СПЕЦИФИЧНОСТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ
У РЕПУБЛИЦИ СРБИЈИ

Едиција *Монографије*
Књига 42

МАРИЈА Д. МИЋОВИЋ

СПЕЦИФИЧНОСТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

КРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКИ УНИВЕРЗИТЕТ
Београд, 2020

СПЕЦИФИЧНОСТИ КРИТИЧНЕ
ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ
Едиција *Монографије*
Књига 42

Издавач
ККРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКИ УНИВЕРЗИТЕТ
Београд, Цара Душана 196 (Земун)

За издавача
Проф. др ДАНЕ СУБОШИЋ
ректор Универзитета

Аутор
Др МАРИЈА Д. МИЋОВИЋ

Рецензенти
Проф. др АЛЕКСАНДРА ЉУШТИНА
Проф. др ЈАСМИНА ГАЧИЋ
Доц. др ВЛАДИМИР ЦВЕТКОВИЋ

Уредник
Проф. др БИЉАНА СИМЕУНОВИЋ ПАТИЋ

Лектор
АНА МИЈАЈЛОВИЋ

Компјутерска припрема слога
ЈОВАН ПАВЛОВИЋ

Дизајн корица
мр НЕБОЈША КУЈУНЏИЋ

Тираж
100 примерака (CD-ROM)

Штампа
Криминалистичко-полицијски универзитет, Београд

Монографија је резултат рада на пројекту „Криминалитет у Србији
и инструменти државне реакције” , који је финансирала и реализовала
Криминалистичко-полицијска академија у Београду у периоду 2015–2018. године.

ISBN 978-86-7020-441-6

САДРЖАЈ

ПРЕДГОВОР

Имајући у виду значај области заштите критичне инфраструктуре у оквирима скоро свих савремених система заштите и спасавања, као и њену уређеност у нормативном, функционалном и институционалном погледу (или да је поступак уређења поменуте области у току), онда је покретање ове теме и њено истраживање сасвим оправдано.

Опасности које могу имати карактер ванредних ситуација прете свим сегментима друштва, државним органима и њиховим институцијама, службама јавних делатности (здравству, социјалној заштиа, просвети, култури и др.). Такав степен угрожености захтева ангажовање свих чинилаца државе, цивилних друштава, привредних субјеката и грађана, с циљем спровођења мера за смањење ризика односно свођења ризика на најмању могућу меру, које се огледају у спремности за адекватан одговор и отклањање изазваних последица.

Веома важан сегмент управљања у измењеним околностима представља област функционисања критичне инфраструктуре у ситуацијама када критична инфраструктура и њени поједини елементи истовремено бивају изложени деструктивним силама одређених опасности.

Анализирајући тренутно стање у Републици Србији, по овом питању, можемо констатовати да наведена област представља новину у реторичком смислу па је, самим тим, и мали број теоријских радова из ове области. Међутим, не може се рећи да се у Републици Србији до сада није чинило ништа на плану заштите критичне инфраструктуре те да се, у том смислу, налазимо на самом почетку јер се зна да су у свим системима које данас називамо критичном инфраструктуром организовани послови одбране, безбедности и заштите у чијем делокругу се налазе и питања процене и смањења ризика и функционисања инфраструктурних система у ванредним ситуацијама.Дакле, реч је о новој реторици, а послови одбране, безбедности и заштите су у поменутим системима одавно успостављени, функционишу у складу са постојећим позитивноправним прописима.

Није могуће одговорити на сва питања која су у вези са темом монографије, али надам се да полазна мишљења, као и домаћа и страна искуства и решења, могу пружити смернице за даља истраживања ове проблематике.

УВОД

Сталне и брзе промене у међународним односима, пораст безбедносних изазова, ризика и претњи, као и недостатак безбедности условљавају комплексност глобалне безбедносне слике, док критична инфраструктура поприма нове димензије и све већи значај на националном и међународном нивоу. Брзи развој и унапређење информационих технологија мењају безбедносно окружење. Како је критична инфраструктура постала важан сегмент националне безбедности тако је заштита критичне инфраструктуре почела да се развија и данас она представља један од главних приоритета сваке државе. Традиционални приступ безбедности посматра војне претње као највеће опасности по друштва и државе, док савремени приступ безбедносне изазове и ризике проналази у информатичкој сфери.

Основна питања упућена друштвеној заједници која организује систем критичне инфраструктуре јесу од кога и од чега треба штитити и на који начин организовати систем критичне инфраструктуре. Одговор на ова питања треба да пружи конкретна решења окренута ка могућим изворима угрожавања. То је истовремено и пут ка успостављању и организовању система безбедности који почиње објашњавањем, проценом, класификовањем облика и извора угрожавања вредности друштвене заједнице. (Мићовић, 2014: 171)

Функционисање модерног друштва, како у редовној тако и у ванредној ситуацији, није могуће замислити без ефикасне заштите значајних инфраструктурних објеката те се, као један од примарних и најзначајнијих безбедносних изазова новог доба, намеће проблем заштите критичних инфраструктура. Инфраструктуре попут саобраћајних мрежа, вода, енергија, хемијске индустрије, нуклеарне индустрије и информационих и комуникационих технологија пружају основне услове за функционисање појединаца па и друштва у целини.

Тема критичне инфраструктуре постаје незаобилазна, посебно током последњих неколико година. Са елементима критичне инфраструктуре сусрећемо се у свим сферама свакодневних активности. Не препозна ли се важност тог задатка, као приоритет на највишем нивоу одлучивања, бојазан од недовољног улагања у критичну инфраструктуру постаће оправдана, а економија изложенија великом ризику. Предуслови за квалитативни напредак и повезаност свих сегмената сигурности критичне инфраструктуре почива у специфичним знањима у која треба улагати знатна средства да би се превентивни механизми пре повезали у стратешки оквир за критичну инфраструктуру.

Критична инфраструктура односи се на имовину, системе, услуге или њихов део, чијим би се прекидом рада или уништењем, угрозиле кључне друштвене функције: здравље, мир, безбедност, економско и социјално благостање или нормално функционисање државе.

Критична инфраструктура је појам која има више дефиниција зависно од окружења у којем се налази, али се може закључити да савремено разумевање критичне инфраструктуре подразумева све објекте и системе чија неактивност или ограничена употреба проузрокује друштвено-кризне ситуације или, чак, представља претњу по мир и безбедност. Оквир

критичне инфраструктуре у многим земљама и организацијама је различито дефинисан у зависности од географског положаја, популације, верске димензије и др.

Данас су кључне инфраструктуре постале саставни део сајбер простора и играју виталну улогу у подршци многим нашим свакодневним активностима (укључујући путовања, коришћење воде и енергије, финансијске трансакције, телекомуникације итд). Поузданост, високе перформансе, континуирани рад, сигурност, одржавање и заштита ових критичних инфраструктура представљају национални приоритет за многе земље широм света. Подручје заштите критичних инфраструктура једно је од кључних подручја интересовања и Европске уније која је развила програме и механизме као помоћ у решавању ових приоритета.

Када говоримо о заштити критичних инфраструктура, првенствено мислимо на активности од пресудног значења, које се тичу заштите инфраструктура. Ту спадају људи, физичка имовина и информационо-комуникациони системи који су неопходни за националну безбедност, економску стабилност и јавни и правни поредак и безбедност. Методе и средства заштите критичних инфраструктура спречавају или ублажавају: нападе људи на критичне инфраструктуре (терористи, криминалци, хакери итд.), настанак природних катастрофа (земљотреси, олујни ветрови, поплаве итд.), пожара и експлозија у нуклеарним или хемијским комплексима. (Radvanovsky, McDougall, 2010: 4)

Изградња адекватног система заштите критичне инфраструктуре данас представља веома сложен задатак за скоро све земље. Имајући у виду да је основна функција и намена критичне инфраструктуре да обезбеди нормално и ефикасно функционисање свих сегмената друштва, државе и њених органа и грађана, као и сложеност безбедносног окружења и претњи, онда је оправдано констатовати да је пред државом и њеним органима и самим операторима изузетно сложен и изазован задатак у погледу обезбеђивања неопходних услова за безбедно функционисање критичне инфраструктуре у свим условима, како у миру тако и у ванредним ситуацијама.

Међутим, у претходном периоду, у многим земљама па и у Републици Србији, веома често се, због ограничености финансијских, људских и организационих ресурса, питање заштите критичних инфраструктура у оквиру дефинисаних приоритета стратешког менаџмента појединих организација или компанија налазило при самом дну лествице примарних циљева и задатака. Присуство различитих ставова и схватања значаја критичне инфраструктуре, парцијалних интереса појединих компанија и државних институција (министарстава) су само неке од тензија које прате неадекватно управљање и функционисање система заштите критичне инфраструктуре. Овакво стање може да доведе до значајних кашњења у развоју система заштите критичне инфраструктуре у нашој земљи.

Систем заштите критичне инфраструктуре у Републици Србији у будућности може бити ефикасан само под претпоставком да све релевантне и заинтересоване стране (мисли се на државе на првом месту, компаније и друге учеснике) разумеју позитивне ефекте успостављања система заштите критичне инфраструктуре и да уложе неопходне напоре и ресурсе у њену изградњу на новим – савременим основама.

Држава представља ослонац и полазну тачку у изградњи и успостављању ефикасног система критичне инфраструктуре те је интерес државе да тај систем, без обзира на власничку структуру компанија, непрекидно функционише, чиме се остварује и функционисање заједнице у свим условима, било да је реч о редовним било о ванредним ситуацијама.

ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У АНТИЧКОМ ПЕРИОДУ

1

Напредак и технолошки развој савремених друштава је у великој мери заснован на достигнућима из римског периода. Чињеница је да западни свет отворено признаје древни Рим за колевку нашег знања и примену модерног календара, конституисање владе и јавне администрације. Такође, имали смо користи од римских инжењерских достигнућа попут проналаска цемента и изградње путне мреже која је повезивала древну Европу.

Према историчарима и археолозима постоје три истакнута римска инфраструктурна 'објекта' – путна мрежа, пољопривреда са продавницама прехрамбене робе и аквадукти.

1.1. ДРЕВНИ РИМСКИ АКВАДУКТИ

Антички Рим је оставио дубок траг у сфери науке и инжењерских достигнућа. То не би требало да буде никакво изненађење јер су и данас видљиве различите грађевинске структуре из тог периода, али се изненађујућим може сматрати податак да су неке од ових древних структуре и данас у употреби.

Први римски аквадукт је саграђен 313. године п. н. е. како би омогућио допремање свеже воде са околних брда. Његова изградња окончана је након конструкције главног путног правца, познатог као „Via Appia". Сматра се да је у то време изграђено укупно једанаест аквадукта ради водоснабдевања Рима, што је омогућило да овај град насели више од милион становника. Један од одговорних за њихово одржавање, управник Секстус Јулиус Фронтинус, забележио је да је овај систем испоручивао десетине милиона литара воде свакога дана. (Dembskey, 2009: 26)

Такође, битно је напоменути да су Римљани схватили значај постојања и функционисања аквадукта због њихове суштинске услуге водоснабдевања и чињенице да није било могућности њихове једноставне замене.

Веровало се да је за изградњу једног од највећих аквадукта „Еифел", дугог око 96 км, било неопходно ангажовање око 2500 радника у трајању од шеснаест месеци. Рим је, у циљу заштите те критичне инфраструктуре, дефинисао неколико закона. У Лиону, у Француској, пронађена је плоча са натписом: „по заповести цара Трајанус Хадријанус Аугустуса никоме није дозвољено да обрађује земљу или напаса стоку у близини аквадукта". Римљани су током изградње ових виталних и специфичних објеката водили рачуна о заштити инфраструктуре.

На слици 1. приказана је подземна конструкција аквадукта.

Слика 1. *Римски аквадукт изграђен под земљом*

Сва досадашња археолошка истраживања потврдила су значај израде ових подземних структура као метод заштите свеже воде од спољних претњи (контаминације или застоја у водоснабдевању). Током периода ране експанзије стари Рим имао је много непријатеља па су постојала три главна разлога за подземну изградњу аквадукта: прикривање и заштита од непријатеља, обезбеђивање додатног нивоа заштите од ерозије и пропадања и да мање ремећење живог света на површини земље. Примарни недостатак система подземног аквадукта био је везан за одржавање и проверу система. Поред тога, постојала је још једна мана у очима поносних Римљана – оваква архитектонска решења и грађевински подухвати били су ван видокруга становништва и спречавали Рим да отворено прикаже своју величину и супериорност. (Dembskey, 2009: 26)

1.2. РАНО СХВАТАЊЕ БЕЗБЕДНОСНИХ РИЗИКА У РИМУ

Напредак неких тадашњих технологија довео је до одређених промена у схватањима како везаним за конструисање будућих аквадукта. Отпочело се са изградњом надземних објеката са предивним упечатљивим луковима (слика 2).

Слика 2. *Новија конструкциона решења Римског аквадукта*

С обзиром на то да је нови дизајн аквадукта промењен и да је укључивао више надземних делова, то је условило већу рањивост инфраструктуре са безбедносног становишта.

Уколико се покуша анализирати тај историјски период у погледу постојећих ризика, тј. претњи, може се констатовати да је племенско функционисање подразумевало постојање константних ризика. Ова безбедоносна ситуација се у великој мери променила у наредних неколико стотина година, у смислу доминације Рима у целокупној Италији и тенденцији ка даљем ширењу. Након уништавања Картагине 146. године п. н. е., Рим је био у стању да елиминише све безбедносне претње. Обезбеђење сигурности у земљи омогућило је многобројне иновације и напредак цивилизације па је Рим постао одраз моћи и развоја. Велики јавни радови из тог периода су били праћени многобројним архитектонским „чудима", као што су специфичне куполе. (Assante, 2009)Основне инфраструктурне промене огледају се у чињеници да се „скривено" трансформише у „видљиво". У ратним разарањима која су уследила уништени су бројни аквадукти, тако да су Римљани прекасно схватили своју грешку.

Уколико се анализирају сва историјска дешавања, могу се извести одређени закључци везани за римске аквадукте. Један од њих је да се постојећа инфраструктура једноставно може претворити у критичну. Друго становиште је везано за римско поимање ризика и његово друштвено схватање. Прича о аквадуктима је еволуирала у периоду од скоро 600 година и указује на утицај ризика одлучивања. Први и најдужи аквадукт био је саграђен у време када су безбедносни ризици били лакше уочљиви. Аквадукти који су изграђивани у наредном периоду одликовали су се одсуством страха Римљана од инвазије непријатеља. Ова смањена осетљивост на пољу безбедносних ризика резултирала је модификацијом и употребом рањивијих грађевинских решења. То значи да би сви инжењери требало да из наведеног примера извуку поуке и разумеју да коначна одлука мора предвидети и чињенице битне за систем безбедности.

Све ово нам може помоћи у разумевању ризика повезаних са данашњом инфраструктуром. Многи стручњаци признају да је један од главних проблема дефинисање модерне инфраструктуре. Ради бољег разумевања, било би најкорисније изабрати један конкретан пример модерне инфраструктуре – модерне електроенергетске мреже (слика 3) и повући паралеле у вези са заштитом те инфраструктуре.

Слика 3. *Модерна електрична инфраструктура*

Као у случају воде за Римљане, лако је тврдити да обиље јефтине електричне енергије омогућава раст и просперитет становништва. Стога су бројна поређења по сличностима и супротностима у инфраструктурном и безбедносном смислу. (Assante, 2009)

Уколико желимо да сагледамо заједничке садржаоце за ове две цивилизације, можемо отпочети са поређењем инфраструктуре. Аквадукти и савремени енергетски систем су слични по потреби да се производи (вода и струја) „крећу" од извора ка крајњим потрошачима. Систем аквадукта чине извори (реке, потоци и језера), системи преноса (резервоари, тунели, покривени ровови, мостови), дистрибутивни системи (сливови, куле и цеви) и потрошачи.Систем за снабдевање електричном енергијом, такође, садржи изворе (који чине производни објекти - хидроцентрале, нуклеарне електране, ветропаркови итд.), системе преноса (подстанице, контролни центри), дистрибутивне системе (трафостанице, торњеви, контролни центри и водови) и потрошаче или оптерећења. Друга релевантна сличност са старом Римом односи се на промене претњи са којима се суочава окружење римских аквадукта и америчких електроенергетских система. Након стотине година мирног живота, древни Рим је опустошен након инвазије немачких племена.

За оба ова система заједнички је дуго очекивани животни циклус. Неки аквадукти су трајали и по хиљаду година, док су други трајали свега неколико година због тога што су их непријатељи прерано уништили. Основни концепт аквадукта је до данас остао непромењен и то је најпожељнији начин за пренос велике количине воде на велике удаљености променом надморске висине. Многи електроенергетски системи широм света се и даље ослањају на компоненте које су биле део првобитно инсталираних система.

Постоје две основне и важне разлике између воде и струје. Први је да вода постоји у употребљивом облику, док се електрична енергије мора произвести, тј. енергија се претвара из једног облика у други. Другу важну разлику представља највеће ограничење са којим се суочава инфраструктура. Вода се може складиштити, а електрична енергија се мора користити одмах након производње.

Иако тероризам и сајбер претње представљају нашу реалност, морамо бити спремни за алтернативна решења. Промене у приступу безбедности веома су драматичне па егзистирају физичке претње држави и сајбер претње информационим системима. То изискује стварање могућности да се ублаже недостаци постојећих структура и система, а затим надокнаде пропуста својствене њиховом дизајну, што подразумева наш проактивнији приступ.

Разлике између античког Рима и других земаља појачавају потребу да се преиспита наш приступ заштите критичне инфраструктуре. Неки од карактеристичних примера су следећи:

– године 1996. откривено је да је Ирска Републиканска Армија покушала оштетити електричну мрежу у Лондону,

– године 2003. је екстремиста из Пакистана покушао диверзију на електричној мрежи за напајање Сиднеја,

– године 2007. исламски екстремисти су планирали напад на америчку војну базу Форт Дик и на компоненте електроенергетског система, чиме би повећали ефикасност свог напада,

– у наредном периоду евидентирано је неколико напада на локалне енергетске системе у Пакистану, Колумбији и Перуу.

Препознајући сличности и разлике између римских аквадукта и модерне електричне мреже омогућено нам је да научимо како да заштитимо инфраструктуру. Морамо идентификовати све што може да допринесе заштити будућих инфраструктурних компоненти. (Assante, 2009)

ДЕФИНИСАЊЕ И КЛАСИФИКАЦИЈА КРИТИЧНЕ ИНФРАСТРУКТУРЕ 2

2.1. ПОЈАМ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Велики број стручњака у области критичне инфраструктуре дефинише ову област наглашавајући да је она веома важан сегмент националне безбедности и безбедности уопште. Људи су постали свесни да није могуће заштити све и у сваком тренутку, као и да морају да одлуче која је инфраструктура од кључног значаја за њих и зашто. Свесни су и важности критичне инфраструктуре, али се још увек нису усагласили по питању њене јединствене дефиниције што доводи до различитих приступа заштити критичне инфраструктуре која се налази на раскршћу између политике, бизниса, технологије и ризика. (Wahle, Beaty, 2004: 29)

Критична инфраструктура препозната је као један од приоритета у процесима интеграција, али процес идентифакције, почетна улагања, као и техничка помоћ недовољни су за оптимално осигурање критичне инфраструктуре. Зато је нужно осмислити програме и заштитити кључне ресурсе за управљање критичном инфраструктуром. У том смислу, критична инфраструктура је инфраструктура чија би онеспособљеност или уништење имала утицај на слабљење националне сигурности те економске и друштвене добробити нације и јавног здравља, а критична информатичка инфраструктура јесте информатичка инфраструктура која подупире вишеструке елементе критичне инфраструктуре.

Како су информациони системи у великој мери међусобно повезани или повезани с јавним системима, критична информатичка инфраструктура у данашње време постаје све изложенија, не само отказима и хаваријама, већ и разним врстама намерних напада. Основни проблем, из којег произилази нужност препознавања критичне инфраструктуре, представља чињеница да напад на одређену критичну инфраструктуру сам по себи увећава степен изазване штете, јер напад релативно ниских размера може имати огроман утицај и проузроковати штету не само на једном, већ на читавом низу међусобно повезаних инфраструктурних објеката.

Критична инфраструктура постаје суштински проблем националне безбедности, а њена заштита приоритет у свим државама света, посебно после терористичог напада на САД, 11. септембра 2001. године. (The Department of Homeland Security, June 2002, White House, 15).

Године 2002, у Брашову, у Румунији, према закључку *Одбора за цивилну заштиту Евроатлантског већа* (енг. Euro-Atlantic Partnership Council, Civil Protection Committee - EAPC, CPC), који је касније усвојио и *Виши одбор за цивилно хитно планирање* (енг. Senior Civil Emergency Planning Committee – SCEPC), појам „критичне инфраструктуре" обухвата одговарајуће националне капацитете, службе и информацијске системе од виталног значаја, чија би немогућност деловања или оштећење могла имати директан утицај на националну безбедност, националну економију, јавно здравље, сигурност становништва и ефикасно

деловање власти. Друга дефиниција са истог заседања гласи: „Критична инфраструктура обухвата посебно (али не искључиво): храну, воду, пољопривреду, здравствене службе и службе хитне помоћи, енергију, саобраћај, информације и телекомуникације, банкарство и финансије, хемијска постројења, одбрамбену индустрију, поште и дистрибуцију робе, као и националне споменике и друге културне вредности" (Јаковљевић, 2010)..

Питање критичне инфраструктуре постало је нарочито значајно у последњих десет до двадесет година. Модерни стил живота и зависност људи и привреде од струје, горива, интернета (комуникације уопште) сваким даном је све већа и већа. Безбедност критичне инфраструктуре је кључно питање савремене националне безбедности (Herga, 2010: 311), јер критична инфраструктура представља основу за опстанак заједнице (Чемерин, 2011: 442), док су асиметричне претње постале уобичајене. Терористички напад који се догодио 11. септембра 2001. године у САД условио је ново значење и нову димензију концепта заштите критичне инфраструктуре. Терористички напади у Мадриду, Лондону, Москви, Мумбају и Исламабаду су само потврдили потребу за новим приступом у заштити критичне инфраструктуре. Поред тога, ураган Катрина у САД, цунами у југоисточној Азији и Јапану су, такође, показали да природне катастрофе могу имати разорне последице на инфраструктуру (Jopling, 2007). Чак и политичке одлуке могу да имају сличне ефекте (Smedts, 2010: 11). Због тога је заштита критичне инфраструктуре постала један од кључних приоритета Европске уније у области безбедности. Такође, у *Националној стратегији за унутрашњу безбедност* САД, из 2007. године, управљање кризама у природним катастрофама налази се на врху листе, испред терористичких напада (Зутер, 2011: 37). Иста је ситуација и широм света.

Појам ,'инфраструктура' потиче од латинских речи 'infra' (значење: под, испод, ниже) и 'struere' (значење: слагати, склапати) и представља темељ, подлогу; основу за привредни и друштвени развој коју чине: саобраћајна мрежа (путеви, железничке пруге, канали и сл.), водоводне инсталације, извори електричне и друге енергије, објекти намењени јавним потребама (осветљење, паркови, тргови, домови здравља, болнице, диспанзери, школе итд.).

Критичне инфраструктуре су физички или виртуелни системи и средства кључни за нормално функционисање државе. Њихово онеспособљавање или уништење могло би да ослаби безбедност, привреду, јавно здравље и сигурност. У критичне инфраструктуре најчешће спадају: телекомуникације, системи електричне енергије, складиштење и транспорт нафте и гаса, банкарство и финансије, транспорт, системи водоснабдевања, хитне службе (медицинске, полицијске, ватрогасне, службе за спасавање), информациони и комуникациони системи. Критичне инфраструктуре постале су битан елемент националне безбедности 1990-их година. Тада је уведена заштита критичних инфраструктура која данас представља један од приоритета сваке државе, пре свега зато што оне могу бити мета терористичких напада. (Moteff, Copeland, Fischer, 2003)

У зависности од критеријума, а у циљу дефинисања критичне инфраструктуре, постоји потреба за детаљнијим сагледавањем различитих типова критичне инфраструктуре. Критична инфраструктура може бити од интереса за: државе, регионе или свет, што значи да можемо говорити о националној, регионалној (европској, афричкој, евроазијској) и светској критичној инфраструктури. С друге стране, у неким државама је могуће говорити о критичној инфраструктури на локалном, регионалном (), државном (националном) и међународном нивоу.

С обзиром на време потребно за спровођење мера заштите, разликујемо: сталну, привремену или потенцијалну критичну инфраструктуру. Стална критична инфраструктура је, за неке државе, кључна инфраструктура, прописана законом, о којој се непрестано мора водити рачуна. У категорију привремене критичне инфраструктуре можемо уврстити неке политичке или спортске догађаје који су кратког трајања (ограничени одређеним временским интервалом), али од велике националне и интернационалне важности Потенцијална критична инфраструктура није непрестано у фокусу, али у неким ситуацијама (које се не могу испланирати унапред) може бити веома важна.

Неки аутори сматрају да критична инфраструктура,према критеријуму власништва унутар једне државе, може бити у поседу: државе, општине, приватног лица, лица за управљање имовином у државном власништву, имовином у власништву правних лица чији су оснивачи локалне самоуправе (Херга, 2010: 314). То значи да критична инфраструктура може бити у јавном, приватном или јавно-приватном поседу. Јавно-приватно партнерство је суштински значајно јер се процењује да је преко 85 % критичне инфраструктуре у САД, а изнад 90% у Немачкој, власништву приватног сектора.

