/future/themes/index_en.cfm, 23.01.2013

76. Community Research and Developement Information Service, http://cordis.europa.eu/,23.01.2013

77. European Security and Research & Inovation Forum, http://www.esrif.eu, 23.01.2013

78. Critical Information Infrastructure Research Co-ordination Project, http://www.ci2rco.org, 23.01.2013

79. Report on the Economic Evaluation of the Data Protection Directive 95/46/EC,

http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf , 23.01.2013

80. Belgian Institute for postal services an Telecommunications, http://www.bipt.be/ShowDoc.aspx?objectID=1020&lang=en, 23.01.2013

81. Treaty of Lisbon, http://europa.eu/lisbon_treaty/full_text/index_en.htm, 23.01.2013

82. Bulgaria National policy response during disasters and accidents, www.mdpba.government.bg, 23.01.2013

83. Annual Work Programme - Prevention, preparedness and consequence management of terrorism and other security related risks, 2009, http://ec.europa.eu/justice_home/funding/cips/doc/awp_cips_2009_en.pdf, 23.01.2013

84. Council Directive (2008/114/EC of 8 December 2008), The identification and designation of European critical infrastructure and the assessment of the need to improve their protection, http://www.infrastrutturecritiche.it/aiic/images/DocArticoli/directive%20epcip%20en_12_01_2009.pdf, 23.01.2013

85. Making the Nation Safer, The Role of Science and Technology in Countering Terrorism, The National Research Council, Washington D.C, 2002, http://www.nap.edu, 23.01.2013

86. Стратегија развоја Словеније (2006-2013), http://www.slovenijajutri.gov.si/fileadmin/urednik/dokumenti/Slovenia___s_Development_Strategy.pdf, 23.01.2013

87. Стратегија развоја сервиса е-Владе Словеније, http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/mju_dokumenti/english/SEP2010_english_final.doc, 23.01.2013

88. Акциони план развоја сервиса е-Владе Словеније, http://e-uprava.gov.si/eud/euprava/akcijski_nacrt_e-uprave_2010.doc, 23.01.2013

89. Закон Републике Словеније о електронским комуникацијама, Slovenian Electronic Communications Act (ZEKom-UPB1), http://www.apek.si, 23.01.2013

90. Закон Републике Словеније о е-трговини и електронском потпису, http://www.uradnilist.si/1/objava.jsp?urlid=200425&stevilka=1066, 23.01.2013

91. Кодекс понашања оператера јавних мобилних електронских комуникација везан за безбедније коришћење мобилне комуникације од стране млађих тинејџера и деце у Словенији, http://www.gsmeurope.org/documents/eu_codes/Slovenian_code_of_conduct.pdf, 23.01.2013

92. Slovenia - ENISA CERT Directory, http://www.enisa.europa.eu/act/cert/background/inv/certs-bycountry/slovenia, 23.01.2013

93. 9/11 Public Discourse Project, final report on 9/11 Commission recommendation, 2005, http://www.9-11pdp.org, 23.01.2013

94. Department of Homeland Security, Transportation Security Administration, http://www.tsa.gov, 23.01.2013

95. Federal Communications Commission, http://transition.fcc.gov/pshs/techtopics/techtopics19.html, 23.01.2013

96. Министарство унутрашњих послова Републике Србије: http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/uprava-za-analitiku.h, 23.01.2013

97. ЈКП водовод и канализација Суботице, http://www.vodovodsu.rs/2-Informacije/131-OSNOVANO-POSLOVNO-UDRUZENJE-VODOVODA-SRBIJE, 23.01.2013

98. Дирекција за воде (Србијаводе), http://www.srbijavode.rs/portret-delatnost.htm, 23.01.2013