Дакле, разноликост типова критичне инфраструктуре условљена је различитим гледиштима оних људи који одређују шта је критична инфраструктура, као и од структуре и нивоа власти. Али област заштите критичне инфраструктуре захтева свеобухватан приступ. То значи да сви нивои државне власти морају препознати своју критичну инфраструктуру и предузетиу мере у циљу њене заштите. Ако само један од нивоа власти није успео да препозна и заштити своју критичну инфраструктуру, могло би доћи до катастрофалних последица, јер су објекти критичне инфраструктуре међусобно повезани и зависе једни од других. (Чемерин, Трут, 2010: 33)

Све врсте критичне инфраструктуре морају се узети у обзир приликом планирања одговарајућих мера заштите. Заштита критичне инфраструктуре дефинисана је као стратегија, политика и спремност да се заштити, спречи, а кад је то потребно, и одговори на нападе на објекте критичне инфраструктуре. Сваки од нивоа власти у држави или у неким организацијама, па чак и на светском нивоу, треба да учествује у активностима везаним за заштиту критичне инфраструктуре. На тај начин ће ресурси бити најбоље искоришћени. Мора се успоставити нека врста система заштите, у зависности од нивоа власти и државне структуре. (Lewis, 2006: 8)

Не постоје опште мере заштите критичне инфраструктуре, примењиве у свим државама, али она, све више, подразумева међународну сарадњу. У заштиту критичне инфраструктуре укључене су јавне власти – на државном и локалном нивоу, као и јавне агенције, корисници критичне инфраструктуре који често припадају приватном сектору и становништво у целини. Различите институције су, у зависности од државе, одговорне за заштиту критичне инфраструктуре. Тако се у САДзаштитом критичне инфраструктуре бави Одељење за унутрашњу безбедност; у Великој Британији постоји слична агенција, Министарство унутрашњих послова; у Немачкој - Центар за заштиту критичне инфраструктуре који је у оквиру Савезне службе за цивилну заштиту и одговор на катастрофе (при Министарству унутрашњих послова). Процес глобализације довео је до све веће међузависности и повезаности тржишта и мрежа у одређеном броју битних сектора као што су енергија, информације и комуникације, храна, превоз, што повећава осетљивост инфраструктуре у сваком од наведених подручја. Већина критичних инфраструктура данас је део приватног сектора, који је, стога, носилац одговорности за заштиту инфраструктуре. (Jopling, 2007)

Критична инфраструктура обухвата поједине институције јавног и приватног сектора, канале дистрибуције те „мреже" особа и информација које гарантују несметан и континуиран проток људи, роба, сервиса, услуга, што је кључно за стабилност економског и безбедносног система земље и има директан утицај на националну безбедност и економију, јавно здравље, сигурност становништва и ефикасност деловања власти.

Европска комисија дефинише критичну инфраструктуру као средство, систем или његов део који се налази у државама чланицама, неопходан за одржавање виталних друштвених функција, здравља, безбедности, сигурности, економског или социјалног благостања, као и нарушавање или уништење које би значајно утицало на државе чланице због немогућности да одржавају поменуте функције.

ОЕБС је дао две дефиниције термина 'критичност' и 'инфраструктура', као покушај помирења различитих дефиниција које постоје у државама чланицама. Термин 'критична' односи се на инфраструктуру која пружа главну подршку за економско и социјално благостање,

јавну безбедност и функционисање кључних владиних одговорности, тако да поремећај или уништавање инфраструктуре доводи до катастрофалних последица и велике штете.[1]

Националне дефиниције 'инфраструктуре' углавном подразумевају физичку инфраструктуру, а често и нематеријална улагања и/или производњу путем комуникационих мрежа. Ове дефиниције су веома широке, свакако шире од појма инфраструктуре који се уобичајено користи у другим областима политике (нпр. „суштински објекат") и укључују не само материјална средстава, него и нематеријалне вредности (нпр. софтвер, услуге итд.).

Критичне инфраструктуре су ресурси, системи и мреже, физички или виртуелни, чије уништавање или онеспособљавање може ослабити националну безбедност, економску стабилност и утицати на друге аспекте нормалног функционисања друштва. (Rinaldi, 2004) У групу критичне инфраструктуре убрајају се телекомуникације, електропривреда, складиштење и пренос плина и нафте, банкарство и финансије, транспорт, водоснабдевање, хитна служба (укључујући медицинске, полицијске, ватрогасне и спасилачке службе) и друге институције.

Постоји више дефиниција критичне инфраструктуре, али се, у основи, све односе на средства и имовину која је кључна за неометано функционисање економије и друштва. Као пример наводе се следеће дефиниције:

• САД:

„Критична инфраструктура и основни ресурси *(*енг. Critical Infrastructure and Key Resources; CIKR*)* је појам који се односи на широк опсег различитих средстава и имовине који су неопходни за свакодневно функционисање друштвених, економских, политичких и културних система у САД. Било какав прекид у елементима критичне инфраструктуре представља озбиљну претњу за правилно функционисање ових система и може довести до оштећења имовине, људских жртава и значајних економских губитака".[2]

• Европска Унија:

(а) „Критична инфраструктура представља имовину, систем или његов део који се налази на територији земље чланице, неопходан за одржавање кључних друштвених функција, здравства, безбедности, сигурности, економског или социјалног благостања, а чије би ометање или уништење значајно утицало на земљу чланицу".[3]

(б) „Европска критична инфраструктура подразумева критичну инфраструктуру лоцирану на територији земље чланице чије би ометање или уништење значајно утицало на бар две земље чланице. Значај поремећаја у функционисању елемената критичне инфраструктуре треба да се процени на основу критеријума међузависности. То подразумева ефекте настале као резултат међусекторске зависности од других типова инфраструктуре".[4]

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, функционисање здравства, безбедност чланица и 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.[5]

Критична инфраструктура састоји се од физичких и информационих технолошких објеката, мрежа, служби и материјалних добара, који, уколико буду урушени или уништени, могу озбиљно утицати на здравље, безбедност, сигурност и економско благостање или ефи-

1 На: http://www.oecd.org/dataoecd/2/41/40700392.pdf
2 Critical Infrastructure and Key Resources, Cansas City Regional Tew, Interagency Analisys Center.
3 Critical Infrastructure Protection in the Fight against Terrorism, Brussels, COM(2004)702, 2004.
4 Исто.
5 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, L 345/75-L 345/82, 2008.

касно функционисање власти. Ову дефиницију најчешће користе институције УН у образложењу садржине појма 'критична инфраструктура'.

Критична инфраструктура може се схватити као објекат који трпи последице одређене ванредне ситуације,и представља предмет заштите, али и као средство које омогућава смањивање опасности или отклањање последица у ситуацијама када је опасност наступила.

НАТО, такође, дефинише појам 'заштита критичне инфраструктуре' наводећи да он обухвата програме, делатности и деловање влада, власника, оператера или корисника, предузето са циљем заштите властите критичне инфраструктуре. Осим НАТО, програме заштите критичне инфраструктуре покренули су и Европска унија, Уједињене нације, Клуб осам најразвијенијих земаља, низ регионалних организација и др. (Јаковљевић, 2010)

Занимљива је дефиниција Гарба који сматра да „критична инфраструктура представља разгранату мрежу независних система, углавном у приватном власништву, капацитета и процеса који синергијским деловањем омогућавају непрекидну производњу и дистрибуцију основних добара и услуга чије уништење или квар могу да проузрокују озбиљне последице по јавно здравство, безбедност, привредно стање, социјално благостање грађана и функционисање јавног сектора". (Garb, 2009)Гарбова дефиниција се (изузевши концентрисаност на приватну имовину која није потпуно разумљива, тиме и коректна) приближава дефиницији критичне инфраструктуре у НАТО-у и у САД, Канади, Финској, Великој Британији, као и ОЕБС, која као последицу оштећења или уништења критичне инфраструктуре наводи директан негативни утицај на јавно здравство.

Табела 1. *Дефиниције критичне инфраструктуре у различитим земљама*

Аустралија	Критична инфраструктура предстаља физичке објекте, ланце снадбевања, информациону и комуникациону технологију и мрежу која, ако је уништена, деградирана или онеспособљена дуже време, може да утиче на друштвени, економски и социјални живот у Аустралији. Проблем са критичном инфраструктуром може утицати на способност Аустралије да одбрани националну безбедност.
Канада	Критична инфраструктура подразумева систем физичких и информационих технологија, објеката, мрежа, услуга и добара који, ако су уништени или онеспособљени за рад, могу озбиљно утицати на здравље, безбедност и добробит Канађана и ефикасно функционисање владе у Канади.
Немачка	Критична инфраструктура обухвата организације и установе од великог значаја за заједницу, чији неуспех или оштећење могу изазвати трајан недостатак залиха, велике поремећаје у јавном реду и друге драматичне последице.
Холандија	Критична инфраструктура обухвата производе, услуге и пратеће процесе који, у случају прекида рада или неуспеха, могу да изазову велике социјалне немире. Прекид рада би довео до великог броја жртава и велике економске штете.
Енглеска	Националну критичну инфраструктуру чине средства, услуге и системи који подржавају економски, политички и друштвени живот уВеликој Британији чији је значај такав да њихов губитак може да: 1) узрокује високу смртност, 2) озбиљно утиче на националну економију, 3) изазове социјалне последице у заједници.
САД	Општа дефиниција критичне инфраструктуре гласи: системи и средства, било физички или виртуелни, који су од виталног значаја за САД, чијанеспособност или уништење могу утицати на безбедност, економску сигурност, јавно здравље или на две или три поменуте ствари истовремено.

2.2. КЛАСИФИКАЦИЈА КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Критична инфраструктура обухвата широк спектар виталних сектора, као што су саобраћај, транспорт, производња и дистрибуција енергије, информациони и комуникациони 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 проблема.

Развијене земље, а последњих година и оне мање развијене, настоје да идентификују и анализирају критичне секторе, подсекторе, 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 сложености инфраструктурних система говоре многи стручњаци из области заштите критичне инфраструктуре. (Lewis, 2006)

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.

Велики је број инфраструктурних сектора који истовремено обухватају већи број подсектора, грана индустрије, служби, производних области и имају специфичну вертикалну структуру. Поједина мишљења указују на опасност идентификовања свих инфраструктура као критичних услед нејасних граница између критичне и некритичне инфраструктуре. Заједно указују на све јачу међуповезаност критичних инфраструктура (међусекторска повезаност). Све у свему, велики број стручњака сагласан је да бројне ризике, претње и рањивости треба идентификовати пре него што се пређе на идентификовање критичних инфраструктура. (Moteff, Parfomak, 2004)

Анализирајући различите приступе дефинисања и класификовања критичне инфраструктуре, може се закључити да она обухвата (не искључиво):

– храну,
– воду,
– пољопривреду,
– здравствене службе и службе хитне помоћи,
– енергију (електрична, нуклеарна, гас и нафта, бране),
– саобраћај (ваздушни, друмски, железнички, луке, пловне путеве),
– информације и телекомуникације,
– банкарство и финансије,
– хемијска постројења,
– одбрамбену индустрију,
– поште и дистрибуцију робе и
– националне споменике и друге културне вредности.

Када се расправља о схватању и класификацији критичне инфраструктуре, веома често се користи Извршна наредба 13010 (Executive Order 13010 - Critical Infrastructure Protection: 37347—37350), коју је потписао председник САД, Клинтон, 1996. године, а која успоставља председничку комисију за заштиту критичне инфраструктуре, односећи се на оно што одређену инфраструктуру чини критичном: „Одређене националне инфраструктуре које су толико виталне да би ометање њиховог рада или уништење имало ефекат слабљења одбрамбене или економске сигурности САД". Према поменутој извршној наредби, ове инфраструктуре су обухватале:

– телекомуникације,
– системе електричне енергије,
– складиштење и транспорт нафте и гаса,
– банкарство и финансије,
– транспорт,
– системе за снабдевање водом,
– хитне службе (медицинске, полицијске, ватрогасне и спасилачке службе) и
– континуитет власти. (Executive Order 13010 - Critical Infrastructure Protection: 37347)

Уз употребу текста ове извршне наредбе, коначни извештај комисије упућен председнику САД дефинише критичну инфраструктуру на следећи начин:

> „Критична инфраструктура је инфраструктура која је толико витална да би њено онеспособљавање или уништење имало ефекат слабљења одбрамбене или економске сигурности" (President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure, 1997)

Такође, извештај комисије дефинисао је инфраструктуре сваког сектора споменутог у извршној наредби:

Банкарство и финансије: Ентитети као што су малопродаје и комерцијалне организације, инвестиционе институције, брокерске куће, трговачке куће и системи резерви, придружене оперативне организације, владине операције и активности подршке, укључене у сваки од аспеката монетарних трансакција, као и штедне улоге, инвестиције, безготовинске исплате, исплате зајмова и других финансијских инструмената.

Системи електричне енергије: Електране и мреже за пренос и дистрибуцију производе и снабдевају електричном енергијом крајње кориснике тако да они постижу и одржавају номиналну функционалност, укључујући транспорт и складиштење горива које је неопходно за ове системе.

Хитне службе: Медицинске, полицијске, ватрогасне и спасилачке службе, као и особље које је на располагању када у тренутку суочавања појединаца или заједнице с ванредном ситуацијом. Ове услуге се углавном пружају на локалном нивоу.

Производња, складиштење и транспорт нафте и гаса: Постројења за производњу и складиштење природног гаса, сирове и прерађене нафте и нафтних деривата, постројења за рафинисање и прераду ових горива, и нафтоводи, бродови, камиони и железнички системи за транспорт ових производа до крајњих корисника.

Информације и комуникације: Компјутерска и телекомуникациона опрема, софтвер, процеси и људи који подржавају: прикупљање, обраду, складиштење и пренос података и информација; процесе и људе који од података стварају информације, а од информација знање.

Транспорт: Системи за физичку дистрибуцију који значајно доприносе националној безбедности и економском благостању, системи националног ваздушног саобраћаја, ваздушне линије, ваздухоплови и аеродроми; путеви и ауто-путеви, копнена возила; луке, водени путеви и пловила; јавни саобраћај, железнички и аутобуски; цевоводи (за природни гас, нафту и друге опасне материје); теретна и путничка железница и сл.

Системи за снабдевање водом: Извори воде, резервоари и постројења за складиштење, водоводи и други транспортни системи, системи за филтрацију, чишћење и прераду воде, цевоводи, расхладни системи и други механизми испоруке који обезбеђују воду домаћинствима и индустријским потрошачима, укључујући системе за рад са отпадним водама и системе за заштиту од пожара.

Као одговор на извештај комисије, Клинтон је потписао 22. 5. 1998. године Председничку директиву бр. 63 (ПДД 63). (The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No. 63, White Paper, May 22, 1998)

Директива је дефинисала критичне инфраструктуре као „физичке и сајбер системе који су витални за минимално функционисање привреде и владе". Физичка безбедност обично значи заштиту физичких средстава (уз то и компјутерску опрему) од оштећења изазваног физичком силом као што су експлозије, ветар, ватра и сл.

Сајбер безбедност може, такође, да означава физичку заштиту сајбер средстава. Међутим, сајбер безбедност подразумева заштиту и физичких и сајбер средстава од оперативног пада или неовлашћеног компјутерског приступа (укључујући и удаљени приступ) оперативном софтверу или подацима.

Током 2004. године група научника израдила је упоредну анализу критичне инфраструктуре у шеснаест земаља света, што се може приказати овако:

– банкарство, финансије, телекомуникације, енергију, информационе и телекомуникационе системе у својим листама наводи 14 земаља,

– превоз, логистику, расподелу – 13 земаља,

– здравствене службе и водоснабдевање – 12 земаља,

– централну власт/владине службе – 11 земаља,

– хитне спасилачке службе – 10 земаља,

– снабдевање нафтиним дериватима – 9 земаља,

– информативне службе, медије (радио и ТВ), јавну администрацију – 8 земаља,

– остала подручја – јачање законодавства, правосуђе, јавни ред и националну безбедност, управљање отпадом, полицију, РХБ заштиту, војску и војне објекте, системе осигурања, социјалне службе, управљање залихама воде, нуклеарне електране – од шест до једне земље. (Јаковљевић, 2010: 66)

Анализом ових осам група приоритета у погледу критичне инфраструктуре лако је закључити да дефиниција критичне инфраструктуре и њен садржај не може бити идентичан у сваком делу света па је и логично да се они морају утврдити на националном нивоу. (Јаковљевић, 2010: 66) Др Миодраг Комарчевић наводи да се сви елементи инфраструктуре најчешћегрупишу према:

– *друштвено-економском значају*: технички и друштвени,

– *пореклу*: природни и технички,

– *функцији*: привредни и непривредни,

– *обиму*: насељски и регионални,

– *значају*: главни и допунски.

– *видовима*: индивидуални, заједнички и елементи мешовите потрошње,

– *рангу мреже*: примарни, секундарни и терцијални,

– *карактеру*: материјална (саобраћајнице, инсталације итд.), институционална (управа, школство, здравство итд.) и персонална инфраструктура (школована радна снага, образовни систем итд.),

– *положају у простору*: подземни и надземни,

– *функцији коју обављају* (елементи мрежа које омогућавају директну интеракцију људи, мрежа без директног контакта) и да ли омогућавају кретање људи, материјалних добара, енергије и информације.

Поред наведених подела, са формално-правног аспекта, битне су и следеће поделе инфраструктуре у односу на:

– власничку структуру – јавна и приватна,

– начин коришћења – индивидуална и колективна и

– статус објекта – у општој употреби и као основна средства.

Са инжењерског аспекта најбитније су поделе према намени и карактеру конструкције инфраструктурних објеката, односно њиховог начина простирања на терену. Комарчевић, цитирајући З. Жегарца, са становишта потреба планирања и уређења простора, све техничке инфраструктурне системе дели на:

– *водне* (водовод, канализација, коришћење вода и заштита од вода),
– *саобраћајне* (сувоземни, водни и ваздушни),
– *телекомуникационе* (комуникациони и информациони),
– *енергетске* (електроенергетске, гасоводе, нафтоводе, топловоде и продуктоводе). (Комарчевић, 2018: 33, 34)

Није могуће прецизно дефинисати критичну инфраструктуру јер дефиниција зависи од просторне и временске димензије. Међутим, већинско мишљење јесте да струја, вода, снабдевање горивом, комуникације, транспортни систем, финансијски сектор, влада и јавне службе представљају елементе критичне инфрструктуре у готово свим земљама.

Већина држава у свету идентификовала је и усвојила одговарајуће стратегије заштите чијом је анализом могуће утврдити сегменте заједничке свим државама (саобраћај, комуникације и информационе технологије, водовод и канализацију, енергетику, финансијско пословање и банке, јавно здравље, хитне службе и др), али и сегменте који су карактеристични само за поједине земље. (Lewis, 2006)

КРИТИЧНА ИНФРАСТРУКТУРА У РЕПУБЛИЦИ СРБИЈИ

3

Полазне основе за успостављање система критичне инфраструктуре леже у Уставу Републике Србије у коме пише да су основна права сваког човека: „…право на заштиту свог физичког и психичког здравља...". Надлежност Републике Србије је да уређује и обезбеђује „одбрану и безбедност Републике Србије и њених грађана и мере за случај ванредног стања"; „систем заштите и унапређења животне средине; заштиту и унапређивање биљног и животињског света; производњу, промет и превоз отровних, запаљивих, експлозивних, радиоактивних и других опасних материја" и „заштиту културних добара". Надлежност општине је да се преко својих органа „стара о заштити животне средине, заштити од елементарних и других непогода и заштити културних добара".

Нормативно-правни систем РС подразумева да домаћи правни акти буду у сагласности са Уставом РС. („Службени гласник РС", бр. 83/06, чл. 97) Уставом су, поред осталог, утврђене надлежности Републике и општина у области безбедности и јавног здравља. Према члану 97. Устава, Република обезбеђује „одбрану и безбедност РС и њених грађана; мере за случај ванредног стања", као и „производњу, промет и превоз отровних, радиоактивних и других опасних материја"; и „систем у областима здравства, социјалне заштите" итд. Чланом 190. Устава утврђено је да општине брину о заштити од елементарних и других непогода и о потребама грађана у области здравствене заштите.

3.1 НОРМАТИВНО-ПРАВНИ ОКВИР ФУНКЦИЈЕ И ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

3.1.1. Закон о министарствима

Овим законом („Сл. гласник РС", бр. 44/2014, 14/2015, 54/ 2015, 96/2015 – др. закони и 62/2017) образују се министарства и посебне организације и утврђује њихов делокруг. Могу се образовати и посебне организације чије се поље деловања може утврдити посебним законом.

У складу са овим законом делују следећа министарства:

1) Министарство финансија,
2) Министарство привреде,
3) Министарство пољопривреде, шумарства и водопривреде,
   3а) Министарство заштите животне средине,
4) Министарство грађевинарства, саобраћаја и инфраструктуре,
5) Министарство рударства и енергетике,
6) Министарство трговине, туризма и телекомуникација,
7) Министарство правде,

8) Министарство државне управе и локалне самоуправе;
9) Министарство унутрашњих послова,
10) Министарство одбране,
11) Министарство спољних послова,
11а) Министарство за европске интеграције,
12) Министарство просвете, науке и технолошког развоја,
13) Министарство здравља,
14) Министарство за рад, запошљавање, борачка и социјална питања,
15) Министарство омладине и спорта,
16) Министарство културе и информисања.

Министарства. у оквиру свог делокруга, остварују међународну сарадњу и старају се о њеном унапређењу, обезбеђују усклађивање прописа са правом Европске уније и учествују у преговарачкој структури, припреми преговарачке позиције и вођењу преговора о приступању Европској унији.

Закон о полицији конципиран је тако да се полицијски послови обављају као јединствени у РС („Службени гласник РС", бр. 6/2016, 24/2018 и 87/2018). Њиме се уређују унутрашњи послови, организација и надлежност Министарства унутрашњих послова, полицијски послови, организација и надлежност полиције, као и друга питања од значаја за рад полиције и Министарства. Полицијски послови у складу са овим Законом обављају се у циљу остваривања безбедносне заштите живота, права и слобода грађана, заштите имовине, као и подршке владавини права. Полицијски послови, у смислу овог закона, јесу:

1) превенција криминала и унапређење безбедности у заједници,
2) откривање и расветљавање кривичних дела, обезбеђивање доказа, њихова анализа, криминалистичко-форензичко вештачење употребом савремених форензичких метода и евиденција и откривање имовине проистекле из кривичног дела,
3) откривање и расветљавање прекршаја и привредних преступа,
4) откривање и хапшење учинилаца кривичних дела, прекршаја и других лица за којима се трага и привођење надлежним органима,
5) одржавање јавног реда и мира, спречавање насиља на спортским приредбама, пружање помоћи у извршењима у складу са законом,
6) регулисање, контрола, пружање помоћи и надзор у саобраћају на путевима и други послови из прописа о безбедности саобраћаја,
7) обезбеђење одређених јавних скупова, личности, објеката и простора,
8) безбедносна заштита одређених личности и објеката,
9) контрола државне границе, послови у вези са кретањем и боравком странаца, послови азила, прекограничног криминала, ирегуларних миграција и реадмисије,
10) извршавање послова утврђених прописима о оружју, приватном обезбеђењу и детективској делатности,
11) безбедносна заштита Министарства унутрашњих послова,
12) извршавање других полицијских послова и задатака утврђених законом и подзаконским актом Министарства донетим на основу овлашћења из закона.

Критична инфраструктура је релативно нов појам у Србији, будући да се као термин први пут помиње тек 2011. године у Уредби о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама. Наиме, Уредба у члану 8. истиче процену критичне инфраструктуре са гледишта елементарних непогода и других већих несрећа, али не пружа тумачење дефиниције овог појма. („Службени гласник РС", бр. 8/2011)

Такође, на основу Упутства о методологији за израду процене угрожености од елементарних непогода и других несрећа и планова заштите и спасавања у ванредним ситуацијама („Сл. гласник РС", 18/2017) утврђују се критеријуми за процену једанаест сектора критичних инфраструктура са становишта њихове угрожености од елементарних непогода и дру-

гих несрећа. Иако је методологија садржина свеобухватнији приступ у заштити критичних инфраструктура у домаћем законодавству, оријентисан је на идентификовање извора опасности и последица које поремећаји и прекид у функционисању инфраструктура имају по економију и екологију.

Приступ садржан у методологији не обухвата процену рањивости и отпорности критичних инфраструктура на све врсте претњи, као и мере повећања отпорности које треба да умање штетне последице елементарних и других несрећа на инфраструктури, укључујући и ефекте међузависности. Посебно се указује потреба да се развију модели и методе за повећање отпорности система критичних инфраструктура у циљу унапређења капацитета којима се амортизују ефекти претњи на штићене вредности. Из наведеног разлога, потребно је дефинисати критеријуме за идентификацију потенцијалних претњи/опасности и генерисање опасности имеђу зависности прилагођене различитим секторима критичних инфраструктура у складу са међународним, европским и националним стандардима. (предог Националних становишта; назив пројекта: „Resilience of Critical Infrastructure Protection in Europe (RECIPE)"; пројекат је финансирао Механизам Уније за цивилну заштиту, пројекте приправности и превенције у цивилној заштити и загађењу мора 2014)

Стратегија националне безбедности[6] из 2009. године, као најважнији стратешки документ који утврђује основе политике безбедности у заштити националних интереса, идентификује и дефинише 22 изазова, ризика и претњи по безбедност Републике Србије. Два ризика директно утичу на безбедност становништва и материјалних добара:

1) „Последице елементарних непогода и техничких и технолошких несрећа, као и угрожавање животне средине и здравља грађана, услед радиолошке, хемијске и биолошке контаминације." и

2) „Опасности повезане са појављивањем и ширењем инфективних болести код људи и зараза код животиња могле би бити све израженије". Један од основних циљева политике националне безбедности је и унапређење безбедности грађана, друштва и државе кроз формирање „ефикасног система одбране".

Област управљања ванредним ситуацијама до краја 2018. године била је уређена Законом о ванредним ситуацијама, донетим у децембру 2009. године, потом су уследиле измене и допуне 2011. и 2012. године. Систем реаговања у ванредним ситуацијама, који је био главни предмет уређивања овог закона, нашао се пред огромним изазовима током катастрофалних мајских поплава 2014. године. Услед поплава били су угрожени животи, здравље и имовина више од 1,6 милиона људи у 119 општина централне и западне Србије, а укупна штета износила је 1,7 милијарди евра, што чини више од 4 % бруто друштвеног производа. Полазећи од искустава стечених применом Закона о ванредним ситуацијама, преузетих међународних обавеза и новог развоја који је, после 2009. године, уследио у области политике смањења ризика од катастрофа на светском и европском нивоу, као и од препорука које су упућене Републици Србији, у вези са доградњом правног и институционалног оквира за управљање ризиком од катастрофа, нарочито у погледу потребе даљег развоја превентивних активности, оцењено је целисходним припремање новог закона који би уредио питања у овој области. Основни циљеви којима теже решења у Закону о смањењу ризика од катастрофа и управљању ванредним ситуацијама („Службени гласник РС", 87/2018) јесу, првенствено, свеобухватно нормирање превентивних мера и активности ради смањења ризика од катастрофа, ефикасно реаговање у случају наступања катастрофа, као и што ефикасније отклањање њихових последица како би се што пре обезбедили опоравак и нормализација услова за живот и рад у погођеном подручју.

Сагласно томе, а у складу са усвојеним документима на Другој и Трећој светској конференцији о смањењу ризика од катастрофа (Хјого оквир за деловање из 2005. године и Сендаи

6 На: http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/strategije/Strategija%20nacionalne%20bezbednosti%20Republike%20Srbije.pdf

оквир за деловање из 2015. године), узимајући у обзир савремена упоредна решења у овој области, поменутим законом стављају се у први план принципи, плански документи и мере и активности које треба да допринесу што успешнијој превенцији од катастрофа, јачању отпорности појединаца и заједнице на последице елементарних и грдих непогода и подизању нивоа спремности за реаговање у случају наступања елементарне и друге непогоде. Акценти су стављени на заштиту рањивих група и родну равноправност, као и на успостављање партнерства јавног и приватног сектора и укљученост научних организација, удружења и организација цивилних друштава у процес креирања и спровођења политике смањења ризика од катастрофа.

Новину представља и нагласак на међународној сарадњи, како у домену превенције, тако и домену хуманитарне помоћи и пружања односно примања међународне помоћи ради заједничког одговора на последице елементарних и других непогода. С тим у вези, поред обавеза које за Републику Србију проистичу из закључених билатералних уговора и мултилатералних конвенција, посебно се имала у виду чињеница да је Влада Републике Србије, 16. априла 2015. године, потписала Споразум о учешћу Републике Србије у Механизму ЕУ за цивилну заштиту. Када је реч о решењима којима се уређује систем реаговања у ванредним ситуацијама, она су углавном ослоњена на постојећа решења, с тим што је из њих отклоњено оно што се у пракси показало нефункционалним и недовољно ефикасним. У целини, та су решења поједностављена и иновирана како би била јаснија и применљивија. Имајући у виду да се поменути систем налази у процесу изградње од доношења Закона о ванредним ситуацијама и да су у томе постигнути одређени резултати, сматрало се да је оптималније да се његова изградња настави на започетим основама, уместо да се излаже непотребним иновацијама.

Основни циљ и разлог за доношење Закона је потреба да се систем смањења ризика од катастрофа и управљања ванредним ситуацијама, као део јединственог система националне безбедности у Републици Србији, правно уреди на јединствен начин, стварањем правних услова за успостављање јединственог и интегрисаног система, а да се истовремено систем организације и функционисања усклади са реалним потребама заштите и спасавања становништва и материјалних добара од елементарних и других непогода. Такође, у периоду примене Закона о ванредним ситуацијама, а на бази искустава у досадашњим ванредним ситуацијама, указала се потреба за доношењем новог закона, са жељом да се прецизније дефинишу поједине одредбе које ће његову примену учинити јаснијом, а самим тим и ефикаснијом и прецизнијом. На тај начин би се омогућило свим субјектима система заштите и спасавања да тачно знају своја права и обавезе а, такође, буду свесни последица уколико не поштују одредбе закона. Доношење закона може се оправдати имплементацијом правних норми које представљају највиши стандард у нормирању оних области чији је предмет заштита основних вредности (живот, интегритет, природна околина и својина), те би се усвајањем закона, усклађеног са поменутим правилима, достигао највиши степен безбедности грађана.

Аутори *Националне стратегије заштите и спасавања* („Службени гласник РС”, бр. 86/2011) образлажу усвајање и спровођење стратегије и наводе да је регион југоисточне Европе све угроженији 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, угрожавању људског здравља, опстанка многих природних врста и очувању културног наслеђа. Национална стратегија заштите и спасавања обухвата системе превенције, ублажавања, заштите, спасавања и обнове. Основ за спровођење стратегије, како се наводи, у Националној стратегији „садржан је у Закону о ванредним ситуацијама којим је дефинисано успостављање интегрисаног система заштите и спасавања”.

Основ за израду Националне стратегије обухваћен је и 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. (Mićović, Jakovljević, 2014: 900—906)

Стратегија одбране Републике Србије („Службени гласник РС", бр. 88) дефинише десет изазова, ризика и претњи по одбрану Републике Србије, од којих се посебно издвајају „елементарне непогоде и хемијске, биолошке, нуклеарне, техничке и технолошке несреће"; дефинише три основна циља политике одбране од којих је посебно важан онај који се тиче формирања „ефикасног система одбране" чији је циљ заштита одбрамбених интереса кроз реализацију војне и цивилне одбране. Носилац цивилне одбране су субјекти одбране (Република Србија, општине), привредна друштва, јавне службе и остали субјекти и снаге система одбране. Тежишна мисија цивилне одбране су заштита и спасавање (скр. ЗиС), првенствено људи – цивилна заштита, затим материјалних и културних добара и очување животне средине.

Осим претходно наведених стратегија и закона везаних за националну безбедност, ванредне ситуације и заштиту и спасавање у Републици Србији постоји још законских оквира који су директно или индиректно тичу (законски још увек недефинисану) заштите критичне инфраструктуре. (Мићовић, 2014: 165—174)

Законом о железници („Службени гласник РС", бр. 41/2018) уређени су управљање железничком инфраструктуром, обављање делатности железничког превоза, лиценцирање железничких превозника, приступ железничкој инфаструктури, услужним објектима и услугама, утврђена су начела и поступци за одређивање и обрачун цена приступа јавној железничкој инфраструктури, цена услуга у вези са обављањем железничког превоза, додела капацитета јавне железничке инфраструктуре, индустријске железнице и индустријски колосеци, надлежности Дирекције за железнице, права путника и услуге јавног превоза путника железницом од општег економског интереса

Законом о безбедности у железничком саобраћају („Службени гласник РС", бр. 41) прописани су услови чије је испуњење неопходно како би се железнички саобраћај у Републици Србији одвијао безбедно и несметано. Одредбе овог закона не примењују се на метрое, трамваје и друге лаке шинске системе.

Законом о интероперабилности железничког система („Службени гласник РС", бр 41) утврђени су услови који осигуравају безбедност и интероперабилност железница у Републици Србији како би се саобраћај одвијао несметано.. Безбедност железнице, према тексту закона, обухвата услове које морају испунити железнички систем и радници, као и услове значајне за остваривање безбедног и несметаног одвијања железничког саобраћаја. Интероперабилност железнице је, у смислу овог закона, способност железничког система да омогући безбедан и непрекинут саобраћај возова који испуњавају потребне захтеве за одређену мрежу. Та способност зависи од свих регулаторних, техничких и експлоатационих услова који морају бити испуњени да би се задовољили основни захтеви интероперабилности. Закон посебно обрађује заштиту железничке инфраструктуре и возила. 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 („Службени гласник РС", бр. 44/2010, 60/2013 – одлука УС, 62/014 и 95/2018 и др закони) прописује услове и начине обављање делатности у области електронских комуникација, надлежности, државних органа у области електронских комуникација, уређује положај Републичке агенције за електронске комуникације, видове спровођења јавних консултација у области електронских комуникација, утврђује упра-

вљање и коришћење адреса и бројева, управљање, коришћење и контролу радио-фреквенцијског спектра, дистрибуцију и емитовање медијског садржаја, заштиту права корисника и претплатника, безбедност и интегритет електронских комуникационих мрежа и услуга, тајност електронских података, законито пресретање и задржавање података, мере за поступање супротно одредбама овог Закона, као и друга питања везана за функционисање и развој електронских комуникација у Републици Србији.

Закон о водама („Службени гласник РС", бр. 30/10, 93/2012 и 101/2016) укључује неколико чланова, којима се регулишу ризици и потенцијалне опасности које проистичу из вода, а који су у складу са Законом о ванредним ситуацијама. Закон о водама утврђује предузимање одговарајућих мера ради заштите водотока, као и критеријуме за одређивање подручја угрожених услед поплава и ерозије водом (поплавних и ерозионих подручја); препознаје 'воде I реда и воде II реда', и утврђује надлежност за њихову заштиту (јавно водопривредно предузеће за воде I реда и јединице локалне самоуправе за воде II реда), као што је и дефинисано планским документима који се израђују за сваки ниво управе. Постоји општи и оперативни план за одбрану од поплава.

У јулу 2014. године, израђен је *Закон о отклањању последица поплава у Републици Србији* („Службени гласник РС", бр. 75/2014, 64/2015 и 68/2015 - др. закон), као и други законски акти, с циљем брже реконструкције на подручјима погођеним поплавама и клизиштима у мају 2014. године.

Законом о метеоролошкој и хидролошкој делатности („Службени гласник РС", бр. 88/2010) уређују се метеоролошка и хидролошка делатност, организација и начин обављања метеоролошких и хидролошких послова од интереса за Републику Србију и осталих метеоролошких и хидролошких послова, систем ране најаве метеоролошких и хидролошких елементарних непогода, фонд метеоролошких и хидролошких података и информација, заштита хидрометеоролошког информационог система, међународна сарадња, као и друга питања значајна за метеоролошку и хидролошку делатност.

Стратегија развоја електронских комуникација („Службени гласник РС", бр. 68/10) у Републици 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[7]. У оквиру Европске уније ИКТ су препознате као главни фактор утицаја на економски раст и иновативност (Annual Information Society Report 2007), а међу седам водећих иницијатива економске стратегије Европа 2020 (Europe 2020 – A strategy for smart sustainable and inclusive growth) 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 како би се повећала ефикасност рада, економски раст, запосленост и побољшао квалитет 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 2015–2018. године и акциони план за спровођење Стратегије за период 2015–2016. године („Службени гласник РС", бр. 107/2015) утиче на развој информационог друштва у областима јавне управе, здравства, образовања, правосуђа, социјалне политике, јавних набавки, партиципација у одлучивању, сигурности података и електронских трансакција, доступности и приступачности,

7 Усвојена је 8. 7. 2010. године.

безбедности података о личности, као и на развој и употребу отворених података које поседују органи јавне власти, а који су настали у раду или у вези са њиховим радом. Стратегија утврђује основне циљеве и приоритете унапређења стања електронске управе у Републици Србији. Постоје различите дефиниције електронске управе. Једна од најчешће коришћених је она која електронску управу описује као коришћење информационо-комуникационих технологија (скр. ИКТ) које пружају могућности грађанима и привреди да комуницирају и пословно сарађују са јавном управом, користећи електронске медије (интернет, мобилни телефон, паметне картице, киоске итд.). Акциони план је пратећи део Стратегије и обухвата активности, носиоце активности, рокове за реализацију, индикаторе успеха и финансијска средства неопходна за остварење сваке од активности. Стратегија се заснива на усвојеним опредељењима Владе утврђеним у Стратегији реформе државне управе, Стратегији развоја информационог друштва до 2020. године, као и процесу реформе јавне управе која је уређена Стратегијом реформе јавне управе и другим стратешким документима. Стратегија утврђује кораке за развој националног Портала еУправа (функционалност и сервиси који ће на њему бити имплементирани), јединствене тачке приступа и магистрале за комуникацију са осталим порталима и системима државних органа, који тренутно пружају електронске сервисе као што су портал еПорези, интернет презентације Агенције за привредне регистре, Управе царина, који ће омогућити грађанима, привредним и свим друштвеним субјектима коришћење јавне услуге у што већој мери посредством интернета.

Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС", бр. 94/2017) уређују се електронски документ, електронска идентификација и услуге од поверења у електронском пословању. Електронски документ је скуп података састављен од слова, бројева, симбола, графичких, звучних и видео материјала, у електронском облику. Електронска идентификација је поступак коришћења личних идентификационих података у електронском облику који једнозначно одређују правно лице, физичко лице или физичко лице у својству регистрованог субјекта. Електронско пословање је употреба података у електронском облику, средстава електронске комуникације и електронске обраде података у обављању послова физичких и правних лица.

Законом о електронској трговини („Службени гласник РС", бр. 41/2009 и 95/2013) уређују се услови и начин пружања услуга информационог друштва, обавезе информисања корисника услуга, комерцијална порука, правила у вези са закључењем уговора у електронском облику, одговорност пружаоца услуга информационог друштва, надзор и прекршаји. Одредбе овог закона не примењују се на: заштиту података о личности, делатност јавних бележника и других сродних професија у погледу примене поверених јавних овлашћења, рестриктивне споразуме, у смислу прописа о заштити конкуренције, опорезивање, заступање странака и заштиту њихових интереса пред судовима, као ни на игре на срећу са новчаним улозима, укључујући лутријске игре, игре у казинима, кладионичке игре и игре на срећу на аутоматима, ако посебним законом није друкчије одређено.

Законом о потврђивању Конвенције о високотехнолошком криминалу („Службени гласник РС", бр. 19/2009) се потврђује Конвенција о високотехнолошком криминалу, настала 23. 11. 2001. године у Будимпешти, којом се као кривична дела 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 кривичних радњи у оквиру ИКТ сектора, а за која се држава потписница обавезује да ће прописати одговарајуће законске казне.

Правилник о издавању временског жига („Службени гласник РС", бр. 112/2009) прописује услове 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 садржа-

но у њему, као и садржај и начин вођења Регистра издавалаца временског жига у Републици Србији.

Закон о приватном обезбеђењу („Службени гласник РС бр. 104/13) у члану 4. дефинише обавезно обезбеђене објекте као објекте од стратешког значаја за Републику Србију и њене грађане, уз њих и објекте од интереса за одбрану земље и посебног значаја чијим би оштећењем или уништењем могле наступити теже последице по живот и здравље људи,

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Службени гласник РС", бр. 61/2005 и 104/2009) по први пут су у Србији утврђени надлежни органи за борбу против сајбер криминала. Високотехнолошки криминал, у смислу овог закона, представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.

Закон о информационој безбедности („Службени гласник РС", бр. 6/2016 и 94/2017) је први кровни закон чији текст прописује мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређује надлежне органе за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

Законом о тајности података („Службени гласник РС", бр. 104/2009) уређује се јединствен систем одређивања и заштите тајних података. Овај закон је изузетно значајан с обзиром на то да Закон о информационој безбедности прописује посебне процедуре и мере заштите које се односе на тајне податке, а да нигде не дефинише исте већ упућује на Закон о тајности података. Информационо-комуникациони систем, према Закону о тајности података, јесу системи од посебног значаја који се користе:

1) у обављању послова у органима јавне власти;

2) за обраду података који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности;

3) у обављању делатности од општег интереса и то у областима:

– производње, преноса и дистрибуције електричне енергије,

– производње и прерада угља,

– истраживања, производње, прераде, транспорта и дистрибуције нафте и природног и течног гаса.

– промета нафте и нафтних деривата; железничког, поштанског и ваздушног саобраћаја,

– електронске комуникације,

– издавања службеног гласила Републике Србије,

– управљања нуклеарним објектима,

– коришћења, управљања, заштите и унапређивања добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја),

– производње, промета и превоза наоружања и војне опреме,

– управљања отпадом,

– комуналне делатности.

– послова финансијских институција,

– здравственеа заштите;

– услуга информационог друштва намењених другим пружаоцима услуга информационог друштва с циљем омогућавања пружања њихових услуга.

Једну од најважнијих законских новина чини оснивање Националног центра за превенцију безбедносних ризика, што је, према међународној пракси, Центар за хитне случајеве (скр. ЦЕРТ), тело задужено за брзо реаговање у случају инцидената, као и прикупљање и

размену информација о ризицима за безбедност информационо-комуникационих система. Национални ЦЕРТ је у надлежности Регулаторне агенције за електронске комуникације и поштанске услуге (скр. РАТЕЛ). Оснивање националног ЦЕРТ-а је, уједно, и једна од основних обавеза прописаних НИС Директивом ЕУ, па тако и обавеза свих држава чланица Уније, као и корак који све земље кандидати треба да имају на уму. Закон, такође, уређује и питања као што су ИКТ системи од посебног значаја и мерење њихове заштите (што је, исто, један од захтева у складу са НИС Директивом) и пружа основно уређење за област криптобезбедности и заштите од компромитујућег електромагнетног зрачења (скр. КЕМЗ). Предвиђено је и формирање инспекције за информациону безбедност која врши надзор над применом закона и радом оператора посебно значајних ИКТ система, која је у надлежности министарства надлежног за послове информационе безбедности, тренутно Министарства за трговину, туризам и телекомуникације.

Један од главних разлога за доношење *Закона о критичној инфраструктури* („Службени гласник РС" 87/2018) јесте непостојање јединственог Закона из ове области и потреба да се она обједини. Термин 'критична инфраструктура' спомиње се у више различитих докумената, и то, најпре, у Закону о ванредним ситуацијама, затим у уредбама и стратегијама, али и у Закону о информационој безбедности и Закону о приватном обезбеђењу. Законом се најпре дефинишу термини унети у садржину, почев од тога шта је сектор критичне инфраструктуре, затим начин на који се врши идентификација, одређивање, заштита, ко су оператори, шта је безбедносни план, официр за везу и на крају шта је европска критична инфраструктура. Начела деловања садржана у овом Закону односе се на надлежне органе, организације и грађане и ови субјекти су дужни да их се придржавају. Начела су таксативно набројана у Закону, а то су начело интегрисаног приступа, начело одговорности, начело заштите од разних врста претњи, начело континуираног планирања заштите критичне инфраструктуре, начело размене података и информација и заштите података.

Закон дефинише критичну инфраструктуру као систем, мрежу, објекте или делове чији прекид функционисања или испоруке роба или услуга може имати озбиљне последице по националну безбедност, здравље, животе и имовину, животну средину, безбедност грађана, односно може угрозити функционисање Републике Србије. За идентификацију и категоризацију критичне инфраструктуре задужена су министарства надлежна за одређене области. Критеријуме за идентификацију прописује Влада. Сектори у којима се идентификује критична инфраструктура су: енергетика, саобраћај, снабдевање водом и храном, здравство, финансије, телекомуникационе и информационе технологије, заштита животне средине и функционисање државних органа. Након што Влада донесе критеријуме за одређивање критичне инфраструктуре, Министарства надлежна за секторе дужна су да у року од шест месеци Министарству доставе предлоге сопствене критичне инфраструктуре. Министарства су обавезна да квартално извештавају о новонасталим променама у свом сектору.

Безбедносни план је документ којим се утврђују мере смањења ризика, дефинишу одговорности и одређују дужности, сви оператори критичне инфраструктуре дужни су да га израде и од Министарства прибаве сагласност.

Предлагач Закона уводи посао официра за везу који се означава као лице које служи за контакт између оператора и надлежног Министарства, које обезбеђује сталну контролу, обавештава о променама, координира Безбедносним планом и бави се осталим пословима везаним за критичну инфраструктуру. Ово лице именује Министарство на предлог оператора и то три месеца након одређивања система и оно мора поседовати лиценцу за обављање наведених послова. Када је реч о критичној инфраструктури у планским документима посебна пажња се обраћа у делу превентивних активности и одговора на ванредне ситуације. У случају наступања угрожавајућих околности Штаб за ванредне околности реагује у сарадњи са Министарством.

Као што је већ споменуто у уводном делу, део Закона односи се и на европску критичну инфраструктуру. Како би било јасније шта све она обухвата предлагач даље прецизира да је то инфраструктура од значаја за најмање две државе чланице Европске Уније. Секторе критичне инфраструктуре одређује Европска комисија, а на територији Србије, на предлог Министарства, одређује Влада у сагласности са чланицама Европске Уније.

Надзор над применом овог Закона врши Министарство преко инспектора, а у вршењу инспекцијског надзора инспектор има низ овлашћења на основу којих може да прегледа документа, проверава да ли су наредбе спроведене, налаже израде докумената, обуставља мере које нису у складу са Безбедносним планом, отклања недостатке, предузима хитне мере, предлаже покретање прекршајног поступка и друге мере на које је овлашћен. Казнене одредбе су предвиђене за две категорија лица, за правно лице које које управља системима који су одређени као критична инфраструктура уколико не прибави сагласност, не достави предлог за именовање официра и не поступи по налогу инспектора. Друга група се односи на одговорно лице у надлежним државним органима уколико не достави Министарству предлоге критичне инфраструктуре, промене и предлоге измена и допуна у свом сектору и уколико не поступи по налогу инспектора. (http://www.otvoreniparlament.rs/akt/3781)

Закон о приватном обезбеђењу („Службени гласник РС“ бр. 104/2013 и 42/2015) дефинише појам ’обавезно обезбеђених објеката’ као „објеката од стратешког значаја за РС и њене грађане, као и објеката од посебног значаја чијим оштећењем или уништењем би могле наступити теже последице по живот или здравље људи или који су од интереса за одбрану земље.“ Под обавезно обезбеђеним објектима сматра се и простор на коме се налазе ти објекти који чине њихов саставни део, као и пратећи објекти који су у функцији тих објеката.

Поред наведених, постоји још читав низ секторских закона у областима одбране, тајности података, вода, безбедности хране, просторном планирању, заштити од пожара, заштити животне средине, јавно-приватном партнерству, који не помињу децидно термин ’критична инфраструктура’, али који третирају поједине сегменте критичне инфраструктуре као полазну основу.

Други релевантни закони укључују *Закон о локалној самоуправи* („Службени гласник РС”, бр. 129/2007, 83/2014 – др. закон и 101/2016 — др. закон и 47/2018) који утврђује старање о безбедности свих грађана као једну од главних надлежности локалних власти. Међутим, смањење ризика од катастрофа и управљање ванредним ситуацијама помиње се у само једном члану овог Закона, где се утврђује да се „општина, преко својих органа, у складу са Уставом и законом... стара о заштити животне средине, заштити од елементарних и других непогода, заштити културних добара од значаја за општину” (члан 20).

3.2. САДАШЊЕ СТАЊЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

Ангажовање на међународној сцени за сваку државу подразумева и одређене обавезе према организацијама у чијем раду учествује. У случају Србије, најзначајније међународне обавезе проистичу из званичног стратешког циља државе да постане земља чланица Европске уније. Србија је 2012. године званично постала земља кандидат за чланство у ЕУ, а прва преговарачка поглавља отворила у децембру 2015. Процес приступања Унији подразумева усаглашавање законодавног оквира државе са постојећим заједничким нормативним оквиром и принципима ЕУ. Када је у питању област информационе безбедности, Србија у процесу развоја националног нормативног оквира мора да има у виду постојеће законодавство у Европској унији, што обухвата и трендове који су, за сада, у развоју и који ће највероватније, постати заједнички принципи земаља Уније до тренутка приступања Србије ЕУ.

Кровни прописи ЕУ, у овој области, првенствено подразумевају Директиву о мерама за обезбеђивање највећег нивоа безбедности мрежних и информационих система широм ЕУ (НИС Директива) из 2016. године и Конвенцију о сајбер криминалу Савета Европе из 2001. године, као и документа попут Стратегије сајбер безбедности Европске уније, Стратегије јединственог дигиталног тржишта, Европске агенде безбедности и сл. Усаглашавање са кровним прописима је обавеза свих земаља чланица па се тако очекује и од држава које стреме да то постану. Међутим, неопходно је имати у виду и принципе и стандарде прописане другим наведеним документима, јер они могу бити водич Србијис обзиром на то да се она налази на самом почетку успостављања свеобухватног нормативног и оперативног механизма националне информационе безбедности. Ово је посебно значајно ако се узме у обзир и чињеница да недавно представљена Глобална стратегија спољне и безбедносне политике Европске уније предвиђа укључивање „сајбер" питања у све области политике, у оквиру Заједничке безбедносне и одбрамбене политике Уније, са којом се Србија у процесу приступања Унији усаглашава.

Почетком друге деценије XXI века, привреда и друштво Републике Србије налазе се у врло дубокој општеразвојној кризи. Република Србија се, у времену продужене економске рецесије, налази пред изазовом да трасира дугорочни пожељни пут развоја енергетике и дефинише стратешка опредељења на којима ће се заснивати тај развој у наредном средњорочном периоду.

Република Србија определила се да Министарство унутрашњих послова буде надлежно за израду процене угрожености од елементарних непогода и других несрећа, коју доставља Влади на усвајање (према тексту до скоро важећег Закона о ванредним ситуацијама – „Службени гласник РС" бр. 111/2009, 92/2011 и 93/2012). Аутономне покрајине, 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.

Предмет закона није се бавио критичном инфраструктуром, већ тиме како опасности, посредством критичне инфраструктуре, утичу на вредности које треба заштити. Овим законом захтевано је да се проценом угрожености идентификују извори могућег угрожавања, сагледаају могуће последице, потребе и могућности спровођења мера и задатака заштите и спасавања од елементарних непогода и других несрећа. Процена угрожености се, пре свега, односи на:

1) утврђивање карактеристика територије, критичних постројења, критичних места и простора, са гледишта угрожености од елементарних непогода и других несрећа, укључујући евентуалне прекограничне ефекте удеса,

2) предвиђање повредљивости територије услед елементарних непогода и других несрећа,

3) анализу могућих последица насталих након елементарних и других несрећа,

4) потребе и могућности за заштиту људи, материјалних добара и животне средине од последица елементарних и других несрећа.

Процена предвиђа свеобухватан приступ у заштити критичне инфраструктуре, мада оријентисан на идентификовање извора опасности и последица које поремећаји и прекид у функционисању критичне инфраструктуре имају по економију и екологију.(Мићовић, 2016)

На основу Закона о ванредним ситуацијама донета је Уредба о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама („Службени гласник РС", бр. 8/2011). Овим документом, поред већ наведених елемената процене угрожености, дефинисаних у Закону о ванредним ситуацијама, предвиђа се да ће део предвиђања 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 одговорни за заштиту критичне инфраструктуре.

Потреба разматрања безбедности критичне инфраструктуре препозната је у оквиру пројекта „Управљање критичном инфраструктуром за одрживи развој у поштанском, комуникационом и железничком сектору Републике Србије". (Gospić, Murić, 2012)Република Србија је последњих година учинила значајне напоре у стварању интегрисаног система заштите и спашавања како би се на адекватан начин одговорило у условима угрожавања критичних националних ресурса.

Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама („Службени гласник РС", бр. 87/2018) ставља акценат на смањење ризика и управљање ризицима од катастрофа; промовише смањење ризика од природних и других непогода, укључујући и спречавање, ублажавање и спремност за реаговање и ефикасан одговор, активности заштите и спасавања у различитим секторима, чиме се јача отпорност појединаца и заједница на опасности; утврђује права и обавезе грађана, удружења, јединица локалне самоуправе, аутономних покрајина и Републике Србије; промовише међународну сарадњу, управну инспекцију и друга питања која се односе на структуру и функционисање система.

Као резултат овог новог Закона о смањењу ризика и управљању ванредним ситуацијама, Србија се тренутно налази у фази трансформације „старог" система, који је у великој мери фокусиран на реаговање на ванредне ситуације, у проактивнији систем, који још увек није формализован, и који је у већој мери фокусиран на смањење ризика од катастрофа и јачање отпорности.