99. Презентација сектора за аналитику МУП-а Србије, http://prezentacije.mup.gov.rs/svs/HTML/organizacija.html, 23.01.2013
100. Economy, http://www.economy.rs/finansije/9790/Poslovanje-finansijskih-institucija-u-Republici-Srbiji-2012--godine.html, 23.01.2013
101. Републички фонд Србије за здравствено осигурање, http://www.rfzo.rs/,23.01.2013
102. Trade statistics for international business development, http://www.trademap.org, 23.01.2013
103. The World Economic Forum on the Middle East and North Africa, http://www.weforum.org, 23.01.2013

Коришћени закони Републике Србије:

1. Закон о ванредним ситуацијама Републике Србије (Сл. гласник РС“, бр. 111/09. Измене и допуне закона у Сл. гласнику РС бр 92/2011 и Сл. гласнику РС 93/2012).
2. Закон о водама ("Службени гласник РС", бр. 30/10, 7.5.2010. године).
3. Закон о безбедности хране.
4. Закон о електронским комуникацијама (2012. године).
5. Закон о електронском документу.
6. Закон о електронској трговини ("Службени гласник Републике Србије" бр. 41/2009).
7. Закон о електронском потпису.
8. Закон о јавним предузећима и обављању делатности од општег интереса, "Службени гласник РС" 25/2000, 25/2002, 107/2005, 108/2005.
9. Закон о заштити података личности ("Службени гласник РС', бр. 97/08 и 104/09).
10. Закон о потврђивању Конвенције о високотехнолошком криминалу.
11. Стратегији националне безбедности Србије.
12. Национална стратегија заштите и спасвања ("Службени гласник РС", бр.86/2011 од 18.11.2011. године.).
13. Стратегија развоја информационог друштва у Републици Србији до 2020.
14. Стратегија развоја електронских комуникација ("Службени гласник РС" 68/10, 02.09.2010. године).
15. Стратегија развоја електронске управе у Републици Србији за период од 2009. до 2013. године.
16. Стратегије развоја енергерике Републике Србије до 2015. године.
17. Стратегија развоја друмског, железничког, водног, ваздушног и интемодалног транспорта у Републици Србији 2008 – 2015. године.
18. Правилник о издавању временског жига ("Службени гласник Републике Србије" бр. 112/2009).

БИОГРАФИЈА АУТОРА

Марко Ракић рођен је 1984. године у Београду где 2003. године завршава XI београдску гимназију и уписује основне студије на Факултету за менаџмент „БК“. Након успешно окончаних основних студија, 2007. године уписује мастер студије на Факултету безбедности Универзитета у Београду. Звање дипломираног менаџера безбедности-мастер стиче 2009. године. Исте године на поменутом факултету уписује докторске студије и након положених испита предвиђених наставним програмом отпочиње писање докторске тезе на тему „Кризни менаџмент у функцији заштите критичних инфраструктура у земљама у транзицији“.

Током студирања бавио се изучавањем кризног менаџмента, истраживањем безбедносних ризика и претњи, као и проучавањем међузависности ових феномена. Аутор и коаутор је више научно-истраживачких радова.

Од 2011. године запослен је у Министарству спољних послова Републике Србије као службеник дипломатско-конзуларне струке. Од јула 2013. године налази се на дужности дипломатског аташеа у Амбасади Републике Србије у Риму.

Говори енглески и италијански језик.

ИЗЈАВЕ

Прилог 1.

Изјава о ауторству

Потписани-а Марко Ракић

број уписа 1/09

Изјављујем

да је докторска дисертација под насловом

Кризни менаџмент у функцији заштите критичних инфраструктура у земљама у транзицији

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, 17.04.2015.

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Марко Ракић

Број уписа 1/09

Студијски програм Докторске студије

Наслов рада Кризни менаџмент у функцији заштите критичних инфраструктура у земљама у транзицији

Ментор Проф. др Жељимир Кешетовић

Потписани Марко Ракић

изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

У Београду, 17.04.2015.

Потпис докторанда

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Кризни менаџмент у функцији заштите критичних инфраструктура у земљама у транзицији

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

(1) Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, 17.04.2015.