У погледу мера заштите критичне инфраструктуре, све државе, укључујући и Републику Србију, морају да утврде и редослед поступака:

а) идентификација критичне инфраструктуре,

б) израда мапа критичне инфраструктуре,

в) размена информација,

г) оспособљавање особља ангажованог на пословима и задацима у системима критичне инфраструктуре,

д) увежбавање система за заштиту критичне инфраструктуре или опоравак у случају кризне или ванредне ситуације. (Национална стратегија заштите и спречавања у ванредним ситуацијама; усвојена на седници Скупштине РС 18. 11. 2011.)

Одредбама чл. 15 и 57 Закона о полицији („Службени гласник РС", бр. 101/2005, 63/2009, одлука УС и 92/2011) утврђене су посебне мере значајне за заштиту здравља и живота људи и спречавање угрожавања безбедности изазваног елементарним непогодама или епидемијама. Те мере своде се на овлашћење државе да у изузетним случајевима, попут поплава 2014. године, адекватно реагује и ограничи или забрани кретање на одређеним подручјима, спречи настањивање неке области, наложи евакуацију односно напуштање извесних подручја или објеката.

Треба нагласити да институционални оквир за дефинисање критичне инфраструктуре представља рад Сектора за ванредне ситуације, надлежних министарстава и регулаторних тела. Одређене мере заштите делова инфраструктуре предузимају оператери, али нису донесене ни стратегија ни политика заштите на нивоу земље.

Република Србија обезбеђује стварање јединственог система заштите и спасавања у складу са Законом о ВС и другим прописима, као и програмима, плановима и другим документима. Овај јединствен чине:

1. *Систем заштите и спасавања* – подсистем националне безбедности и интегрисани облик управљања и организовања субјеката система заштите и спасавања на спровођењу превентивних и оперативних мера и извршавању задатака заштите и спасавања људи и добара од последица елементарних непогода, технолошких несрећа и катастрофа, последица тероризма, ратних и других већих несрећа, укључујући и мере опоравка од тих последица и

2. Цивилна заштита која је организован систем чија је, такође, основна делатност заштита, спасавање и отклањање последица елементарних непогода, техничко-технолошких не-

срећа и других већих опасности које могу угрозити становништво, материјална, културна добра и животну средину у редовном, али и у ванредном и ратном стању.

У данашње време поменути системи удружују се стварањем основног државног система заштите становништва и територија под општим називом „систем заштите и спасавања у ванредним ситуација". Системом заштите и спасавања у ванредним ситуацијама, као делом система националне безбедности, руководи Савет за националну безбедност РС, на чијем челу је председник. Основни систем заштите и спасавања у ванредним ситуацијама у РС обједињује снаге и средства органа државне управе, аутономних покрајина, градова и јединица локалне самоуправе, привредних друштава и других правних лица, грађана, група грађана, удружења, професионалних и других организација које су овлашћене и оспособљене да решавају питања заштите и спасавања становништва и територија од ванредних ситуација.

Такође, у Републици Србији се критична инфраструктура помиње и у оквиру поглавља 6.2. Стратегије развоја информационог друштва у Републици Србији до 2020 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 електроенергетског система."

Осим Закона о критичној инфраструктури, Национална стратегија заштите и спасавања у ванредним ситуацијама бави се питањем критичне инфраструктуре. Усвојена су и друга два документа, међутим, у њима се не помиње термин 'критична инфраструктура', , мада закони себаве питањима везаним за заштиту критичне инфраструктуре.

Овим документом се, по први пут, уводи појам критичне инфраструктуре који није јасно дефинисан и чија садржина није прецизно одређена. У нашој земљи појам и проблематика критичне инфраструктуре, како у теорији тако и у пракси, нису непознати, већ редефинисани. За време СРЈ, а на основу члана 36. става 3 Закона о одбрани („Службени лист СРЈ", бр. 43/94 и 28/96), Савезна влада је донела Одлуку о одређивању великих техничких система од интереса за одбрану земље. Овом одлуком одређени су велики технички системи важни за одбрану земље, као и техничка средства значајна за функционисање тих система у области веза, информатике, електроенергетике, водоснабдевања, саобраћаја и другим областима, при чијем су избору, изградњи и развоју те набавкама техничких средстава за њихово функционисање, инвеститори дужни да их ускладе са потребама одбране земље; прописује се поступак обавештавања о избору, изградњи и развоју система, набавкама техничких средстава и постављању захтева за њихово усклађивање са потребама одбране земље. Такође, Влада РС је још 1992. године донела Уредбу о објектима и регионима од посебног значаја за одбрану РС („Службени гласник РС", бр. 18/92). Објектима од посебног значаја за одбрану РС сматрају се, према тексту Уредбе, објекти за које се проценом утврди да би њиховим оштећењем могле настати теже последице за одбрану и безбедност РС. У ове објекте спадају реони и објекти у области саобраћаја, телекомуникација, енергетике, водопривреде и индустрије.

У Републици Србији критичне инфраструктуре су, у највећој мери, власништво државе, привредна друштва која имају монополски положај на тржишту роба и услуга, док је мали број привредних друштава у приватном власништву.

На основу Одлуке о одређивању великих техничких система значајних за одбрану („Службени гласник РС", бр. 41, 35, 86 и 53) дефинисани су велики технички системи за одбрану и техничка средства која су битна за функционисање тих система у области телекомуникација, информатике, саобраћаја, енергетике, водоснабдевања и другим областима значајним за одбрану и прописује се поступак обавештавања о избору, изградњи и развоју

тих система, набавкама техничких средстава и начин обезбеђења техничких средстава и постављању захтева за њихово усклађивање са потребама одбране земље.

Великим техничким системом, у смислу тачке 1 наведене Одлуке, сматра се целина, односно скуп међусобно уређених делова и поступака који обезбеђују техничко-технолошко јединство и самосталност система или његову функционалну повезаност са другим техничким системима значајним за одбрану.

Велики технички системи на територији Републике Србије су:

1) у области телекомуникација: Предузеће за телекомуникације „Телеком Србија" акционарско друштво, Београд; „Теленор" д. о. о., Београд и „Випмобајл" д.о.о., Београд;

2) у области саобраћаја: Акционарско друштво за ваздушни саобраћај „Ер Србија", Београд; Акционарско друштво аеродром „Никола Тесла", Београд; Контрола летења Србије и Црне Горе СМАТСА д. о. о., Београд; Јавно предузеће „Пошта Србије", Београд и Акционарско друштво „Железнице Србије", Београд; Акционарско друштво за железнички превоз путника „Србија Воз", Београд; Акционарско друштво за железнички превоз робе „Србија Капго", Београд и Акционарско друштво за управљање јавном железничком инфраструктуром „Инфраструктура железнице Србије, Београд";

3) у области енергетике: Јавно предузеће „Електропривреда Србије", Београд и његова зависна привредна друштва; Акционарско друштво „Електромрежа Србије", Београд**;** „НИС" а. д., Нови Сад и његова зависна привредна друштва; Јавно предузеће „Србијагас", Нови Сад; Друштво за производњу уља „Рафинерија нафте" акционарско друштво, Београд; Акционарско друштво фабрика мазива „ФАМ", Крушевац и Јавно предузеће „Транснафта", Панчево;

4) у области водоснабдевања: Јавно водопривредно предузеће „Србијаводе", Београд; Јавно водопривредно предузеће „Воде Војводине", Нови Сад; Јавно комунално предузеће „Београдски водовод и канализација", Београд; Јавно предузеће за водоснабдевање „Рзав", Ариље; Јавно комунално предузеће за водовод и канализацију „Наисус", Ниш; Јавно предузеће за водоснабдевање и за производњу и дистрибуцију електричне енергије „Ибар", Зубин поток и Јавно комунално предузеће „Водовод и канализација", Нови Сад;

5) у другим областима: Јавна медијска установа „Радио-телевизија Србије", Београд; Јавно предузеће „Емисиона техника и везе", Београд; „Месер Техногас" акционарско друштво за производњу и промет техничких и медицинских гасова и пратеће опреме, Београд; Јавно предузеће за газдовање шумама „Србијашуме" са потпуном одговорношћу, Београд и Јавно предузеће за газдовање шумама „Војводинашуме", Петроварадин.

Као један од важних задатака Републике Србије на путу европских интеграција јесте усвајање нормативног оквира везаног за критичну инфраструктуру који ће бити усклађен са елементима Директиве Европског савета 2008/114/ЕС. Директива Савета Европе 2008/114/ЕС из 2008. године дефинише критичну инфраструктуру, заједничке процедуре за идентификацију и означавање европске критичне инфраструктуре, заједнички приступ у процени потреба за побољшавање заштите; представља основу за наредне кораке у дефинисању критеријума за критичну инфраструктуру. У складу са тим Република Србија је донела закон о критичној инфраструктури који се примењује од новембра 2018. („Службени гласник РС", бр. 87)

Уставни основ за доношење овог закона садржан је у одредбама члана 97, став 1, тач. 4 и 17, Устава, којима је утврђено да Република Србија уређује и безбедност њених грађана. Заштита критичне инфраструктуре првобитно је, у оквирима ЕУ, била посматрана из угла борбе против тероризма. Изазови са којима се данашње друштво суочава у сфери безбедносне политике су врло разноврсни, од све учесталијих елементарних непогода до различитих изазваних катастрофа, па је неопходно применити динамички, стратешки и, пре свега, мултидисциплинарни приступ када се ради о процесу планирања заштите критичне инфра-

структуре. Приступи утврђивању критичне инфраструктуре у државама разликују се међу државама ЕУ.

Занимање ЕУ за критичну инфраструктуру земаља које су у њеном саставу проистиче из опасности да би разарање или поремећај извесне критичне инфраструктуре у једној од земаља чланица могло непосредно утицати на друге земље чланице. Европска комисија идентификовала је области критичне инфраструктуре: енергија, информационе и комуникационе технологије, вода, храна, финансије, грађанске власти, јавни и правни поредак и сигурност, саобраћај, хемијска и нуклеарна постројења, космос и научно истраживање. Имајући у виду да се ради о широкој, недефинисаној теми, неопходно је критичну инфраструктуру регулисати законом, којим би се дало усмерење за друге посебне законе. С обзиром на то да је Република Србија рањива, постоји потреба да се овим Законом дефинишу стриктне надлежности и одговорности државе.

3.2.1. Улога Сектора за ванредне ситуације у заштити критичне инфраструктуре

По питању проблематике везане за ванредне ситуације, као и последица по критичну инфраструктуру, основни субјект одговора је у надлежности Сектора за ванредне ситуације Министарства унутрашњих послова, који је формиран 2009. године спајањем Сектора за заштиту и спасавање Министарства и Управе за ванредне ситуације Министарства одбране у јединствену службу.[8]

Искуства из досадашњих ванредних ситуација показала су да је примена важећих прописа у области о којој је реч створила проблем јединственог функционисања свих релевантних служби у ванредним ситуацијама, првенствено због подељене надлежности између појединих министарстава и других државних органа. (Благојевић, 2011).Сектор за ванредне ситуације 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; обједињује све постојеће ресурсе у заштити, спасавању и реаговању у ванредним ситуацијама. Сектор настоји да изгради, одржи и унапреди способност читаве нације да превентивно делује на ризике и одговори на изазове и ублажи последице различитих катастрофа које могу погодити наш регион. (Blagojevic, Nikac, 2010: 151-161)

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 с циљем подизања безбедности и смањења броја жртава и материјалне штете.

Главни задаци Сектора су: превентива; надзор; припрема грађана за ванредне ситуације; обука оперативних јединица: набавка опреме за оперативне јединице; спасилачке активности; управљање у ванредним ситуацијама; координација републичке и локалне управе са осталим организацијама на националном, регионалном и локалном нивоу; спровођење мера отклањања последица ВС; размена информација; међународна сарадња.

У извршавању своје функције Сектор обавља следеће послове:
– нормативне,
– управне,
– организационо-техничке,

8 Више о томе на сајту Сектора за ванредне ситуације МУП РС.

– превентивне,
– превентивно-техничке,
– образовне,
– информативно-васпитне,
– друге природе за организовање, 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, техничко-технолошких незгода, 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 с циљем потпуног правног уређивања за обављање послова,
– успостављање институционалних, организационих и персоналних услова за спровођење заштите и спасавања у ванредним ситуацијама,
– предузимање превентивних мера ради спречавања избијања пожара и ублажавања последица елементарних непогода, технолошких незгода и сл,
– предузимање превентивних мера како би се спречило угрожавање здравља грађана услед дејства опасних материја и других опасности,
– стручно оспособљавање припадника организационих јединица на пословима делокруга Сектора и др.

У извршавању наведених задатака Сектор остварује непосредну сарадњу и координацију са свим министарствима и органима државне управе (републички, покрајински и органи локалне самоуправе), привредним друштвима и другим правним лицима, удружењима, професионалним и другим организацијама. Сектор за ванредне ситуације у свом саставу има:
1) Управу за превентивну заштиту,
2) Управу за ватрогасно-спасилачке јединице,
3) Управу за управљање ризицима,
4) Управу за цивилну заштиту,
5) Национални тренинг центар за ванредне ситуације и
6) управе и одељења за ванредне ситуације при полицијским управама.

Управа за превентивну заштиту у свом саставу има:
1) Одељење за спровођење превентивних мера при изградњи објеката,
2) Одељење за спровођење превентивних мера при коришћењу објеката и
3) Одељење за контролу промета и превоза опасних материја.

Управа за ватрогасно-спасилачке јединице у свом саставу има:
1) Одељење за материјално-техничко опремање ватрогасних и спасилачких јединица,
2) Одељење за контролу рада ватрогасних и спасилачких јединица и
3) Одељење за здравство и психолошку превенцију.

Управа за управљање ризиком у свом саставу има:
1) Републички центар за обавештавање (112) и
2) Одељења за: осматрање, обавештавање, узбуњивање и телекомуникације, управљање ризиком од технолошких удеса и терористичких напада и управљање програмима и пројектима.

Управа за цивилну заштиту у свом саставу има:
1) Одељење за оперативно организационе послове цивилне заштите,
2) Одељење за стратешко планирање и координацију и
3) Одељење за техничку подршку и неексплодирана убојна средства.

Функционисање система за заштиту и спасавање у ВС реализује се, у зависности од услова и обима прогнозиране или настале ванредним ситуацијама у три режима (фазе):
1) режим редовне делатности,

2) режим приправности - повећане спремности и

3) режим ванредних ситуација.

Важан део система за ванредне ситуације су снаге и средства која се деле на снаге и средства за надзор и контролу, и снаге и средства за одговор (локализацију и ликвидацију) на ванредне ситуације. Снаге и средства за надзор и контролу обухватају органе, службе и установе, који врше државни надзор, инспекцију, мониторинг, контролу, анализу стања животне средине, потенцијално опасних објеката, материјала, здравља људи.

Снаге и средства за одговор (локализацију и ликвидацију) на ванредне ситуације чине:

– ватрогасно-спасилачке јединице Сектора за ванредне ситуације Министарства унутрашњих послова РС,

– специјализоване јединице цивилне заштите Сектора за ванредне ситуације Министарства унутрашњих послова РС и других предузећа,

– службе хитне медицинске помоћи и мобилне екотоксиколошке лабораторије Министарства здравља РС,

– опште и специјализоване јединице Министарства унутрашњих послова РС (жандармерија, специјална антитерористичка јединица, противтерористичка јединица, хеликоптерска јединица, речна полиција; полицијска бригада, интервентне јединице дежурних служби и др.),

– јединице за уклањање и уништавање неексплодираних убојних средстава (скр. НУС),

– противградне службе Републичке хидрометеролошке службе,

– ватрогасне јединице привредних и добровољних ватрогасних друштава,

– јединице опште намене Цивилне заштите локалне самоуправе и привредних друштава;,

– инжењеријске и друге јединице и јединице радијацијске, хемијске и биолошке заштите Министарства одбране РС, као и национални центар за контролу тровања (ВМА),

– Црвени крст Србије,

– рударско-спасилачке јединице и интервентне екипе „Србија гаса" и електропривредних предузећа,

– ватрогасно-спасилачки возови и специјална шинска возила железница Србије,

– привредна авијација Министарства пољопривреде,

– хаваријско-спасилачке екипе и јединице у предузећима,

– јединице и специјалисти - добровољци друштвених удружења (ватрогасци, спелеолози, алпинисти, кинолози и др.).[9]

Потреба за брзом, организованом и ефикасном акцијом захтева да Сектор за ванредне ситуације буде вођен из једног центра, а неопходна потреба за квалитетном логистиком цивилног друштва у ванредним ситуацијама, као и фокусирање јавног мњења и медија на готово све облике ових ситуација, детерминишу организовање Сектора за ванредне ситуације у оквиру МУП-а. (Blagojevic, Nikac, 2010.)

Начела заштите и спасавања

Систем заштите у спасавања у условима ванредних ситуација у Републици Србији заснива се на сарадњи и правовременом деловању субјеката система у заштити и спасавању првенствено људских живота.

Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама („Службени гласник РС", бр. 87/2018) препознаје:

– *начело приоритета* - смањење ризика од катастрофа и управљање ванредним ситуацијама представља национални и локални приоритет;

9 Званичан сајт Сектора за ванредне ситуације: <http://prezentacije.mup.gov.rs/svs/>.

– *начело интегрисаног деловања и међусекторске сарадње* - управљање ризиком од катастрофа на међусобној координацији и усклађеним процедурама и плановима деловања свих институција и субјеката уз међусекторску сарадњу и партнерство;

– *начело примарне улоге локалних заједница* – јединице локалне самоуправе имају примарну улогу у управљању ризиком од катастрофа и ту улогу подржавају све надлежне државне и покрајинске институције;

– *начело поступности при употреби снага и средстава* – у заштити и спасавању прво се користе снаге и средства са територије јединице локалне самоуправе, а када те снаге и средства нису довољне, надлежни орган обезбеђује употребу других снага и средстава са територије Републике Србије, укључујући полицију и Војску Србије, када је то потребно;

– *начело равноправности и заштите људских права* – субјекти система смањења ризика од катастрофа и управљања ванредним ситуацијама посебно се старају о остваривању принципа равноправности полова и нарочито воде рачуна да ниједна одлука, мера или радња не подстиче или доводи до неповољнијег положаја жена и њиховог неравноправног учествовања у систему смањења ризика од катастрофа и управљању ванредним ситуацијама. Надлежни органи и други субјекти укључени у спровођење мера и активности управљања ризиком од катастрофа дужни су да доследно воде рачуна о заштити људских права, родној равноправности и посебно о заштити сиромашних, старих, деце, особа са инвалидитетом, избеглих и расељених лица, као и других рањивих група становништва. Мере и активности на смањењу ризика од катастрофа морају бити приступачне и односити се и на особе са инвалидитетом, децу, старе и друга лица која су најизложенија ризику;

– *начело партиципативности и солидарности* - право угрожених грађана је да: учествују у осмишљавању садржаја и имплементацији активности на смањењу ризика од катастрофа; учествују у предлагању, предузимању и извршавању одређених мера, задатака и активности у заштити и спасавању и изразе своје потребе у средствима помоћи. Грађани који су погођени последицама катастрофа имају право на помоћ сходно својим потребама и приоритетима које пружају хуманитарне и друге регистроване организације у складу са законом, а уколико су претрпели већу материјалну штету имају и право на државну помоћ, у складу са посебним законом;

– *начело информисања јавности* - надлежни органи благовремено и детаљно информишу јавност о ризицима од катастрофа, релевантним подацима и мерама за заштиту од њихових последица, као и о другим мерама које се предузимају ради управљања ризиком од катастрофа. („Службени гласник РС”, бр. 87/2018)

3.3. ЗНАЧАЈ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ВАНРЕДНИМ СИТУАЦИЈАМА

Ванредне ситуације изазивају смањење сигурности становника услед великих природних катастрофа, прометних, хемијских или инфраструктурних сигурносних угрожавања. Сведоци све више намерних, организованих инцидената са последицама великих размера као што су тероризам, енергетска или финансијска криза. Пратећи трендове и штете изазване оваквим ванредним раздобљима нужно се намеће организовано решење као императив.

Према општој дефиницији, ванредне су оне ситуације које доводе или могу да доведу до људских и материјалних губитака. Поред опште, постоје још неке дефиниције ванредних ситуација:

– Ванредна ситуација је свака непланирана ситуација која може да изазове смрт или значајне повреде запослених, корисника или шире популације, прекине посао или операцију, битно оштети материјална и природна добра или да запрети финансијском стању или угледу предузећа;

– Ванредном ситуацијом сматра се нарушавање нормалног живота и рада људи у објекту или на одређеној територији изазвано хаваријом, елементарним или еколошким удесима,

епидемијама и сл., које доводи или може да доведе до људских или материјалних губитака; (Wahle, Beaty, 2004: 29)Ванредна ситуација је стање при коме се нарушавају нормални услови живота ирада људи у објекту, на одређеној територији или акваторији, угрожава њихов живот и здравље, наноси штета имовини и угрожава животна средина. (Архипова, Кульба, 1998)

Посматрано у ширем контексту, под ванредном ситуацијом подразумева се неочекиван, специфичан ризик који нарушава постојећу динамику процеса рада, утиче на услове живота, социјалну сферу и природну средину. (Јаковљевић, 2010: 15)

Термин ванредна ситуација настао је почетком XX века, јавивши се у руској литератури (рус. 'чрезвычайная ситуация' - ванредна, изванредна, тј. изузетна ситуација). Ванредна ситуација је нарушавање нормалних услова живота и рада, у објектима или на датој територији, хаваријом, елементарном непогодом, катастрофом, еколошким акцидентом, епидемијом и слично; применом расположивих средстава која потенцијални противник може употребити, а чије деловање може да доведе до људских и материјалних губитака, наштети здрављу људи или природи и окружењу, изазове значајне материјалне губитке и наруши квалитет живота и рада људи. (Млађан, Кекић 2007: 64.)

Организација УН је, 1965. године, пошавши од учесталијег присуства различитих опасности које су окарактерисане као ванредне ситуације и потребе да се међународна заједница тим опасностима супротстави, својом Резолуцијом 2034 позвала владе да успоставе одговарајуће националне структуре за планирање и деловање у условима ванредних ситуација, као и пружање неопходне помоћи. Владе су, у већини случајева, успоставиле такве системе планирања и координисале деловање у ванредним ситуацијама у оквиру националних служби цивилне заштите, тако да је смањење учинака свих ванредних ситуација данас повезано са цивилном заштитом и представља њен основни задатак.

Расподела одговорности и надлежности у вези са управљањем ванредним ситуацијама организује се на два нивоа - државном и локалном, а заступљена је у скоро свим државама света. У борби са ванредним ситуацијама влада има највећу одговорност и мора да успостави оквир за:

– превентиву и спречавање настанка ванредних ситуација,

– припрему органа државне управе, специјализованих служби, свих других учесника у заштити и спасавању и становништва за реаговање у ванредним ситуацијама,

– тражење међународне помоћи, пружање помоћи и организацију заштите и спасавања у ванредним ситуацијама значајним за државу,

– санирање последица ванредних ситуација и

– пружање међународне помоћи.

– Одговорност локалне заједнице односи се на:

– процену ризика од ванредних ситуација и планирање,

– прописивање, припрема и спровођење превентивних и оперативних мера заштите и спасавања,

– организовање хитних и других специјалистичких служби за пружање помоћи у ванредним ситуацијама у оквиру своје надлежности,

– оспособљавање и информисање грађана према специфичностима ризика у подручју које настањују;

– спровођење и свих других послова и активности из области заштите и спасавања. (Јаковљевић, 2009: 16.)

Ванредну ситуацију треба разликовати од ванредног стања које представља правну категорију. Ванредно стања које представља посебан правни режим на целој или на делу државне територије за време непосредне ратне опасности или ванредних унутрашњих прилика. Према члану 4, тачка 6, Закона о одбрани, ванредно стање је „стање јавне опасности

у којем је угрожен опстанак државе или грађана, а последица је војних и невојних изазова, ризика и претњи безбедности (Устав РС, „Сл. гласник РС", бр. 98/2006).

Уопштено говорећи, ванредне ситуације изазивају догађаји који нарушавају нормално функционисање служби и предузећа, угрожавају живот грађана, природна и материјална добра (животну средину) и представљају претњу по стабилност (одрживост) локалног, националног и глобалног развоја. Анализа реаговања служби на овакве ситуације (удесе, хаварије и природне катастрофе) у Србији, а и у свету, указује на недостатке, како у организацији, тако и у методологији за реаговање и управљање. (Stanković, 2006: 54-62)Због тога је неопходно развијати системе за подршку у одлучивању, али и системе за образовање и обуку актера у процесу управљања ванредним ситуацијама. Развој ових система треба да буде базиран на савременим информационим технологијама које ће омогућити адекватан, ефикасан и ефективан рад институција, служби и појединаца - учесника у процесу управљања. Овакви системи за подршку управљању ванредним ситуацијама треба да обезбеде бољу комуникацију и размену података између служби одговорних за управљање оваквим ситуацијама. (Stoimenov, Predić, Mihajlović, Stanković, 2005: 635-640)

Имамо ли у виду узроке настанка ванредних ситуација (елементарне непогоде, техногене хаварије и катастрофе, примена средстава за масовно уништење и антропогено деловање на природу), али и последице (људске жртве, нарушавање здравља људи, уништавање материјалних артефакта, загађење, деградација или деструкција природне компоненте животне средине), можемо се сложити са схватањима да је остваривање општепланетарне безбедности приоритетан задатак и циљ на глобалном и националном нивоу. (Ljustina, Malis Sazdovska, Knezevic Lukic, 2014: 263-273)

Треба имати у виду да се сам појам 'безбедност' најпре везује само за одсуство насиља у држави и између држава, а студије безбедности баве се изучавањем претњи, употребе и контроле војне силе. Међутим, у савременим условима појам безбедности схвата се шире, као непостојање војних, политичких, економских и еколошких претњи (Buzan, Waewer, Wilde, 1998), односно као стање заштићености виталних интереса с циљем задовољавања потреба и обезбеђивања могућности прогресивног развоја личности, државе и друштва. („Словарь виталитской социологии", стр. 10.)

Како би се ефикасно управљало ризиком, неопходно је да постоје механизми за мониторинг и извештавање о акцијама усмереним ка митигацији конкретног ризика. Неке од акција могу бити концентрисане само на праћење одређеног ризика у циљу идентификације промена у његовом статусу. Мониторинг се састоји из:

– провере извршења планираних акција и остварења њиховог жељеног ефекта,

– правовремене идентификације развоја ризика,

– моделовања тренда, с циљем прогнозе потенцијалних ризика или могућности и

– система провере комплетног управљања ризиком да би се утврдила ефикасна примена система.

Управљање (менаџмент) је неопходно онда кад две или више особа усклађују своје деловање и изворе како би постигли циљеве које не могу постићи самостално. Управљање се састоји од активности процеса одлучивања које предузимају и спроводе једна или више особа с циљем вођења и координације активности и деловања других људи, и постизања резултата које не може постићи једна особа. Ефикасно управљање фокусирано је на заједничко деловање, различите облике координације и начине доношења одлука.

Вођење операција обухвата доношење одлука, управљање информацијама, решавање проблема, пројекте и програмско планирање, управљање изворима и надзор.

Управљање људима укључује вођење, организацију, управљање кадром (особљем) и процењивање кадра.

Вођење организација односи се на планирање, контролу и усмеравање, развој организације, контролу квалитета, физичку контролу, управљање изворима, комуникације и евалуацију деловања целокупног система и његових делова.

Критичне инфраструктуре део су окружења које у великој мери одређује њихово функционисање. Окружење се може описати на следећи начин: прво, то је пословно окружење које највише утиче на деловање критичних инфраструктура. Иновације и технологија осигуравају развој и на разне начине креирају међузависности, са тенденцијом синергетског повећавања учинака. Често су својства међузависности повезана са власништвом над инфраструктурама, при чему државно и власништво локалних заједница чешће усмеравају инфраструктуре на осигуравање услуга, док приватни сектор тежи повећању профита. Јавне политике представљају другу димензију окружења.

Табела 2. *Класификација ванредних ситуација према размерама*

Ванредне ситуације	**Број настрадалих**	**Нарушеност услова за живот и рад**	**Материјална штета**	**Место дешавања**
Локалне	< 10	< 100	< 1000	На територији где се налази објекат
Месне	10 ÷ 50	100 ÷ 300	100 ÷ 300	На насељеној територији
Територијалне	50 ÷ 500	300 ÷ 500	5000 ÷ 500000	На територији града
Националне	> 500	> 1000	> 5000000	На територији већој од два града
Глобалне (међународне)		Изван граница једне државе		

Критични инфраструктурни системи интегрисани су у модеран живот, граде се како би обезбедили услуге за неколико генерација и током неколико деценија. Данас људи очекују могућност несметаног путовања, у било које време, могућност да комуницирају кад год пожеле. У савременим индустријама сасвим је очекивано да постоји потребна расположива инфраструктура која треба да омогући транспорт сирових материјала, финалних производа, испоруку хране и трајних добара на тржишта и луке, као и размену идеја и финансијских трансакција електронским путем. (Кљајић, 2010)

Сваки инфраструктурни систем састоји се из индивидуалних или међусобно повезаних структура, опреме, извора струје, контролних система итд. Следећи типови инфраструктурних система су изузетно значајни током ванредне ситуације:

– јавне услуге (болнице, полицијске станице, ватрогасне станице, центри за снабдевање храном итд.),
– вода (извори воде и канализациона мрежа),
– саобраћај (путеви, пруге, аеродроми и луке),
– телекомуникације и
– извори енергије (струја, гас, бензин итд.).

У оквиру једног инфраструктурног система, нема свака структура или подсистем подједнаку важност за одржавање функционалности читавог система. Током катастрофе не мора сваки јавни сервис, тј. услуга да функционише у оном обиму као кад кад су у питању нормални услови: нпр. за одржавање система јавног здравља у току ванредних периода нема свака болница исту важност или подједнаке капацитете кад кад су у питању хитне или ванредне ситуације.

Физичка рањивост подразумева рањивост инфраструктурних елемената као што су путеви, зграде, пруге итд. Уколико је посебно рањива инфраструктура сконцентрисана на једном месту, то може значајно да утиче на степен оштећења у случају неког катастрофалног догађаја, било да су у питању последице природних хазарда или хазарда другог порекла. Ови догађаји могу имати различите потенцијалне утицаје на инфраструктуру, у зависности од врсте догађаја, његове локације, као и делова инфраструктуре који се налазе на том месту. (Bankoff, 2004: 26)

Значај ресурса критичне инфраструктуре за живот модерног човечанства је неоспоран. У измењеним околностима у највећем броју случајева долази до оштећења и застоја на инфраструктурним постројењима, што ремети устаљен начин снабдевања становништва, привреде и осталих корисника. С друге стране, застој у свакодневном функционисању инфраструктурних система може проузроковати ванредну ситуацију. Приоритет у овим околностима јесте спасити животе, али и нужност заштите критичне инфраструктуре.

Последице угрожавања и уништавања критичне инфраструктуре могу се огледати у следећем:

– губитак имовине и смртним исходима,
– прекид деловања значајних служби за производњу,
– губитак посла и основних средстава за живот,
– уништавање комуналне инфраструктуре,
– прекид уобичајеног начина живота и
– последице по животну средину; здравствене, социјалне и психолошке последице.

На питање *Зашто је заштита критичне инфраструктуре значајна и актуелна*, можемо одговорити следеће: екстремни ванредни догађаји су све учесталији, расте број потенцијалних облика угрожавања, пре свега, објекти критичне инфраструктуре су све повезанији, међузависни и рањиви. У отклањању последица ванредних ситуација, великих несрећа, као и терористичких напада, критична инфраструктура је кључни елемент на којем треба отклонити штету и оспособити га за функционисање, елемент који представља и инструмент за отклањање последица.

Критичне инфраструктуре имају виталан значај за 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 њих су терористички напади (ситуације кад једна особа или група људи намерно напада инфраструктуру из политичких или идеолошких разлога – напади на Светски трговински центар у САД 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 кад кад једна особа или организована група [нпр. бивши запослени у неком од инфраструктурних објеката, политички противници влада или група за заштиту животне средине] нападају критичну инфраструктуру и преузимају контролу над њом); информационо ратовање (приватни корисници – појединци (хакери) или читаве државе могу из различитих разлога да нападају информационе системе разних земаљам и доведу до великих проблема не само у функционисању информационе инфраструктуре, већ и 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., такав је био ураган Катрина).

Посебно је важна улога објеката критичне инфраструктуре у ванредним ситуацијама:

– производња и дистрибуција електричне енергије (хидроелектране, термоелектране, далеководи, трафостанице),

– производња и снабдевање енергентима (рафинерије, налазишта нафте, складишта гаса, нафтних деривата, магистарални нафтоводи и гасоводи),

– телекомуникације (преносни путеви, фиксна и мобилна телефонија, централе),

– производња и снабдевање питком водом (изворишта и фабрике воде, дистрибутивни центри),

– производња и снабдевање храном (погони за производњу хране),

– здравствена заштита (здравствене установе и објекти),

– материјална и културна добра (музеји, позоришта, културно-историјски споменици) и

– национални паркови.

Имајући у виду важност инфраструктуре једне државе, њену употребну вредност и значај за развој и унапређење сваке заједнице, као приоритетан задатак сваког друштва намеће се 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.

Ефекат, који би прекид рада инфраструктуре произвео на друштво, може бити директан и индиректан. Директна штета односи се на моменталне ефекте отказивања инфраструктуре и последице по становништво, економију, јавност и окружење. Процена штете врши се на основу три претпоставке: потпуног прекида функционисања инфраструктуре, непостојања противмера, непостојања сценарија. Прва претпоставка је да се инфраструктура суочава са потпуним прекидом функције или са тоталним уништењем. У стварности је ово скоро немогуће, али је, с друге стране, то једини добар начин да се утврди улога конкретне инфраструктуре у друштву.

Друга претпоставка је да процена треба да се обави без претходне примене мера заштите. У стварности је и то готово неизводљиво 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 немогућом.

Трећа претпоставка је да се процена значаја неке инфраструктуре за друштво треба радити без разматрања било каквог сценарија. Процена претњи и рањивости у пракси је углавном заснована на разматрању 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 у случају престанка рада инфраструктуре, односно процена апсолутног друштвеног значаја одређеног инфраструктурног сектора. (Lewis, 2006)

О значају критичне инфраструктуре (скр. КИ) говори и чињеница да су националне КИ, у данашње доба, у све већој мери повезане са КИ истог типа у другим државама. Ефекти великих кварова и отказивања инфраструктура у једној држави могу да се пренесу на суседне државе, па чак и на удаљеније. Стога, националне КИ представљају део јако комплексне међународне мреже. Због тога се Европска унија, током последњих пар година, озбиљно бави питањима прекограничних ефеката отказивања и кварова на КИ.

Улога КИ као и међузависност сектора свакодневно се повећава. Велики број истраживања указује на то да сектор енергетике и сектор информационих и телекомуникационих технологија имају најбитнију улогу међу КИ и да скоро сва остала КИ зависи од ових сектора. Зимерманова база података из 2004. године (Zimmerman, 2004: 23) о кроссекторским

инцидентима у САД за период од 1990. године до 2004. године показала је да неке КИ више и чешће утичу на функционисање других, него што друге утичу на њих. (Pereboom, 2001)

кад кад кад кад Витални друштвени сектори су међусобно повезани и зависе једни од других, што доводи до стварања рањивости. Ометање функционисања једног сектора може да утиче и на друге секторе и обрнуто (међузависност). Истраживања у овој области указују на то да међузависност сектора свакодневно расте и постаје хијерархијски структурирана и мултикатегоријска. Врсте међузависности су:

– физичка (повезаност инпута и аутпута, производ једне инфраструктуре неопходан је за функционисање друге),

– сајбер (стање једне инфраструктуре зависи од информација пренесених кроз информациону инфраструктуру),

– географска (један или више елемената инфраструктура су физички близу тако да догађај [нпр. пожар] ремети обе инфраструктуре) и

– логичка (реципрочни ефекти јављају се на две или више инфраструктура без физичке, сајбер или географске међузависности, уз финансијске губитке).

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 (Rinaldi, 2004):

– перцепција претњи, рањивости и ризика одговорних менаџера, власника и оператера инфраструктуре,

– предвиђена штета по друштво коју би изазвало отказивање инфраструктурног сектора,

– временски период који протекне од тренутка кад дође до престанка функционисања инфраструктуре до тренутка настанка ванредне ситуације,

– прекограничне последице престанка функционисања инфраструктуре,

– међузависност инфраструктурних сектора,

– критични објекти и географска област у којој су концетрисани,

– одговорност менаџера, власника и оператера инфраструктуре,

– власништво над инфраструктуром,

– законске основе,

– спроведене и планиране безбедносне мере.

Ови критеријуми су заправо најважније карактеристике критичних инфраструктура које треба анализирати. Подаци о њима представљају кључне улазне податке, за сваку државу, на основу којих се формира политика заштите критичне инфраструктуре у ванредним ситуацијама.

Република Србија има искуства са ванредним ситуацијама, пре свега са оним изазваним елементарним непогодама. Посебна пажња придаје се поплавама из 2014. године. Ова природна катастрофа је истакла неке слабе тачке које се тичу становништва у Републици Србији и у српске економије, и које, имајући у виду климатске промене, заслужују посебну пажњу и захтевају предузимање мера за смањење ризика од природних катастрофа. Побољшање, јачање и ширење система за одбрану од поплава, предвиђање поплава и превентивне активности, као и физичко планирање с циљем избегавања градње кућа и производних постројења у областима склоним поплавама, представљају неке од активности које је нужно предузети у скоријој будућности.

Оно што је кључно за смањивање ризика јесте поправка, реконструкција, проширење и унапређење инфраструктуре за одбрану од поплава, као и напредаке у области одлагања отпада у рударству и осталим производним активностима. Уз то, унапређивање система за предвиђање поплава је још један предуслов за смањење ризика од природних катастрофа, чему се може приступити на регионалном нивоу, кроз сарадњу са суседним земљама и стварањем економија обима.

Последице природних катастрофа имају директан и индиректан утицај на равнотежу природе. Поред непосредних последица по људе и материјалне штете, могу да проузрокују и посредне последице као што су глад, епидемије, социјални немири, економски слом итд., односно последице могу бити далеко теже уколико друштво није спремно на адекватан одговор приликом њиховог настанка.

Подаци о последицама поплавног таласа на путевима од 14. до 20. маја 2014. године:

– *мостови*: на категорисаним путевима срушено је око 30, а оштећено око 50 мостова; на општинским и некатегорисаним путевима срушено је или оштећено око 200 мостова;

– *путеви*: услед одрона или клизишта оштећени су категорисани путеви на више деоница; преко 20 категорисаних путева и више стотина општинских и некатегорисаних путева;

– *пруге*: бујица је однела део пруге у Тамнави (Уб), у дужини од око 10 км;

– *стамбени објекти*: срушено преко 200, оштећено више стотина, а неколико хиљада кућа је онеспособљено на угроженим подручјима;

– *јавни објекти*: преко 50 (највише основних школа);

– *пословни објекти*: преко 300 оштећених и онеспособљених објеката;

– *енергетски објекти*: поплавни талас умањио је поузданост система за пренос електричне енергије, посебно виталних објеката за пренос из термоелектране „Колубара" и термоелектране „Никола Тесла А" у Обреновцу („Службени гласник РС", бр. 52/14). (http://www.obnova.gov.rs/uploads/useruploads/Documents/Izvestaj-o-proceni-potreba-za-oporavak-i-obnovu-posledica-poplava.pdf)

Због претходно поменутих догађаја, Република Србија уложила је значајне напоре у стварању интегрисаног система заштите и спасавања, како би се на адекватан начин одговорило на угрожавање критичних националних ресурса. Полазну основу данас, свакако, представљају Закон о критичној инфраструктури и низ других стратегијских и подзаконских докумената који треба да се усвоје и који ће одговорити на питање шта у Републици Србији представља КИ, односно ко има надлежност над управљањем том КИ.

Национални програм управљања ризиком од елементарних непогода Влада је усвојила 19. децембра 2014. године. Програм је донет с циљем да се обезбеди општи оквир за израду свеобухватног програма заштите од елементарних непогода, као и за координацију, усмеравање фондова и спровођење активности везаних за смањење ризика, као и управљање истим.

Циљ Националног програма је изградња одговарајућег дугорочног система управљања ризицима од елементарних непогода у земљи, на коме би различите институције сарађивале и заједно радиле на смањењу ризика и ефикаснијем реаговању на непогоде, кроз креирање општег оквира за израду свеобухватног програма заштите од елементарних непогода, као и за координацију, усмеравање фондова и спровођење активности везаних за смањење ризика, као и управљање тим ризицима. (http://www.obnova.gov.rs/uploads/useruploads/Documents/Nacionalni%20program%20upravljanja%20rizikom%20od%20elementarnih%20nepogoda.pdf)

3.4. РИЗИЦИ И ПРЕТЊЕ КРИТИЧНОЈ ИНФРАСТРУКТУРИ

Циљеви система управљање ризиком су планирање, контрола и смањење ризика. Разноврсност и сложеност задатака који се јављају при настанку и развоју ризичног/ванредног догађаја, као и неопходност њиховог брзог решавања, захтевају декомпозицију система управљања на низ међусобно координисаних подсистема. (Trim, 2004) При томе, неопходно је обезбедити оптимално рашчлањавање, најчешће по фазама управљања, да би се испунили циљеви система. (Kash, Darling, 1998) Декомпозиција подразумева поделу управљања на планирање ризика (стратешко планирање) и смањивање ризика (оперативно управљање ризиком). Структура подсистема одређена је циљевима и критеријумима система и његовим

ограничењима, а значајан део обефазе управљања чине подаци о потенцијалним факторима ризика. Због тога имплементација система управљања захтева реализацију модула за евиденцију фактора ризика. (Yusko, Goldstein, 1997; Crichton, Flin, Rattray, 2000)

Процес управљања ризиком, везан за настанак ванредних ситуација, као специфичну манифестацију, обухвата следеће фазе: идентификацију опасности, анализу последица, процену ризика, планирање мера за превенцију ванредног стања или смањивање ризика, организовање мера приправности и одговора на настало стање и планирање мера санације насталих последица. (Савић, Анђелковић, Станковић, 2006)

Мере заштите критичне инфраструктуре подразумевају мере превенције, ублажавања и минимизације ефеката угрожавања; стога су кључне фазе превенције, ублажавање и припремљеност. (Мићовић, Никач, 2012: 199–211)

Једну од тешкоћа приликом покушаја класификације ризика представља чињеница да је број претњи које могу угрозити КИ готово неограничен, због чега их је веома тешко све предвидети. Другим речима, свакој класификацији може се 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 још увек не постоји јединствено решење ни на нивоу теорије. С 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.

Безбедносном претњом сматра се све оно што представља извор опасности и прети да нанесе озбиљну штету лицима, имовини, друштву или држави.

Идентификовање ризика подразумева процес проналажења, прописивања и карактерисања елемената ризика релевантних за циљеве управљања, односно процену ризика. Неопходно је препознати изворе ризика, догађаје или низ околности, као и њихове потенцијалне последице. Свеобухватна идентификација и регистровање ризика су суштински важни 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. (Papa, Shenoi, 2008, 3–17)

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. кад кад је извор ризика људски фактор, онда се говори о намерним и ненамерним ризицима. Ненамерни се везују за могућност настанка људске грешке настале услед умора, немара, непажње и сличних околности. Извор намерних ризика су криминалне радње и они се могу поделити на високофреквентне – некатастрофичне и нискофреквентне – катастрофичне ризике. У високофреквентне ризике убрајају се криминални догађаји или прекршаји чији се тренд испољава са одређеном дозом статистичке правилности, иако кумулативно могу довести до катастрофалних последица, што је случај са нискофреквентним ризицима (нпр. терористички напади).

С обзиром на то да су ризици и претње по КИ бројни, најважнији корак у стварању успешне стратегије унапређења безбедности и њихове заштите јесте идентификација и процена ризика у КИ.

Идентификовање ризика подразумева процес проналажења, прописивања и карактерисања елемената ризика релевантних за циљеве управљања, односно процену ризика. Неопходно је препознати изворе ризика, догађаје или низ околности, као и њихове потенцијалне последице. Свеобухватна идентификација и регистровање ризика је суштински важнос јер се ризик, који у овом стадијуму није идентификован, искључује из даље анализе. Иденти-

фикација би требало да укључи све ризике без обзира на то да ли су они контролисани или неконтролисани. (Кековић, Савић, Комазец, Милошевић, Јовановић, 2011)

Говорећи о ризицима везаним за КИ, треба поменути чиниоце који могу угрозити безбедно функционисање КИ и нормално обављање дужности оператера, као и власника КИ, социјалну климу и интерперсоналне односенеопходне за функционисање КИ, обезбеђеност објеката, техничких и информационо-комуникационих система и осталих средстава, и правила функционисања КИ. Такође, 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 што је пожељно узети у обзир субјективне доживљаје свих одговорних за нормално функционисање КИ у вези са степеном и врстом 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.

Могуће опасности и процена ризика од елементарних непогода и других несрећа разврставају се, у зависности од узрока настанка, на: сеизмичке, хидросферске, атмосферско-метеоролошке, биосферске и техничко-технолошке. Евидентирање карактеристика потенцијалних опасности врши се за сваку потенцијалну опасност посебно, а према могућим размерама:

1) Величина 1– минимална,
2) Величина 2– мала,
3) Величина 3– средња,
4) Величина 4– велика и
5) Величина 5– максимална опасност.

Након завршетка прелиминарне анализе потенцијалних опасности од елементарних непогода и других несрећа, анализира се ризик, а тај процес резултује детерминисањем нивоа ризика.

Ниво ризика добија се као производ степена вероватноће и степена последица и може бити у границама од минимално 1 до максимално 25.

Степеновање величине вероватноће које одговара степену вероватноће, врши се на следећи начин:

1– немогуће, 2– невероватно, 3– вероватно, 4– скоро извесно и 5– сигурно.

Степеновање последица које одговара размери последица, врши се према следећем:

1– минималне, 2– мале, 3– умерене, 4– озбиљне и 5– катастрофалне.

Ризик се, на основу одређеног нивоа, класификује у категорије од најниже (прва) до највише (пета), а потом одређује прихватљивост/неприхватљивост ризика. Прихватљиви ризици су ризици прве, друге и треће категорије, док су ризици четврте и пете категорије неприхватљиви. На основу листе прихватљивих и неприхватљивих ризика дефинише се листа приоритета за третирање.

3.4.1. Извори угрожавања критичне инфраструктуре

1) извори угрожавања објеката ризика по критичне инфраструктуре могу се класификовати на више начина. Према Лапорту могуће их је, с обзиром на порекло, сврстати у две категорије (Papa, Shenoi, 2008: 3—17): елементарне непогоде,

2) грешке унутар система инфраструктуре, које се могу даље, према пореклу узрока, поделити на оне изазване:

– људским фактором– лоше планирање активности у оквиру сектора, несмотреност оператера, неадекватна кооперација или координација активности и

– из техничко-технолошких разлог– отказивање машина, дефектност драјвера или грешка у софтверу који се користи у оквиру неког инфаструктурног сектора.

Напади на систем критичне инфраструктуре деле се на физичке (директни терористички напади и саботаже) и виртуелне (сајбер напади). Такође, у оквиру ове категорије могли би се као претња рачунати и могући ратни сукоби.

Угрожавање критичне инфраструктуре представља стални научни изазов и инспирацију за истраживаче широм света.

Према директности утицаја на безбедност, извори угрожавања деле се на: посредне и непосредне; кад је реч о активности на: латентне и активне; с обзиром на константност могу бити: стални и повремени; у зависности од времена настанка можемо их сврстати у: прошле, садашње или будуће. Свака од ових група извора угрожавања представља комплекс заснован на одређеном критеријуму класификације.

Један од највећих изазова будућности јесте глобално загревање које покреће низ питања као што су очување околине, храна, вода, енергија, здравство, пољопривреда, а св то утиче и на безбедност. Најпре желимо нагласити недостатак питке воде и хране који је у непосредном контакту са проблематиком глобализације. (Мићовић, Цветковић, 2015: 333–337)

Не само да су климатске промене проблем безбедности у будућности, већ представљају велики проблем садашњице јер могу да изазову сукобе око ресурса, економске штете и ризик за приобалне градове и кључну инфраструктуру, губитак територије и граничне спорове, миграције условљене погоршањем услова у окружењу (Цветковић, Вучић, Гачић, 2015: 184)

3.4.1.1. Природни облици угрожавања

Природне катастрофе све озбиљније угрожавају безбедност савременог човечанства. Последњих деценија запажа се тренд повећања броја природних катастрофа, али и њихове деструктивности, што за последицу има и повећане људске губитке, материјалну и нематеријалну штету. Уз то, угрожавањем критичне инфраструктуре онемогућава се или ограничава реализовање виталних државних функција (вршења власти, здравствене, просветне, енергетске, економске, социјалне и, уопштено, безбедносне функције), а то се додатно рефлектује на безбедност држава и грађана. Без обзира на технолошко напредовање, друштва су све угроженија. Јасно је да се ванредне ситуације и катастрофе и њихов утицај на људе и критичну инфраструктуру не могу спречити, али могу се унапредити механизми предвиђања и раног упозоравања на катастрофе, односно повећати отпорност и способност за бржу и ефикаснију ревитализацију угрожених вредности и добара.

Климатске промене су претња основним елементима живота људи у свету – приступу води, производњи хране, здрављу и коришћењу земљишта и окружења Човек је само део живота и животне средине ни изнад њих ни мимо њих. Предуслов опстанка човека, као и осталог живог света је везан за сунчеву светлост и топлоту, ваздух, воду, земљишни слој, флору и фауну. (Мићовић, Цветковић, 2014 : 319)

Последњих деценија људи се учесталије сређу са озбиљним директним и индиректним последицама природних катастрофа. У светском геопростору друштва су била суочена са последицама 25552 природне катастрофе, при чему је живот изгубило око 65 милиона људи, повређено је око 15 милиона, а погођено последицама око 13 милијарди људи. (Цветковић, Филиповић, 2017: 572–578)

Стратегија реаговања у насталој ванредној ситуацији зависиће од степена деструктивноси, врсте катастрофе, али и од врсте критичне инфраструктуре и конкретних угрожених добара и вредности.

Поплаве, земљотреси, олујни ветрови, клизишта, снежне падавине, град итд. представљају природне облике угрожавања који негативна дејства могу да испоље својом великом природном снагом.

Систем критичне инфраструктуре РС су могу угрозити и земљотреси (природни извори), чије је дејство испољено више пута и које је изазвало оштећења. Земљотрес — изненадно подрхтавање земљине коре — спада у ред најразорнијих геофизичких природних катастрофа. Сам удар земљотреса је изненадан, скоро да се дешава без упозорења, због чега га је немогуће предвидети. Услед њега долази до оштећења насеља, зграда, конструкција и инфраструктуре, нарочито мостова, надвожњака, железничких пруга, водних торњева, цевовода, објеката за производњу електричне енергије, те до дестабилизовања власти, економије и друштвене структуре земље. (Edward, 2005) Накнадни удари земљотреса могу да узрокују већа оштећења већ ослабљених конструкција. Секундарни ефекти подразумевају пожаре, пуцање брана и одроне који могу да блокирају копнене и водне путеве и да узрокују поплаве. Могу се оштетити објекти у којима се користе или производе опасне материје, што резултује цурењем хемикалија. Такође, може доћи до кварова објеката за комуникацију.

Последице земљотреса су разноврсне. Постоји велики број жртава због лошег пројектовања зграда и система критичне инфраструктуре. Од укупног броја лица која су погинула у земљотресима, њих 95% изгубило је живот приликом рушења зграда. (Murray, 2012) При томе, огромне су штете у области јавног здравственог система, транспорта, комуникација и снабдевања водом у погођеним подручјима.

Према резултатима статистичке анализе геопросторне и временске дистрибуције различитих природних катастрофа, може се са лакоћом закључити да да природне катастрофе сваким даном све више угрожавају људе и њихова добра (критичну инфраструктуру). Дешавају у/на различитим сферама земље (атмосфера, хидросфера, литосфера и биосфера) као поплаве, урагани, земљотреси, епидемије и др. Последице природних катастрофа по људе, околину, материјална добра (критичне инфраструктуре) могу бити примарне и секундарне. Нпр. примарне последице земљотреса су разни видови рушења објеката (КИ), док су секундарне последице повезане са изазивањем клизишта, цунамија, пожара. (Цветковић, 2014: 1283–1284)Тако је земљотрес који је задесио Краљево 3. 11. 2010. године озбиљно угрозио критичну инфраструктуру. Тог дана у граду није било грејања, а делимично и струје, вода се није препоручивала за пиће. Породилиште је било поплављено, у Клиничком центру „Студеница" нису радиле операционе сале, док су у продавницама попадали рафови и полице, па је снабдевање грађана било веома отежано. Услед потреса, мобилна телефонија у Краљеву била је у прекиду. У селу Витановац је, од укупно 850 домаћинстава, страдало око 70% објеката. У Матарушкој Бањи неколицина кућа била је оштећена и напукла. У Краљеву су улице биле прекривене комадима стакла, бетона и малтера што је онемогућило нормално одвијање саобраћаја. (Цветковић, 2015: 326)

3.4.1.2. Спољни облици угрожавања

Оружана агресија као спољни облик угрожавања безбедности земље па представља озбиљан облик угрожавања.

Оружана агресија, без обзира на циљ који агресор жели да постигне, директно је усмерена против слободе, независности, суверенитета и територијалне целокупности. Свака оружана агресија има освајачки карактер. (Гаћиновић, 2013: 188)

Обавештајно извиђачка делатност — може бити и унутрашњи и спољни облик угрожавања, а најчешће је комбинован. Изводи се с циљем прикупљања што више тачних података о: стању привредног друштва, намерама руководећег кадра, свим слабостима у систему привредног друштва, процедурама за деловање у различитим ситуацијама, стању опреме, запосленима, задовољству запослених, подели међу запосленима, документацији о технички-технолошком процесу делатности и сл. Остварује се посредством страних обавештајних служби или дипломатских, привредних представника, разних добротворних, мировних, хуманитарних и других организација, као форма сарадње са предузећем. Следећи начин свакако је и вербовање запослених за остварење тих циљева путем поткупљивања, уцењивања, условљавања, довођења пред свршен чин и сл. Имајући у виду веома разгранату мрежу оваквих служби, као и ниску безбедносну културу наших радника, процена је да су овакви видови деловања веома могући. Прибављање наведених информација, поред наведеног, може бити и насилним путем (проваљивање у просторе где се налазе информације, хаковањем и преузимањем података са рачунарске мреже) или разним врстама превара (лажно представљање, фалсификовање докумената и сл. јер су начини превара неисцрпни).

Диверзантско-терористичка дејства, најгрубљи облик субверзивне делатности против неке земље, представљају добро осмишљене и припремљене активности извођене тајно како би се нанели велики губици противничкој страни и остварили сопствени политички, војни или други циљеви. С обзиром на савремене карактеристике ДТД, као и на значај ППВ у систему водоснабдевања, он је могућа мета ових активности.

3.4.1.3. Унутрашњи облици угрожавања

Саботажа представља смишљену, прикривену делатност запослених појединаца или група с циљем изазивања материјалне штете привредном друштву.

Поред претходно поменутих, у последње време — време великих међупартијских, синдикалних и других подела, мотиви могу бити и политичке или синдикалне природе с циљем, условно речено, слабљења владајуће противничке групације.

Саботери делују прикривено како би остали неоткривени као извршиоци, и да би, кад се открије, узрок застоја кад кад био приписан претходно поменутим разлозима. Саботери могу бити радници на пословима где се саботажа догодила, али могу бити и други запослени или руководиоци који имају приступ тим местима. Саботаже су могуће и на другим деловима система. Управо овде долази до изражаја основна карактеристика саботаже (најбољи извршиоци саботаже су најбољи познаваоци система), тако да су начини извођења и облици остварења препуштени машти и знању извршиоца.

Диверзија је смишљена, прикривена и неочекивана акција појединаца, група или организација, државних органа или оружаних снага у миру или рату, који употребљавају експлозив ради убистава људи, наношења материјалне штете или постизања политичких и психолошких ефеката.

Криминалитет бисмо, као облик угрожавања, упркос различитим дефиницијама, могли окарактерисати као негативно друштвено понашање које се манифестује као укупност свих кривичних дела у посматраном временском периоду.

У структури савременог криминалитета све више места заузимају кривична дела организованог криминала транснационалног карактера. Због тешких економских и политичких последица, ова појава представља међународни проблем. (Ђукић, 2016: 129)

Извршиоци могу бити из свих структура запослених, чак и радници на руководећим функцијама који својим деловањем причињавају много већу штету предузећу, с обзиром на то да их је на та места поставило актуелно руководство.

Асоцијална — преступничка понашања изазивају негативну реакцију већине запослених, у супротности су са обичајним и моралним нормама понашања и нису санкционисана законом. Оваква понашања називају се још и социопатолошке појаве.Асоцијална понашања су посебно опасна јер могу бити узрок многих кривичних дела, акцидената, пропуста у раду, пожара и других опасности.

Објекти критичне инфраструктуре често су погодна мета напада терориста који на тај начин демонстрирају снагу и моћ своје организације, а слабост и немоћ власти. Врсте, облици, модус операнди и средства за извођење терористичких напада могу бити: атентати, бомбашки напади, диверзантски препади/краткотрајни оружани упади у стационарне и покретне објекте критичне инфраструктуре, отмице средстава јавног превоза/јавног транспорта, злонамерна изазивања хемијских или физичких експлозија, употреба оружја за масовно уништење и сл. (Кулишић, 2008)

Тероризам је све озбиљнија претња човеку, животној средини, правној држави, демократији, владавини права, међународном миру и стабилности. Стога је и јасан раст политичког приоритета решавања овог проблема: некадашњи проблем националне безбедности постао је предмет светске безбедности, а тиме и високе – светске политике, па и (оправданог и неоправданог) међународног интервенционизма. (Милашиновић, Мијалковић, 2011: 8)

3.5. РАЊИВОСТ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Критична инфраструктура, по својој природи, испољава карактеристике великих техничких система. Њена технологија и организација су веома комплексне и чврсто везане. Кључни елементи су расути географски, али су различито повезани у мреже и чворове, функционишу у реалном времену, што значи да није прихватљиво да дође до рањивости и прекида. Технолошка промена сама по себи може бити извор поремећаја великих комплексних система.

Неколико примера из блиске прошлости, укључујући нападе 11. септембра и др. указало је на недостатак планова за заштиту критичне инфраструктуре и подстакло на размишљање о безбедности критичне инфраструктуре. (Solano, 2010)

Рањивост је динамична, својствена одлика сваке заједнице (или домаћинства, регије, државе, инфраструктуре, неког другог елемента ризика) и садржи много компоненти. Степен до којег је утврђена рањивост одређује озбиљност догађаја. Рањивост указује на потенцијалну штету и променљива је која је усмерена унапред. У том смислу, рањивост се може описати и на следећи начин: „рањивост би требало да подразумева и предвидљивост као особину, заправо да предвиђа дешавања у оквиру одређене популације, у условима одређеног ризика и хазарда". (Adger, 2006: 268–281) Одредити рањивост значи поставити питање шта ће се десити ако одређени догађај/догађаји утиче/утичу на елементе који су изложени ризику.

Рањивост је унутрашња карактеристика заједнице, чак и у периоду између догађаја. Не појављује се и не нестаје како догађај дође и прође, већ је особина која је стална и дина-

мичка, испољава се у одређеној мери, у зависности од јачине штетног догађаја. Ово доводи до закључка да се рањивост може мерити само индиректно или ретроспективно, што подразумева да је настала штета тада главни показатељ рањивости (оно што се обично уочава након катастрофе није рањивост, већ причињена штета). Сагледавајући само насталу штету, без претходног сазнања о интензитету догађаја, недовољно је за извођење закључка о рањивости одређене заједнице или друштва. Веза између јачине догађаја и штете рефлектује рањивост елемента који је угрожен (заједница, домаћинство, инфраструктура...). Рањивост се, уопштено, може дефинисати као „степен до кога ће систем, подсистем или компонента система вероватно бити оштећена због своје изложености хазарду, притисцима или стресорима различитог порекла". (Harrington, 2005)

Кључни параметри у процени рањивости инфраструктуре су следећи:

– *уочљивост*: Колико је лако уочити рањивост?;

– *репродуктивност*: Колико је лако репродуковати напад?;

– *искористљивост*: Колико је процена рањивости сложен процес са становишта искоришћавања рањивости (непотврђен доказ концепта, функционалан или врло вероватан);

– *векторски приступ*: мерење рањивости за експлоатацију локалним или даљинским путем;

– *комплексни приступ*: мерење сложености напада ради искоришћења рањивости кад кад нападач има приступ циљном систему;

– *аутентификација*: Мора ли нападач да буде оверен у циљном систему, како би се искористила рањивост?;

– *ниво санације*: мерење нивоа доступног решења;

– *извештај*: мерење степена поверења — рањивост и кредибилитет извештаја (непотврђено, непоткрепљено и потврђено). (Baker, 2005)

Приликом процене угрожености критичне инфраструктуре могу се додати и други параметри:

– поверљивост, интегритет и доступност информација (утицај рањивости),

– осетљивост на кашњење,

– регулаторна ограничења која утичу на техничку подршку,

– уграђеност различитих безбедносних система и служби,

– непозната рањивост за специфичне уређаје,

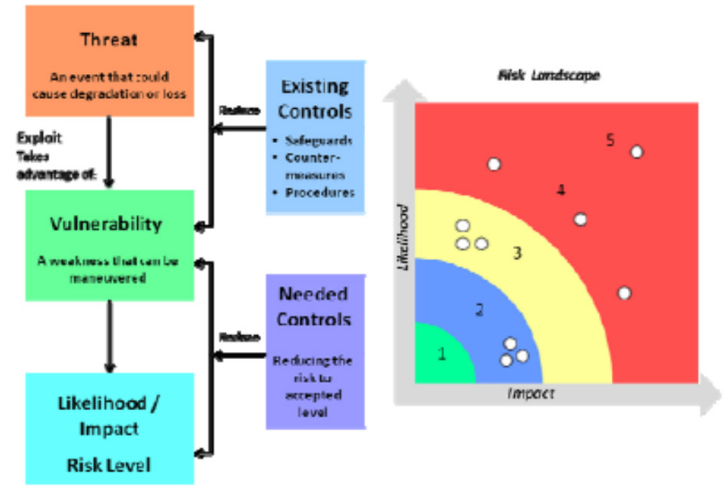
– сложеност различитих средства информационе технологије. (Tagarev, 2006: 16)

Осим тога, још један важан параметар представља фактор независности, зависности или узајамне зависности инфраструктуре. Ово, такође, утиче на вероватноћу и врсту каскадног и појачаног ефекта:

– у каскадном неуспеху, поремећај у једној инфраструктури изазива поремећај и друге инфраструктуре;

– у нарастајућем неуспеху, поремећај у једној инфраструктури погоршава другу инфраструктуру (на пример време за опоравак и обнову инфраструктуре повећава се због недоступности друге инфраструктуре);

– могућа је и дисфункција две или више инфраструктуре у исто време, која се јавља због заједничког узрока (природне катастрофе и сл.). (Roper, 1999)



Source: E. Adar, Task Force participant (2010).

Слика 4. *Један од приступа објашњењу рањивости инфраструктуре*

Предуслов за постојање ризика или јављање катастрофе је, поред хазарда и рањивости, изложеност. Изложеност (енг. 'exposure') подразумева број људи или других елемената под ризиком који могу бити погођени одређеним догађајем. Када су у питању ненасељена подручја, људска изложеност тада је једнака нули. Без обзира на то да ли ће ненасељено место погодити поплава, ураган или било који катастрофални догађај, људска изложеност, тиме и ризик од смртних случајева, биће једнака нули.

Док рањивост одређује озбиљност утицаја одређеног догађаја на елементе који су под ризиком, изложеност је компонента ризика од које зависи степен настале штете или повреде. Рањивост и отпорност су у директној вези са ризиком. (Egan, 2007)

3.5.1. Димензије рањивости

Као што је претходно напоменуто, анализа рањивости је изузетно сложена, управо због чињенице да је присутна у неколико облика. Четири основне димензије рањивости су:

– инфраструктурна (енг. 'physical vulnerability'),
– рањивост животне средине (енг. 'environmental vulnerability'),
– економска (енг. 'economic vulnerability') и
– социјална рањивост (енг. 'social vulnerability').

Поред ове поделе, у литератури се јављају и институционална и људска рањивост, али се и оне могу посматрати као део основних облика рањивости.

Рањивост се дефинише као степен губитка елемента у ризику, који је последица датог хазарда одређеног нивоа јачине. Потребно је разликовати рањивост целог инфраструктурног система и рањивост сваке од његових компоненти (линије услуга, структурни и контролни систем). Конвенционална процена рањивости концентрише се често искључиво на рањивости система (штети структурама система), али функционална рањивост скоро је подједнако важна. Функционална рањивост често је већа од структурне рањивости, што значи да оштећење функција претходи структурним оштећењима. (Brown, Carlyle, Salmer, Wood, 2005)

3.5.2. Жилавост и истрајност

Причињена штета не зависи само од хазарда, рањивости и изложености, већ и од истрајности и жилавости елемента изложеног ризику. Велики број дефиниција у литератури указује на то да постоје преклапања када су у питању наведени појмови, тј. веома је тешко раздвојити ове две димензије штетног догађаја.

Истрајност се може дефинисати као „начин на који људи или организације користе расположива средства како би се суочили са штетним последицама које би могле довести до катастрофе" (УН/ИСДР, 2004). У овом смислу, истрајност обухвата оне стратегије и мере које делују директно на штету, ублажавајући је, сузбијајући њене утицаје или пружајући ефикасну помоћ, као и стратегије прилагођавања које мењају понашање или активности како би се избегли штетни ефекти. Жилавост подразумева све наведено, али обухвата и способност одржавања функционалности током догађаја и опоравка. Сложено питање које произилази из овакве дефиниције је: да ли рањивост обухвата истрајност и жилавост или су ово потпуно раздвојени и супротни термини? Одговор на ово питање зависи од начина дефинисања незгоде или настале штета. Уколико је степен штете дефинисан и трајањем штетних утицаја и последицама по материјални статус, економију или свесност људи, тада рањивост мора да укључује и истрајност и жилавост. Овај закључак произилази из претпоставке да рањивост описује осетљивост на незгоду или штету.

Рањивост је функција осетљивости система (заједнице, домаћинства, инфраструктуре, нације итд.). Она је „независна од јачине (магнитуде) било ког одређеног природног догађаја, али зависи од контекста у коме се појављује". Рањивост не може бити процењена у апсолутном смислу: „особине урбаног места требало би да буду процењене са освртом на одређене просторне и временске скале". Из практичних разлога, анализа рањивости, сама по себи, ограничена је на известан сценарио, нпр. јачину догађаја који се анализира, што је обично одговарајући приступ процени рањивости, али је избор сценарија догађаја субјективан. (Rashed, Weks, 2003)

Комплексност рањивости не огледа се само у томе што је рањивост мултидимензионална компонента ризика, већ и у чињеници да су њени параметри географски условљени. Параметри који одређују рањивост различити су на нивоу домаћинства, заједнице и државе. Узимајући у обзир економску димензију рањивости, параметри као што су износ и разноврсност прихода сваког појединца су релевантни, док су, на нивоу државе, стопа инфлације и бруто домаћег производа изузетно битни.

Неки аутори наводе да је рањивост сувише комплексна и компликована да би се могла генерализовати као модел или оквир. Постоје следеће димензије рањивости: економска, демографска, политичка и психолошка. (Twigg, Bhatt, 1998)

Како би се боље разумео концепт рањивости, потребно га је разложити на такозване „компоненте ланца ризика" који чине:

а) сам ризик, или ризични догађај,

б) начини управљања ризиком или одговор на ризик и

в) исход.

Циљ декомпозиције рањивости управљање ризиком на правилан начин, у сваком од делова поменутог ланца.

Развој свести о рањивости почиње идејом ризика. Појам ризика одликује се познатом или непознатом вероватноћом простирања догађаја одређених магнитудом (она подразумева величину и ширење), фреквенцијом тј. учесталости, трајањем, као и историјом (сви аспекти рањивости на посматрани ризик). Важно је напоменути да друштвене активности могу да смање ризик и излагање ризику. (Ezell, 2007: 571–583)

3.6. ЖИВОТНИ ЦИКЛУС ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Заштита критичне инфраструктуре у ванредним ситуацијама може се посматрати као део јединственог процеса превенције и одговора на ванредну ситуацију. У том контексту, организација успоставља, примењује и одржава процедуре за идентификовање потенцијалних инцидената који могу негативно утицати на неку организацију, њене активности, функције, услуге, заинтересоване стране и окружење. Ове процедуре имају за циљ заштиту живота, имовине, спречавање прерастања инцидента у ванредну ситуацију или катастрофу, скраћивање времена прекида операција или активности организације, опоравак најважнијих активности организације, повратак на редовне активности и заштита угледа и репутације организације.

Развијене земље улажу пуно ресурса у истраживање могућности и моделе заштите. Заштита представља спремност, одбрану, умањење, одговор односно опоравак од поремећаја или уништења критичне инфраструктуре. То су активности власника, оператора, произвођача, корисника и регулаторних власти, с циљем очувања перформанси критичних инфраструктура. Методологија процеса заштите критичних инфраструктура може да садржи следеће елементе:

– прецизну идентификацију критичних инфраструктура и њихова дефиницију;

– утврђивање опасности које прете датим критичним инфраструктурама;

– анализу рањивости/осетљивости оних инфраструктура којима прети опасност, и то оних које доприносе прекиду у случају:

а) намерних напада;

б) природног или случајног догађаја;

– процену ризика од деградације или губитка критичне инфраструктуре и приоритизацију оних које су у опасности и рањиве;

– примену контрамера тамо где је ризик неприхватљив, како би се штитиле способности инфраструктура да ефикасно делују у хитним ситуацијама. (Ribeiro, Bezerra, Nakamura, 2005)

Процедуре су прилагођене потребама организација и односе се на: природу хазарда; карактеристике окружења и хазарда са потенцијалним утицајем на организацију; највероватнији тип и размеру инцидента; одговарајући метод за ублажавање и одговор на инцидент да би се спречило његово прерастање у ванредну ситуацију или катастрофу; процедуре командовања и контроле у ланцу командовања, оперативном центру и резервним локацијама, процедуре и овлашћење за проглашавање ванредне ситуације, иницирање процедура, активирање планова и активности, процену штете и одлуке везане за финансије; планове комуникације; процедуре за обезбеђење медицинске помоћи; активности с циљем умањења људских, материјалних и других губитака; заштиту виталних информација, информационих система; успостављање и евалуацију корективних мера после инцидента; периодична увежбавања одговора на инциденте; обуку персонала за управљање ванредним ситуацијама; листу и основне информације о кључном персоналу и агенцијама (службама) надлежним за пружање помоћи у ванредним ситуацијама (нпр. противпожарне јединице, службе медицинске помоћи, полицијске службе, комуналне службе; евакуационе руте са листама кључног персонала и контакт-детаљима); потенцијални утицај инцидента на критичну инфраструктуру; могућност за узајамну помоћ; процедуре за повратак на редовне активности са потребним временом и ресурсима. (Liscouski, 2004)

Карактеристике, бројност и последице ванредних ситуација на критичној инфраструктури захтевају од друштва и државе спремност у предузимању контрамера најпре за спречавање ванредних ситуација и, уколико је то могуће, елиминисање њихових последица.

Заштита критичне инфраструктуре подразумева стратегије, политике и спремност за спречавање напада, односно за одговарајући одговор, у случају да дође до напада. Заштита

критичних информационих инфраструктура представља програме и активности које реализују власници, корисници, оператери научно-истраживачке институције, владе, регулаторна тела, да би одржавали перформансе критичних информационих инфраструктура у случају отказа, напада или инцидената и како би умањили последице и време опоравка.

Политика заштите критичне инфраструктуре није ограничена искључиво на обезбеђивање непосредног и ефикасног одговора у случају прекида. Напротив, евидентно је постојање одређених фаза у циклусу заштите критичне инфраструктуре које комбинују поступке превенције и одговарајућег третмана. (Goetz, Shenoi, 2008) То значи да владе треба да креирају ефикасне политике у функцији превенције и раног упозоравања, откривања главних претњи, ризика и рањивости.

Уколико дође до одређених проблема у критичним инфраструктурама те мере би морале бити усмерене ка осигурању благовремене реакције и ефикасно управљање кризама. (Murray, 2012)

На основу досадашње праксе у САД идентификовано је шест главних фаза циклуса заштите критичне инфраструктуре; дешавају се пре, за време и после неког догађаја који могу угрозити или деградирати инфраструктуру. Ових шест фаза представљају оквир свеобухватног решења за инфраструктуру квалитета. Структуиране су на следећи начин:

– I фаза**:** анализа и процена **—** представља темељну активност и најважнија је фаза животног циклуса у заштити критичне инфраструктуре. Ова фаза идентификује имовину или функције критичне за успех мисије, одређује средства/функције слабе тачке, као и њихову међузависност, конфигурацију и специфичне карактеристике. Таква процена садржи анализиране утицаје везане за губитак или деградацију одређене инфраструктуре (нпр. постојање сајбер проактивне одбране оправдава очекивани напад на рачунарске мреже).

– II фаза**:** санација **(ремедијација) —** подразумева превентивне мере и радње које се предузимају пре него што дође до нежељених догађаја. Засноване су на фиксирању свих познатих сајбер опасности и физичке рањивости које могу довести до прекида функција. На пример, поступци ремедијације могу обухватити области образовања, оперативне процесе, процедуралне промене, конфигурације различитих система.

– III фаза**:** индикације и упозорења (пре и/или за време догађаја) **—** обухвата праћење процене способности осигурања имовине критичне инфраструктуре. Индикације представљају припремне радње које указују на то да ли је догађај вероватан или се планира његово дешавање. Индикације су засноване на улазним подацима тактичког, оперативног или стратегијског нивоа. На тактичком нивоу, улаз је везан за имовину власника, на оперативном нивоу за секторе критичне инфраструктуре, а на стратешком нивоу укључује све безбедносне аспекте.

3.7. ОСПОСОБЉАВАЊЕ ЛИЦА АНГАЖОВАНИХ НА ПОСЛОВИМА И ЗАДАЦИМА У СИСТЕМУ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

У циљу очувања, али и елиминисања нежељених последица урушавања критичне инфраструктуре насталих као резултат ванредне ситуације, неопходно је едуковати и оспособити особље којем ће ови послови и задаци бити приоритет.

Унутрашњу структуру организација одређених као критична инфраструктура чине ресурси који кроз процесе обављају виталне функције организације пре, за време и после ванредне ситуације. Основне ресурсе за управљање критичном инфраструктуром у ванредним ситуацијама чине (Брзаковић, 2009):

– људски ресурси,

– материјални ресурси,

– простор,
– ресурси знања и информација,
– инфраструктура (ИТ инфраструктура, саобраћај, енергетика итд.),
– финансијски ресурси и
– време.

Наведени ресурси пресудно утичу на успешно одговорање на изазове, ризике и претње по безбедност људи, материјална добра, простор, а тиме и на заштиту од свих видова ризика било ког облика ванредне ситуације. Да би употреба ресурса била оптимална и да би се избегла могућа „уска грла", потребно је обезбедити континуитет управљања ресурсима у свим фазама управљања ванредним ситуацијама.

Људски ресурси својим знањем, вештинама, идејама, визијама покрећу процесе и контролишу њихову реализацију. Људи у организацијама повезани су усвојеним одговорностима, овлашћењима и међусобним односима. Активности људских ресурса проистичу првенствено из прописаних обавеза и упутстава за поступање у одређеној ситуацији насталој и изазваној ванредном ситуацијом. Међутим, значајни део активности везан је, поред мотивације и свести о насталој ситуацији, стеченим знањем и вештинама итд.

Функционално управљање људским ресурсима треба да обједињује активности и задатке везане за људе, њихово обезбеђење, избор, образовање и друге активности осигуравања и развоја уз конкретне задатке. Улога људских ресурса у обезбеђењу потребног нивоа интероперабилности (организационе и семантичке) огледа се првенствено у нивоу оспособљености, квалитету попуне и планске и адекватне употребе:

Свеобухватна инвестициона политика и стратегија треба да поставе потребне стандарде и предвиде инвестиције за управљање ванредним ситуацијама узимајући у обзир природу захтева за реализацију активности у ванредним ситуацијама. Будући да се свака организација веома често суочава са рестрикцијама буџета, неопходно је успостављање реалних инвестиционих планова који ће омогућити обезбеђивање инфраструктуре и опреме на структуриран начин и у складу са успостављеним временским распоредом и динамиком реализације финансијских планова.

Људски ресурси располажу знањем неопходним за обављање радних активности и развој предузећа. Улагање у људске ресурсе, кроз реформу образовног система, примену концепта доживотног образовања и унапређење заштите здравља и безбедности на раду, уз постепено редуковање запослености у сивој економији, као кључни механизми побољшања квалитета и повећања продуктивности рада, треба да допринесу смањивању постојећег јаза између српског и европског тржишта рада. (Јаковљевић, 2010)

Приватизација, реструктурирање и модернизација привреде стварају нову привредну структуру у којој све већи значај трговине, саобраћаја, финансијских, интелектуалних, личних и других услуга. Прилагођавање овим далекосежним променама подразумева не само реформу образовања, већ и сталне програме преквалификација и додатне обуке радне снаге, посебно незапослених или лица са већим ризиком од уласка у статус незапослености.

Планирање и ангажовање људских ресурса, као и других потребних ресурса, јесте планска активност коју спроводе државни органи, с циљем адекватне заштите и спасавања људи, материјалних добара и осталих вредности.

Планирање људских ресурса јесте стратешка функција јер се плански обезбеђују људски ресурси путем кадровских решења, попуном служби обученим кадровима који су неопходни органима заштите и спасавања.

Управљање људским ресурсима одвија се у окружењу у којем се морају поштовати закони и прописи у условима ванредних ситуација. Развој менаџмента људским ресурсима односи се на процес образовања и развоја кадрова у сврху стицања знања и вештина потребних за рад на пословима организације и руковођења у ванредним ситуацијама.

Појмовима управљање, руковођење и менаџмент често се приписује исто значење, тј. сматрају се синонимима. Међутим, иако има сличности међу њима, они се разликују. Управљање је организацијска функција и процес. Функцију управљања у организацији обављају власници или њихови представници, а она се реализује доношењем управљачких одлука. Руковођење означава активност планирања, организовања, вођења и контроле. Руковођењем се налаже извршиоцима да изврше радне задатке, чиме се остварују предвиђени циљеви — пословни резултати у одређеном временском раздобљу. Менаџмент се појмовно одређује на три начина: означава процес максималне употребе расположивих ресурса; представља управу и надзорни одбор организације и означава менаџере — директоре организација који су одговорни за извршавање одређених задатака. Управљање људским ресурсима треба схватити као процес унутар ког свака појединачна активност и функција има важну улогу у изградњи успешне организације коју чини задовољан и ефикасан радник.

Руководилац јединице за интервенцију и спасавање мора да савлада низ основних знања, вештина и способности у области менаџмента персоналом. Иако се нека знања могу окарактерисати као теоретска, имају директну примену у вођењу јединице за интервенцију и спасавање. Такође, велики значај придаје се јакој лидерској позицији, вођењу примером, поштовању запослених, личним вођством, као и другим особинама и понашањем. Етички чиниоци су значајни јер утичу на правилно и успешно управљање људским ресурсима у јединицама за интервенцију и спасавање. Запослени у једној организацији могу радити самостално, у организованим групама (одељци, секције), у тимовима (двоје или више људи) или повремено, у специјалним тимовима за неки пројекат. Зато је неопходно створити окружење у коме запослени поштују једни друге.

ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ЕВРОПСКОЈ УНИЈИ И ДРУГИМ ДРЖАВАМА

4

Европска унија је један од кључних и доминантних фактора на међународном нивоу кад је у питању заштита критичне инфраструктуре. Покренула је низ иницијатива и истраживачких програма како би се проучили различити аспекти претњи и заштите, као и утицаји угрожавање и оштећење критичних инфраструктура има на образовање, привреду, здравство, комуникације и многе друге сегменте људске делатности. Терористички напади скренули су пажњу јавности на опасност од напада на Европске критичне инфраструктуре те је Европски савет затражио од Европске комисије да припреми целокупну стратегију и акциони план за побољшање заштите — „Европска критична инфраструктура (енг. „European Critical Infrastructure; ECI"). Као резултат овог захтева, Европска комисија предложила је оснивање „Европског програма за заштиту критичне инфраструктуре" (енг. „European Programme on Critical Infrastructure Protection; EPCIP". Програм чине три главна дела: „Директива за идентификацију и именовање; ЕЦИ", „Финансијски програм" и „Информационе мреже критичне инфраструктуре" (енг. „Critical Infrastructure Warning Information Network; CIWIN". (Koubatis, Schonberger, 2001)

Извештај Европске комисије о заштити критичне инфраструктуре у борби против тероризма дефинише критичну инфраструктуру, 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". (Critical infrastructure protection in the fightagainst terrorism, COM(2004)702 final: 3)

Након извештаја Комисије објављен је и „Зелени документ о европском програму заштите критичне инфраструктуре" (Green Paper on a European Program for Critical Infrastructure Protection — Green Paper on EPCIP). У овом документу наводи се дефиниција заштите критичне информационе инфраструктуре: „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 информационе инфраструктуре би требало да се посматра у контексту међусекторске повезаности с обзиром на то да прожима скоро све остале критичне секторе и требало би да координише заштитом свих осталих критичних инфраструктурних сектора. (Green Paper on a European Program for Critical Infrastructure Protection — Green Paper on EPCIP)

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

„Зелени документ о европском програму заштите критичне инфраструктуре" даје и преглед критичних инфраструктурних сектора. У критичне инфраструктуре се, према овом документу, убрајају:

– 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),

– 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) и

– истраживање свемира. (Green Paper on a European Program for Critical Infrastructure Protection — Green Paper on EPCIP)

У одлуци Савета за унутрашње послове и правосуђе (децембар 2005. године) од Европске комисије затражен је 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 помоћу 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 две или више земаља чланица, било три или више земаља чланица.

Директива Европског савета 2008/114/ЕС из 2008. године представља саставни део „ЕПЦИП програма" и дефинише критичну инфраструктуру, заједничке процедуре за идентификацију и означавање европске критичне инфраструктуре (скр. ЕКИ), заједнички приступ у процени потреба за побољшавање заштите, као и све ризичне приступе са приоритетом претње од тероризма.

Директива Европске Комисије 2008/114/ЕС основа је за наредне кораке у дефинисању критеријума за критичну инфраструктуру. У Анексу III истог документа наведене су процедуре које свака земља чланица треба да имплементира кроз неколико консеквентних корака.

Кад је донета ова Директива, она је представљала први корак у идентификацији и одређивању Европске критичне инфраструктуре и потребе да се унапреди њихова заштита. Наглашена је њена усмереност на сектор енергетике и транспорта, али и напоменуто да је треба размотрити са посебним освртом на процену међуутицаја сектора, између осталог, посебно

у односу на сектор информационих и комуникационих технологија. Прва ревизија Директиве почела је у јануару 2012. године.

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 (2008. година) Европског савета где се наводи да „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. У даљем процесу идентификовања инфраструктура које су критичне на нивоу ЕУ, јако је битан Члан 2(б) Директиве Европског савета који гласи: „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 националном оквиру, онда се она не сматра критичном на нивоу ЕУ. Државе, а са њима и власници и оператери критичних инфраструктура, учесници Европског програма заштите критичне инфраструктуре, имају обавезу да најпре поштују одредбе Директиве о заштити критичне инфраструктуре и европског програма, а затим још неколико захтева .

Директива Европског савета о идентификовању европске критичне инфраструктуре и неопходности заштитите критичне инфраструктуре из 2008. године (Council Directive 2008/114/ECof 8), прописује процедуру које се свака држава чланица мора придржавати, како би успешно идентификовала и заштитила критичну инфраструктуру. Према њој, свака држава чланица мора да идентификује потенцијалну критичну инфраструктуру у сектору енергетике и саобраћаја на основу дефинисаних критеријума критичности инфраструктуре из чланова 2(а) и 2(б) Директиве.[10]

Одређивање критичности сваког појединачног инфраструктурног сектора представља комплексан задатак. Комисија ЕУ предложила је три фактора која треба разматрати приликом идентификовања потенцијалних критичних инфраструктура у оквиру сваке земље чланице:

1) обим – губитак елемената критичне инфраструктуре изазива негативне последице, али не губитак сваког од елемената нити штету на инфраструктури; ррема величини географског простора на који губитак или оштећење неке инфраструктуре може утицати разликују се инфраструктуре са међународним, националним, покрајинским и локалним значајем;

2) интензитет – према степену у коме отказивање или уништење неке инфраструктуре може имати утицај на читаво друштво формира се 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 страдалих, број оболелих, број озбиљно повређених и 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 повезаности једне инфраструктуре са осталим инфраструктура-

10 Процедура идентификације је описана у члану 3 и Анексу III Директиве Савета ЕУ (2008/114/ЕС).

ма и у којој мери функционисање других инфраструктура зависи од исправног функционисања инфраструктуре чији се утицај разматра),

– политички утицај (зависи од способности и успешности владе једне земље у намери да се избори са проблемом отказивања или губитака неког инфраструктурног сегмента).

3) временски ефекат – односи се 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).

Директива је основа за даље кораке у дефинисању критеријума за КИ. У анексу III овог документа наведене су процедуре које земље чланице треба да имплементирају кроз четири консеквентна корака:

– I *корак*: свака земља чланица треба да примени секторске критеријуме како би извршила селекцију критичне инфраструктуре унутар једног сектора;

– II *корак*: свака земља чланица треба да примени дефиницију критичне инфраструктуре на потенцијалне европске критичне инфраструктуре идентификоване канон првог корака;

– III *корак*: свака земља чланица треба да примени прекогранични елемент дефиниције европске критичне инфраструктуре на потенцијалне европске критичне инфраструктуре које су прошле претходна два корака;

– IV *корак*: свака земља чланица треба да примени унакрсне, међусекторске критеријуме за преостале европске критичне инфраструктуре.

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 ванредним ситуацијама знатно се разликују у државама ЕУ. Из тих разлога Европска комисија, кроз „Европски програм за заштиту критичне инфрастуктуре", обезбеђује опште процедуре за идентификовање КИ. Предуслов за ефикасно управљање ванредним ситуацијама 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. (Prezelj, 2008: 16–34)

4.1. СТАЊЕ И ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ЗЕМЉАМА У ОКРУЖЕЊУ

4.1.1. Република Бугарска

Бугарска има одличан стратешко-географски положај јер представља мост између Европе и Азије.

Према Закону о кризном менаџменту у Бугарској се критична инфраструктура дефинише као „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 и функционисање државних институција".[11] Иако се објашњава појам критичне инфраструктуре, дефиниција не садржи конкретан критеријум на основу кога би се вршила евалуација критичности одређених инфраструктура. Сама дефиниција није довољна ни када се жели утврдити да ли се одређе-

11 Дефиниција је сачињена на основу документа који је издала Комисија ЕУ: Green Paper on a European programme for critical infrastructure protection (COM 576 final).

но добро, систем или служба могу третирати као критични. Бугарска је чланица Европске уније од 2007. године па мора да прати активности и регулативу ЕУ у области заштите критичне инфраструктуре.

Велики број објеката бугарсех критичне инфраструктуре екстремно је осетљив на природне катастрофе попут земљотреса, сурових временских услова, поплава, олуја и сл. Чак и кад је елиминисан физички утицај непогода, нагло повећање потребе за критичном инфраструктуром током криза може да доведе до нпр. нестанака струје (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 представљају малициозни програми и кодови (компјутерски вируси, црви, логичке бомбе, тројанци), чија је сврха 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.

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 (Engelbrekt, Förberg, 2005: 27–43):

1) идентификација главних сектора, подсектора и осталих елемената критичне инфраструктуре и утврђивање најкритичнијих међу њима (путем секторске анализе); ритичност 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 (Dunn, Mauer, 2006: 347):

– негативан утицај на јавност, тј. на становништво (број грађана који су угрожени отказивањем инфраструктуре — очекивани број погинулих, повређених, оболелих, евакуисаних људи),

– економски утицај (утицај који отказивање инфраструктуре има на БДП, други економски губици, деградација производа и службе),

– утицај на животну средину,

– 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),

– 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 нападну и способност процене намере нападача;

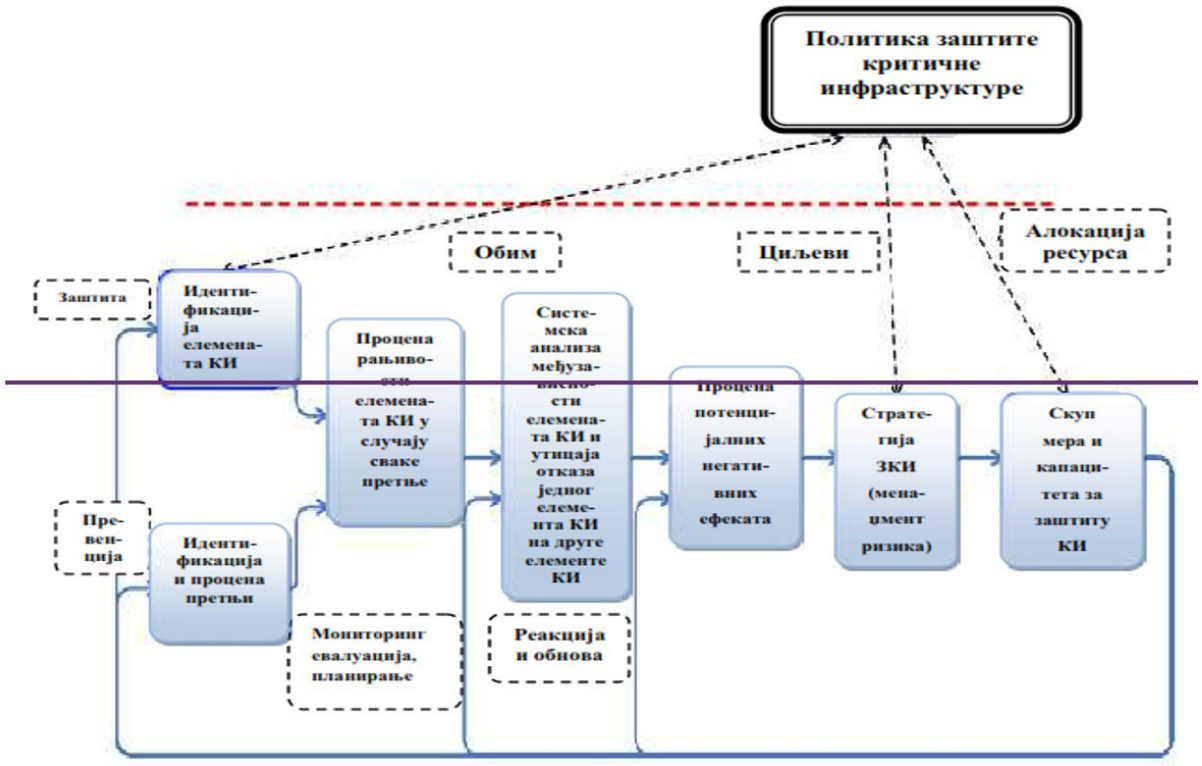
3) процена рањивости главних сектора критичне инфраструктуре у односу на специфичне претње; рањивост се може дефинисати као постојање слабости (осетљивих тачака), које могу бити изложене нападима, природним катастрофама и сл;

4) процена међузависности подсистема и инфраструктура, са фокусом на међузависностима које потенцијално доводе до домино ефекта или сличних отказивања критичних инфраструктурних сектора; међузависност и повезаност критичних инфраструктура су суштински значајне приликом доношења мера заштите критичне инфраструктуре, с обзиром на то да оштећење једног инфраструктурног сектора може да има ефекат на један или више других сектора (чак и да више оштети неке друге секторе, него нападнути сектор, тј. сектор који је први угрожен);

5) процена ризика (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, а њени резултати 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; циљ стратегије је ублажавање претњи по критичну инфраструктуру, смањење ризика и ублажавање евентуалних последица напада, природних катастрофа и непогода, људских грешака;

7) формулисање мера и капацитета за заштиту критичне инфраструктуре и смањење ризика у оквирима стратегије. (Engelbrekt, Förberg, 2005: 27–43)



Слика 5. *Приказ процеса заштите критичне инфраструктуре у Бугарској* (Tagarev, Pavlov, 2007: 42)

Формирање политике заштите критичне инфраструктуре (скр. ЗКИ) укључује одлуке о:
– обиму критичних инфраструктура,
– циљевима политике ЗКИ,
– мерама за идентификовање и приоритизовање критичних инфраструктура и
– алокацији ресурса за ЗКИ.

Процес заштите критичне инфраструктуре у Бугарској подразумева имплементацију седам корака приказаних на слици, као и повратну информацију о резултатима мера ЗКИ (представља интерактиван процес).

Оквири процеса планирања капацитета за ЗКИ морају да дефинишу и поставе баланс између четири кључне компоненте: циљева, стратегија, расподеле улога различитим државним и приватним организацијама и начина имплементирања стратегије и управљања ризицима. (Bartlett, Holman, Somes, 2004: 17–33) Термин 'капацитети за заштиту критичне инфраструктуре' се у бугарском Закону о кризном менаџменту дефинише као скуп ресурса којима се постиже мерљиви резултат у области ЗКИ и остварује одређени квалитет резултата. (Tagarev, 2006: 15–34) Сем четири главне компоненте за детаљније описивање процеса планирања ЗКИ неопходно је дефинисати скуп могућих сценарија, као и скуп задатака које треба обавити у случају реализације ових сценарија.

Заштита критичне информационе инфраструктуре (скр. КИИ) у Бугарској има три стратешка циља (Andreas, Metzger, Dunn, 2004):

– превенцију сајбер напада на критичне инфраструктуре,

– смањење националне рањивости на сајбер нападе,

– минимизирање штете и времена опоравка од сајбер напада.

Како би се постигли ови циљеви, неопходна је нова стратегија, која укључује следеће елементе:

– предузимање превентивних мера на свим нивоима,

– 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, потребно је дефинисање нових физичких, информационих и психолошких заштитних мера.

Спровођење мера заштите КИ на националном нивоу врши се кроз пет националних приоритета Бугарске у области заштите КИ, који се могу дефинисати на следећи начин (Andreas, Metzger, Dunn, 2004):

– 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 сајбер безбедности и о мерама за њено очување, као и формирање програма обуке у овој области,

– обезбеђивање система државне управе,

– јачање националне безбедности и међународне сарадње у области сајбер безбедности.

Проблеми са којима се Бугарска суочава на пољу заштите КИИ су недостатак:

– законских оквира (овај проблем веома успорава и отежава сваки судски процес везан за сајбер криминал),

– обученог особља,

– неопходних техничких алата за одговор на сајбер нападе,

– поузданих система за интеракцију са специјалним организацијама из других земаља,

– националних организација на државном нивоу које би се бавиле координацијом активности у области заштите КИИ,

– који се тиче националне стратегије, тачније непостојања одредби о усмеравању финансијских ресурса државе ка развоју организација које ће се бавити заштитом КИИ и координацијом активности на пољу заштите КИИ,

– националног акционог плана за повезивање националних фондова са међународним пројектима на регионалном нивоу, уз помоћ којег би се развијале организације чији би циљ био заштита КИИ и координација активности у области заштите КИИ.

Бугарска ради на развоју законских оквира којима би владине агенције биле овлашћене да читају електронску пошту, пресрећу бежичну комуникацију (позиве и интернет комуникацију), 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 хаковање је проглашено кривичним делом и уведен је појам сајбер тероризма.

Бугарска ради на неколико пројеката и унапређује заштиту своје КИИ:

– ради се на остварењу ефикасније сарадње између судских органа и специјалних служби за заштиту КИИ балканских и европских земаља и, уопштено, на развоју међународне сарадње,

– унапређују се националне стратегије за превенцију и борбу против сајбер криминала,

– ради се на развоју националне службе за борбу против сајбер криминала и међународну сарадњу приликом транснационалних сајбер инцидената,

– проширује се међународна сарадња у области правосудне помоћи у борби против сајбер криминала,

– доносе се специјални закони из области телекомуникација и компјутерских мрежа у складу са тренутним међународним стандардима и са Конвенцијом Европске комисије о сајбер криминалу. (Tagarev, 2007: 46)

Препорука бугарских стручњака у области заштите КИИ је да се оформи контакт служба у коју би се сливале све релевантне информације везане за заштиту КИИ и актуелне ванредне ситуације, а која би, након пријема, те информације прослеђивала свим релевантним службама. Тиме би се успоставила квалитетнија координација активности свих учесника у заштити КИИ, а као последица боље координације, олакшало би се идентификовање извора напада, као и формирање и спровођење решења за одбрану од напада или опоравак од сајбер напада.

4.1.2. Република Словенија

Република Словенија спада у млађе демократске државеу Европи. Године 2004. постала је чланица Европске уније.

На добре пословне резултате Словенаца утиче више фактора – од њихове пословичне марљивости, географског положаја (на раскршћу су трговачких путева), па до бриге за животну средину, мотивисаности и иновативности. Привреда је усмерена ка услужној делатности, а могу се похвалити врхунским услугама у области информационе технологије. Развијене су фармацеутска и аутомобилска индустрија. Такође, међу значајније привредне гране спадају прехрамбена индустрија, индустрија електричних апарата, металопрерађивачка и хемијска индустрија. Све значајнија привредна делатност постаје и туризам.

Република Словенија се, у појединим областима истраживања (компјутерске науке или нанотехнологије), сврстава у најуспешније државе на свету. Знање је један од главних стубова националног развоја, а истраживачка политика Републике Словеније спроводи се као у свим развијеним државама. Од 1991. године активно је укључена у програме истраживања и развоја Европске уније, као и у друге европске програме у тој области, а до сада је учествовала у више од хиљаду европских оквирних истраживачких програма.

Након стицања независности Република Словенија је успела релативно брзо да уђе у састав ЕУ чиме је обавезана да своје законске регулативе, на свим пољима, усклађује са европским , па и на пољу ЗКИ. Критична инфраструктура у Словенији је веома разноврсна и комплексна.

Године 2017. донет је Закон о критичној инфраструктури (Zakon o kritični infrastrukturi, št. 75/17) којим се дефинише и именује критична инфраструктура Републике Словеније, прописују начела ЗКИ, права и обавезе државних органа и организација у области информисања и извештавања о критичној инфраструктури.

У Републици Словенији 2006. године установљена је међуресорна група за усклађивање припрема за ЗКИ, у складу са одредбама Директиве 114/2008. Основни задаци ове групе били су:

– припрема и преглед организованости и нормативне уређености ЗКИ према појединачним активностима, тј. подсистемима националне безбедности;

– проучавање организације процедура, као и смерова развоја ЗКИ на узорку чланица НАТО и ЕУ;

– припрема оцене безбедносних околности, ризика и извора угрожавања државне инфраструктуре, уз то и оцена могућег опсега последица по становништво, економију и окружење;

– одређивање унифицираног означавања виталне инфраструктуре државе;

– обликовање предлога примерених мера и поступака за ЗКИ, узимајући у обзир усмерења и ставове НАТО и ЕУ;

– припрема предлога органа и организација који би требало да планирају мере за ЗКИ.

У складу са одредбама овог закона, наводи се да критична инфраструктура Републике Словеније обухвата објекте од виталног значаја за земљу који би, у случају прекида рада, узроковали озбиљне последице по националну безбедност, економију и друге кључне друштвене функције. Поред тога, дефинисан је однос између европских критичних инфраструктура и критичних инфраструктура Републике Словеније. У том контексту наводи се да је критична инфраструктура Републике Словеније и европска критична инфраструктура која егзистира на територији Републике Словеније, а заштита подлеже прописима који регулишу европску критичну инфраструктуру.

Такође, законом се захтева обавезна процена ризика рада критичне инфраструктуре, а Министарство одбране прописује упутства за процену ризика и координира активностима у области критичне инфраструктуре.

Надлежни органи и организације за имплементацију овог закона су: Влада Републике Словеније, Министарство одбране, носиоци најважнијих инфраструктурних сектора, државни органи који сарађују са носиоцима кључних инфраструктурних сектора у обављању својих задатака према овом закону, менаџерима за критичну инфраструктуру, Национални центар за управљање кризама и инспекторат одбране.

Одговорност за заштиту националних критичних инфраструктура сносе државе. Влада Републике Словеније као највиши државни орган регулише систем критичне инфраструктуре, док је Министарство одбране одговорно за стање у секторима критичне инфраструктуре и њихове заштите. Оператери су одговорни за обезбеђивање континуираног рада критичне инфраструктуре. Полазећи од принципа одговорности, као што је дефинисано Законом о критичној инфраструктури, оператери су дужни да обезбеде неопходан материјал и организационе услове за рад критичне инфраструктуре, која укључује обуку руководилаца и других запослених.

Сектори критичне инфраструктуре Републике Словеније су:

– сектор критичне инфраструктуре који обезбеђује енергетску подршку,

– сектор критичне инфраструктуре што пружа саобраћајне везе,

– сектор за критичне инфраструктуре — обезбеђивање хране,

– сектор критичне инфраструктуре који омогућава снабдевање питком водом,

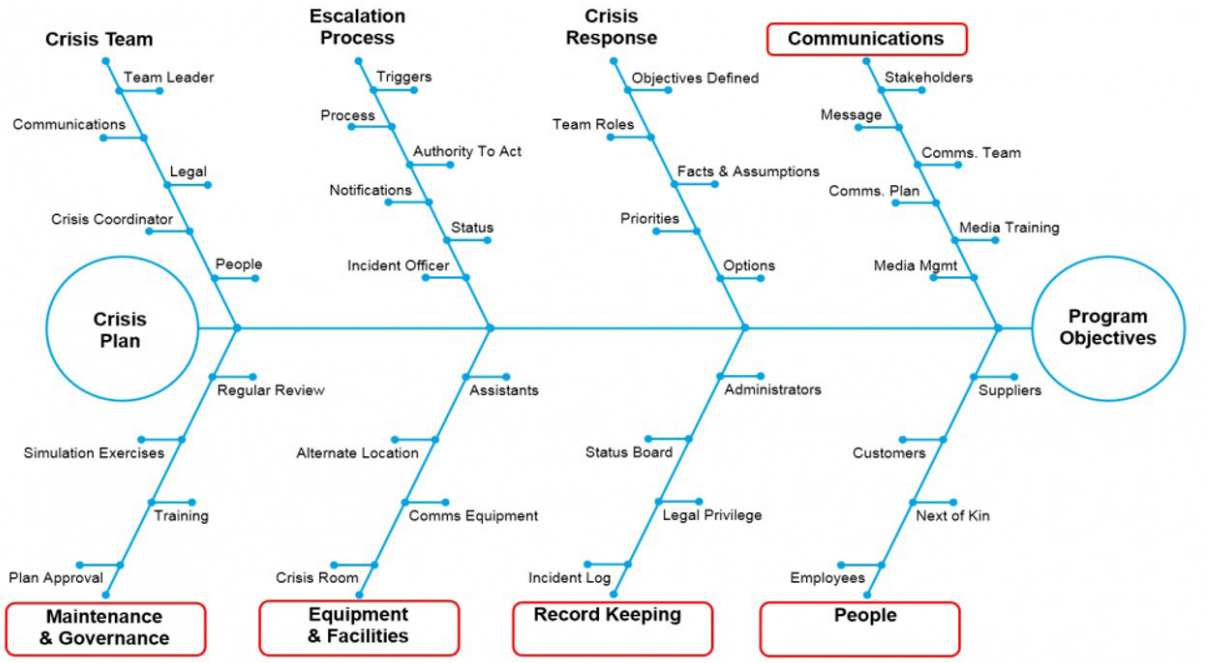
– сектор критичне инфраструктуре који пружа медицинску негу,

– сектор критичне инфраструктуре — обезбеђивање финансирања,

– сектор критичне инфраструктуре што осигурава заштиту животне средине,

– сектор критичне инфраструктуре који пружа информације и подршку комуникацији.(http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/javne_objave/2018/MORS_Zgibanka_kriticna_infrastruktura_v3_splet.pdf)

У Републици Словенији је успостављен национални центар за кризни менаџмент, који је приказан на слици 6.



Слика 6. *Национални центар за кризни менаџмент*

Одређивање приоритетних сектора који проистичу из међузависности и интеракције сектора критичне инфраструктуре (кварови у једном сектору могу имати значајан утицај на друге секторе). Према приоритетима деловања, директан утицај на другим критичним секторима инфраструктуре класификује се према следећем редоследу приоритета:

– снабдевање електричном енергијом,
– информације и комуникације подршка,
– снабдевање питком водом,
– снабдевање храном,
– пружање здравствене заштите,
– набавка нафтних деривата,
– железнички саобраћај,
– ваздушни саобраћај,
– речни саобраћај,
– снабдевање гасом,
– платни промет,
– обезбеђивање снабдевања готовином,
– функционисање државног буџета и
– заштита животне средине. (http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/javne_objave/2018/MORS_Zgibanka_kriticna_infrastruktura_v3_splet.pdf)

Географске области у којима су концентрисани критични објекти могу се разврстати у неколико категорија:

– критични објекти,
– критичне везе (повезаности),
– критична укрштања инфраструктура и

– критични процеси који се дешавају у критичним објектима или у њиховој близини. (Prezelj, Kustec Lipicer, 2010: 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 (представљају везе између материјалних инфраструктурних објеката, као што су аеродроми и луке). И поред тога што руте не представљају физичке објекте, општеприхваћен је 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 на територији Републике Словеније и, у већој мери, су смештени у урбаним срединама. Посебно су критичне мултиинфраструктурне области, тј. области у којима је лоциран већи број различитих типова инфраструктура (главни национални аеродром и национална лука). У оквиру главног националног аеродрома смештен је већи број инфраструктура — 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. (The Structure, Role and Mandate of Civil Protection in Disaster Risk Reduction for South Eastern Europe South, South Eastern Europe Disaster Risk Mitigation and Adaptation Programme: 24–35) Критична инфраструктура је највећим делом смештена у главном граду Љубљани. Република 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 индустрије. 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). (The Structure, Role and Mandate of Civil Protection in Disaster Risk Reduction for South Eastern Europe South, South Eastern Europe Disaster Risk Mitigation and Adaptation Programme: 24–35)

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 (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.

4.1.3. Република Хрватска

У Републици Хрватској су, током 2013. године, објављени следећи акти из области ЗКИ: Закон о критичним инфраструктурама („Народне новине", бр. 56/13), Правилник о методологији за израду анализе ризика пословања критичних инфраструктура („Народне новине", бр. 128/13) и Одлуку о одређивању сектора из којих средишња тела државне управе идентификују националне критичне инфраструктуре и листе редоследа сектора критичних инфраструктура („Народне новине", бр. 118/13).

Законом о критичним инфраструктурама (донет 28. 5. 2019. године) уређују се националне и европске критичне инфраструктуре, сектори националних критичних инфраструктура, управљање критичним инфраструктурама, израда анализе ризика и сигурносних планова власника, сигурносни координатор за критичну инфраструктуру, поступање са осетљивим и класификованим подацима, као и надзор спровођења Закона (Деканић, 2008).

Проглашењем Закона о критичним инфраструктурама Република Хрватска ускладила је своје законодавство са правном тековином Европске уније, садржаном у Директиви Већа 2008/114/ЕЦ из 2008. године, која се односи на идентификацију и одређивање европских критичних инфраструктура и процену потребе унапређења њихове заштите. (Таталовић, 2008)

Националне критичне инфраструктуре су, према поменутом закону, дефинисане као системи, мреже и објекти од националне важности, чији прекид деловања или прекид испоруке роба или услуга може имати озбиљне последице по националну сигурност, здравље, животе људи, имовину, околину, сигурност, економску стабилност и непрекидно функционисање власти. (Стратегија националне сигурности Републике Хрватске, „Народне Новине", бр. 32/2002)

Сектори националних критичних инфраструктура подељени су на следећи начин:

– енергетика (производња, укључујући акумулације, бране, пренос, складиштење, транспорт енергената и енергије и системи за дистрибуцију),

– комуникациона и информациона технологија (електронске комуникације, пренос података, информациони системи, пружање аудио и аудиовизуелних медијских услуга),

– промет (друмски, железнички, ваздушни, поморски и промет унутрашњим пловним путевима),

– здравство (здравствена заштита, производња, промет и надзор лекова),

– храна (производња и снабдевање храном и систем сигурности хране и робних залиха),

– финансије (банкарство, инвестиције, системи осигурања и плаћања),

– производња, складиштење и превоз опасних материја (хемијски, биолошки, радиолошки и нуклеарни материјали),

– јавне службе (осигурање јавног реда и мира, заштита и спашавање, хитна медицинска помоћ),

– национални споменици и друге вредности.

Осим наведених сектора, Влада Републике Хрватске може одлуком одредити и критичне инфраструктуре из других сектора. Анализом ризика утврђују се укупни ефекти прекида рада критичне инфраструктуре, а она се спроводи уз поштовање међусекторских и секторских мера.

Међусекторска мерила примењују се у анализи ризика свих критичних инфраструктура према следећем редоследу и укључују:

– људске губитке (могући број страдалих или озлеђених због прекида рада поједине критичне инфраструктуре),

– привредне губитке (процењују се с обзиром на значај привредног губитка и/или умањење квалитета производа или услуга),

– утицај на јавност (утицај на поверење јавности, телесне патње и ремећење свакодневног живота, укључујући и губитак основних и јавних услуга).

Ради успешне имплементације Закона о критичним инфраструктурама Републике Хрватске, успостављање Националног центра за критичне инфраструктуре (скр. НЦКИ) представља важан задатак Владе РХ, надлежног тела државне управе, девет ресорних министарстава, власника/оператора критичних инфраструктура и других заинтересованих страна. НЦКИ би имао јасно дефинисане задатке, надлежности и одговорности у спровођењу прописа из области критичних инфраструктура, координисање и побољшану сарадњу свих учесника и хоризонтално и вертикално. Што се устројства тиче, предлаже се избор једног од следећа два модела. Према првом, НЦКИ би се устројио као самостални сектор, служба унутар Сектора за цивилну заштиту или Службе за превентиву, планирање и аналитику у оквиру Сектора за цивилну заштиту. Други модел би успоставио НЦКИ устројио међусекторски као засебна агенција Владе РХ.

Што се његове функционалности тиче, НЦКИ би био задужен за: израду целовитог концепта ЗКИ, ревизију, хармонизацију и унапређење референтног легислативног оквира и надзор спровођења тог легислативног оквира. У неке од важних краткорочних активности НЦКИ спадају: израда секторских и међусекторских мерила за идентификовање степена критичности, дефинисање мера заштите које се морају примењивати у зависности од идентификовано разреду критичности; и (3) Спровођење поступка за идентификовањег нивоа критичности. Без обзира на будуће устројство, НЦКИ ће своје задатке испуњавати преко повереништва за заштиту критичне инфраструктуре (међуресорна радна група).

Чланови тог повереништва постали би већ именовани безбедносни координатори за критичну инфраструктуру. Основни задатак повереништва састојао би се у верификацији документације и поступака које је сачинила НЦКИ. Такав приступ раду подразумева да НЦКИ има мандат за ангажовање одговарајућих стручних институција и појединаца у сврху израде докумената и поступака везаних за успоставу система заштите критичне инфраструктуре. Рад повереништва не би захтевао нека значајна додатна средства.

Секторска мерила одређују надлежна средишња тела државне управе у сарадњи са регулаторним агенцијама и струковним удружењима за сваки појединисектор.

Средишња тела државне управе именују сигурносног координатора за критичну инфраструктуру и његовог заменика за сваки сектор критичне инфраструктуре из свог делокруга.

Власници/управници критичних инфраструктура дужни су поставити сигурносног координатора за критичну инфраструктуру који је у спровођењу заштите критичне инфраструктуре одговоран за комуникацију у сигурносним питањима између власника/управника и надлежног средишњег тела државне управе у чијем је делокругу критична инфраструктура, како би се осигурала заштита и континуитет рада критичне инфраструктуре. (Перинић, 2007: 47-66) На пример, овим законом дефинисана је новчана казна (од 500.000 до 1.000.000 куна) за власнике/управнике критичне инфраструктуре ако:

– не израде документацију везану за анализу ризика,

– не израде и не донесу сигурносни план власника/управника са мерема заштите и осигурања наставка пословања критичне инфраструктуре, испоруке услуга/робе,

– не одреде сигурносног координатора за критичну инфраструктуру.

За прекршај из првог става овог члана казниће се новчаном казном од 10.000 до 50.000 куна и одговорна особа власника/управника критичних инфраструктура. (Закон о критичним инфраструктурама Републике Хрватске)

ПОСТОЈЕЋИ СЕКТОРИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

5

Повољан природно-географски положај Србије представља компаративну предност за развој копненог, речног и ваздушног саобраћаја и омогућава привлачење транзитног саобраћаја. Србија се налази у средишту Балкана, на раскршћу главних саобраћајних коридора VII и X. Преко наше територије пружају се најкраће и најрационалније транзитне друмске и железничке везе од западне и средње Европе ка делу земаља јужне Европе и земљама Блиског и Далеког истока.

Нема сумње да је енергетика посебно значајна област за опстанак друштва и економије што је случај и са Републиком Србијом.

Можемо констатовати да су се, почетком друге деценије XXI века, привреда и друштво Републике Србије налазили у дубокој развојној кризи.

Енергетски потенцијал Републике Србије, 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. Енергетску привреду Републике Србије у најширем смислу чине:[12]

– *електроенергетски сектор* (електроенергетски извори — електране [термоелектране на лигнит, термоелектране на мазут и природни гас]; системи за пренос електричне енергије, са око 10.200 км далековода и трафостаницама, преко кога се преноси електрична енергија произведена у земљи и обавља размена са суседним системима; електродистрибутивни системи, лоцирани у потрошачким центрима преко којих се испоручује електрична енергија крајњим потрошачима);

– *сектор нафте* (експлоатација домаћих резерви нафте и природног гаса; увоз, транспорт и прерада сирове нафте и нафтних деривата; дистрибуција и продаја, али и извоз деривата нафте),

– *сектор природног гаса* (увоза и примарна прерада гаса из домаће производње, складиштење, транспорт и дистрибуција до крајњих потрошача; на главни магистрални гасовод, укупне дужине око 400 км, који се простире од границе Мађарске до Ниша, повезан је већи број дистрибутивних мрежа за снабдевање потрошача природним гасом; већина ових мрежа изграђена је на територији Војводине);

12 Егзактни подаци преузети су из Стратегије развоја енергетике Републике Србије до 2025. године са пројекцијама до 2030. године, „Службени гласник РС”, бр. 101/2015.

– *сектор угља* (експлоатација и прерада угља; експлоатација угља одвија се у рудницима са површинском експлоатацијом у три рударска басена — Колубарском[13], Костолачком[14],[15] и Косовско-Метохијском који тренутно не функционише у саставу енергетског система Србије; рудницима са подземном експлоатацијом — Вршка Чука, Ибарски рудници, Боговина, Соко, Јасеновац, Штаваљ, Лубница, Алексинац и Рембас; рудницима са подземном експлоатацијом (Ибарски рудници, рудници Рембас, Боговина, Соко, Штаваљ, Јасеновац, Алексинац, Лубница и Вршка Чука); преко 95 % укупне производње угља на површинским коповима користи се за производњу електричне енергије; за финалну потрошњу користи се угаљ из 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);*систем даљинског грејања* (системи градских топлана, који постојиеу 57 градова Србије и системи индустријске енергетике),

– *обновљиви извори енергије* о(употреба расположивог потенцијала природних ресурса за добијање примарне и финалне енергије; процењени технички искористив потенцијал обновљивих извора енергије износи 5,65 милиона тона еквивалентне нафте годишње, од чега потенцијал биомасе износи 63%, сунчеве енергије 17%, потенцијал малих водотокав (МХЕ) 10%, енергије ветра 5% и геотермалне енергије 5%),

– *сектор мазива* (производња, увоз и извоз мазивих уља и сродних производа; степен истражености територије Републике Србије неравномеран је, а производња сирове нафте и природног гаса остварује се само из Панонског басена; савремени концепт нафтно-геолошких истраживања усмерен је ка истраживању неструктурних замки терцијара, истраживању мезозојског комплекса, откривању лежишта у неструктурним замкама и колекторима нетрадиционалног типа у АП Војводини, као и ка откривањеувеликих антиклиналних замки у зонама судара регионалних тектонских структура и у близини могућих путева миграције угљоводоника на слабо истраженој територији уже Србије; тек након детаљних геолошких истраживања на подручју централне, источне и југоисточне Србије, моћи ће се, прецизније, говорити о евентуалним потенцијалима ове области са аспекта резерви нафте и гаса).

– *систем градских топлана* (у 45 градова Републике Србије, чине га децентрализовани топлотни извори и одговарајуће дистрибутивне мреже; користе се за загревање стамбеног и пословног простора, а обухватају 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 (ИКТ сектор) чине претежно мала и средња приватна предузећа којима су ИКТ доминантна делатност. Ту су информациони центри у великим привредним системима са израженом развојном функцијом у области информационо комуникационих технологија. У прошлости су велики информациони центри у великим системима били ослонац информатизације у Републици Србији. Касније, у процесу транзиције, створен је низ других малих и средњих приватних предузећа у тој области.

13 Колубарски басен налази се 60 км југозападно од Београда. Угаљ се откопава на коповима: Поље Б, Поље Д, Поље Е, Тамнава — Западно поље и Велики Црљени. У 2013. години на површинском коповима рударског басена Колубара ископано је 30,71 милиона тона лигнита. Доња топлотна моћ колубарског угља креће се у интервалу од 7500 до 9000 kJ/кг. У склопу прераде угља налази се и сушара. Пројектовани капацитет сушаре је 855 хиљада тона годишње. После процеса досушивања, угаљ се транспортује у бункер сушеног угља, а одатле у класирницу где се издваја по асортиманима. Године 2014. сушара је осушила 0,50 милиона тона лигнита.

14 Рударски басени Колубара и Костолац налазе се у саставу ЈП „Електропривреда Србије" (ЈП ЕПС).

15 У оквиру рударског басена Костолац, смештеном на око 50 км источно од Београда, активан је површински коп Дрмно где је, 2013. године, ископано 8,80 милиона тона лигнита у 2013. години. Доња топлотна моћ костолачког угља креће се у интервалу од 8800 до 11500 kJ/кг.

Битан елемент ИКТ сектора су и универзитети и институти, као и научно-истраживачки центри, технолошки паркови, инкубатори итд. који представљају спој универзитета и имплементације у привреди.

Упечатљив је податак да је број предузећа, претежно приватних, велики, што на неки начин оповргава уобичајено мишљење о стању ИКТ у Републици Србији. Потписан уговор о сарадњи са Мајкрософтом и низ договора са представницима компанија CISCO, IBM, HewlettPackard, 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. Такође, телекомуникације имају важну улогу у оквиру ИКТ сектора, као и сви сегменти, подгрупе у области телекомуникационих технологија.

Интересантна је регионална расподела ИКТ сектора у Републици Србији. Највећа концентрација ИКТ 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 Републици Србији — заступљен је са 13 %, а остали градови са 16 %. (Медаковић, 2007) Предности ИКТ сектора у Републици Србији су, пре свега, квалитетни кадровски ресурси, 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. Веома је значајна међународна конкурентност индустрије софтвера: ценовна и неценовна конкурентност, базирана на квалификованој радној снази.

С обзиром на то да у свету више не важи подела на Исток и Запад, него на дигитално развијене и неразвијене, односно на информациона друштва и она која то нису, Република Србија, по овом питању, не заостаје за светом. Развој и примена информационих технологија је у пуној експанзији и ефекти и сви елементи глобализације директно се осликавају и бивају потпомогнути применом информационо-телекомуникационих 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 стартап компанија. Оснивају се мала, флексибилна предузећа која могу да одговоре на захтеве једног фрагментираног и разноврсног тржишта. То је тржиште наменског софтвера и услуга што омогућава широк спектар могућности за рад малих фирми односно компанија. 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.

ИКТ тржиште у Републици Србији има тренд раста који се може поредити са било којом земљом у региону. Највећа очекивања су, по питању ИКТ тржишта, од е-Владе, е-локалне самоуправе и, уопштено, сектора Владе. Затим, ту су инфраструктурни привредни системи, јавна предузећа, успешни привредни системи, али и мала и средња предузећа оријентисана на савремене пословне моделе пословања.

Република Србија има развијен друмски, железнички, ваздушни и водни саобраћај. Саобраћај и транспорт у најширем смислу чине:

Друмски транспорт чини окосницу саобраћаја у Републици Србији. Најважније чвориште је Београд, потом Нови Сад и Ниш. Путна мрежа у Републици Србији обухвата јавне и некатегорисане путеве. (Стратегија развоја друмског, железничког, водног, ваздушног и интермодалног транспорта у Републици Србији 2008–2015)Друмски транспорт у Републици Србији представља динамичан и доминантан вид саобраћаја — око 80 % укупног количине превезеног терета, односно око 74 % укупног броја превезених путника. Привредни субјекти који обављају друмски транспорт и друштвена су својина, углавном су приватизо-

вани и функционишу у условима слободне конкуренције. Улога државних органа ограничена је на уређивање ове области у смислу издавања лиценци, дозвола за друмски превоз, надзор итд. Међународни друмски транспорт у Републици Србији или приступ међународном транспортном тржишту, већим делом обавља се 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.

Неуједначени развој саобраћаја потврђује чињеницу да су поједини његови видови прилагодљивији крупним променама у економији и производњи. Повољнији економски услови за привредне субјекте, флексибилност и способност да брзо одговоре на захтеве савремене економије омогућили су највеће учешће друмског транспорта на транспортном тржишту. Узимајући у обзир географски положај Републике Србије као транзитне земље, друмски транспорт, нарочито међународни, има важну улогу у економском развоју захваљујући константном расту.

Резултат компаративних предности друмског транспорта и повећања обима транзита преко територије Републике Србије биће даље повећање обима друмског транспорта. Изазови са којима се суочава друмски транспорт карактеришу већа очекивања корисника — квалитетнија услуга, временски губици на граничним прелазима и застоји у централним градским подручјима, високи трошкови и све већа конкуренција. Убрзан развој друмског транспорта може довести до загушења на главним правцима, у градовима и имати негативни утицај на животну средину и здравље становништва и смањења нивоа безбедности саобраћаја, тако да треба створити услове за преусмеравање на друге видове саобраћаја с циљем контроле прекомерног развоја друмског транспорта.

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. (Стратегија развоја друмског, железничког, водног, ваздушног и интермодалног транспорта у Републици Србији 2008–2015) Јавни превоз путника у градским подручјима значајно је фреквентнији у односу на ванградска. Око две трећине путовања обавља се средствима јавног градског 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 транспорт одвија се путем магистралне железничке пруге пролази кроз све веће градове и укршта се у зонама Београда и Ниша. Управљање јавном железничком инфраструктуром, јавни превоз путника и робе и одржавање железничких возних средстава су претежне делатности „Железнице Србије" а. д. Од укупне дужине железничке мреже у Републици Србији (3809 км), 1768 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 опада ка југу. Недовољно улагање у основно одржавање железнице 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 1000 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.

*Дирекција за железнице***,** као посебна организација, обавља послове државне управе у области железнице утврђене овим законом, као и законом којим се уређује безбедност и интероперабилност у железничком саобраћају. („Службени гласник РС", бр. 41/2018)Дирекција регулише тржиште железничких услуга, безбедност и интероперабилност железничког саобраћаја.

*Водни транспорт***.** Република Србија има повољне економске и географске карактеристике за теретни, путнички и туристички водни транспорт. Потенцијалирека 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 биће, према проценама, потребно око 290 милиона евра, а око 220 милиона евра потребно је за развој интермодалног транспорта.

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" основала је Република Србија, са компанијом Етихад из Уједињених Арапских Емирата, за обављање делатности превоза путника и робе.

Директорат цивилног ваздухопловства Републике Србије обавља послове који доприносе континуираном јачању безбедности ваздушног саобраћаја:

– доношење ваздухопловних прописа и првостепених управних аката,

– издавање јавних исправа (сертификата односно дозвола), и то:

• организацијама за обављање јавног авио-превоза и других делатности у ваздушном саобраћају; ваздухопловно-техничким организацијама за пројектовање, производњу, испитивања које претходе утврђивању типа, одржавања и обезбеђивања континуиране пловидбености ваздухоплова и других ваздухопловних производа, делова, уређаја и опреме,

• оператерима аеродрома, хелиодрома, летилишта, терена и пружаоцима услуга земаљског опслуживања; пружаоцима услуга у ваздушној пловидби (услуге у ваздушном саобраћају, услуге комуникације, навигације и надзора, ваздухопловно-метеоролошке услуге, услуге ваздухопловног информисања и услуге трагања за ваздухопловом и спасавања лица), пружају се услуге узбуњивања у склопу услуга контроле летења и информисања ваздухоплова у лету а не услуге трагања и спасавања,

• центрима за обуку ваздухопловног особља,

• здравственим установама прегледају ваздухопловно особље,

• организацијама које обављају преглед обезбеђивања на аеродрому,

• ваздухопловном особљу,

– обављање основне и периодичне провере (опита), ради утврђивања да ли објекат провере испуњава услове за обављање делатности или пружање услуга у ваздухопловству,

– инспекцијски надзор над спровођењем Закона о ваздушном саобраћају, подзаконских аката донетих на основу тог закона, међународних аката и прихваћених домаћих и међународних стандарда и препоручене праксе и Закона о основама облигационих и својинско-правних односа у ваздушном саобраћају у делу заштите права путника,

– сарадња с надлежним органима других држава,

– издавање потврда о пловидбености ваздухоплова и уверења о регистрацији ваздухоплова,

– учествује у припреми Националног програма безбедности у цивилном ваздухопловству,

– прописивање услова под којима се успоставља и користи Систем управљања безбедношћу,

– давање сагласности ваздухопловним субјектима за успостављање и коришћење Система управљања безбедношћу,

– давање сагласности ваздухопловним субјектима за безбедносну анализу за функционалне промене,

– спровођење Националног програм за обезбеђивање у ваздухопловству, Програма за контролу мера обезбеђивања у ваздухопловству и Програма обуке у области обезбеђивања у ваздухопловству и утврђује мере за заштиту ваздушног саобраћаја од незаконитих радњи,

– вођење јавних књига, регистра ваздухоплова и евиденције ваздухоплова, регистра аеродрома и регистра ваздухопловног особља;

– издавање дозвола за обављање редовног и ванредног јавног авио-превоза, дозвола за транспорт наоружања и војне опреме и опасних материја ваздушним путем;

– прописивање које се исправе и књиге морају налазити у ваздухоплову у току лета,

– издавање сагласности са условима за пројектовање и изградњу аеродрома, хелиодрома, летелишта и ваздухопловних објеката,

– организацију и управљање системом трагања за ваздухопловом и спасавање лица,

– управљање квалитетом,

– обуке у цивилном ваздухопловству. (http://www.cad.gov.rs)

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 (у Новом Саду, Београду, Панчеву и Прахову) за претовар контејнера. Код постојећих терминала присутна су значајна ограничења условљена тренутном 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.

Здравство је веома значајно, посебно током ратних конфликта, масовних миграција, политичке и економске нестабилности. Међутим, квалитет здравствене заштите, као и инфраструктуре везане за здравство у Републици Србији, постао је неадекватан. Здравствени систем у Републици Србији пати од недостатка средстава и инвестиција, али обезбеђује основну услугу грађанима.

Приватни здравствени сектор је развијен, постепено се инкорпорира у национални здравствени систем. Организацијом и управљањем здравственим системом у Републици Србији баве се три најзначајније институције: Министарство здравља, Институт за јавно здравље „Др Милан Јовановић Батут" и Републички завод за здравствено осигурање.

Министарство здравља Републике Србије:

– одређује здравствену политику,

– доноси стандарде за рад здравствене службе,

– одређује механизме контроле квалитета,

– контролише квалитет.

Такође, Министарство здравља је задужено за систем здравствене заштите, здравствено осигурање, очување и унапређење здравља грађана, здравствену инспекцију, надзор над радом здравствене службе и друге послове из области здравствене заштите.

Институт за јавно здравље Србије „Др Милан Јовановић Батут" надлежан је за:

– прикупљање података о здравственом стању грађана и раду здравствених установа,

– анализу прикупљених показатеља јавног здравља,

– предлоге мера за побољшање јавног здравља,

– предлог годишњег плана рада здравствених установа,

– развој и координацију здравствених информационих система.

Институт „Батут" је здравствена установа која обавља послове из области социјалне медицине, хигијене, епидемиологије и микробиологије. Такође, то је и стручно-методолошка и образовна институција која координира и прати стручни рад ЗЈЗ и других установа.

Републички завод за здравствено осигурање финансира функционисање здравствене заштите на свим нивоима, уговара пружање услуга са здравственим установама у јавном и приватном сектору, контролише спровођење обавеза преузетих приликом уговарања, дефинише основни пакет здравствених услуга. Републички завод је национална организација кроз коју грађани остварују своје право из здравственог осигурања и финансирају своју здравствену заштиту.

Неспорно је да се у данашње време рад бројних критичних инфраструктура заснива на информационо-комуникационим (ИКТ) системима и да нарушавање безбедности ових система може имати штетне последице. Критична информациона инфраструктура састоји се од комуникационих или информационих система чија је доступност, поузданост и отпорност суштински важна за функционисање модерне економије, безбедности и других важних друштвених вредности. Оваква инфраструктура све чешће је предмет напада.

Појам критичне инфраструктуре у правним актима Републике Србије помиње се у Стратегији развоја информационог друштва у Републици Србији до 2020. године, где је у оквиру тачке 6. 2. предвиђена заштита критичне инфраструктуре као један од стратешких циљева у области информационе безбедности. Констатовано је да је потребно развијати и унапређивати заштиту од напада применом информационих технологија на критичне инфраструктурне системе, поред ИКТ система то могу бити и други инфраструктурни системи којима се управља коришћењем ИКТ, попут електро-енергетског система. (Стратегија развоја информационог друштва у Републици Србији до 2020. године)

*Вода***.** Проблем заштите воде као критичног инфраструктурног сектора у Републици 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 Републици 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.[16]

Велики загађивач вода Републике 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.

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 очувању здраве воде, а веома ефикасан начин је и изградња површинских акумулација и малих брана

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. (http://www.economy.rs/finansije/9790/Poslovanje-finansijskih-institucija-u-Republici-Srbiji-2012-odine.html)

16 Податак са сајта ЈВП „Србијаводе".

Јавне службе. У контексту овог сектора већи део организација које обављају послове државне управе могао се 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.(Управно право РС) 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.

У највећем броју случајева јавне услуге не подразумевају производњу добара. Могу их пружати локални или национални монополи и то у областима у којима постоје природни монополи. Њихови резултати тешко се могу приписати одређеном индивидуалном напору и тешко их је оценити по квалитету. Обично подразумевају висок ниво обучености и образовања запослених.

Да би се са поузданошћу оформила листа критичних инфраструктура неопходно је да се, на основу једног од модела који је претходно описан 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.

5.1. ЕЛЕМЕНТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

Неоспорна је чињеница да у Републици Србији постоји свест о значају критичне инфраструктуре упркос местимичном навођењу и одређењу овог термина. Као земља која претендује да постане члан Европске Уније, пред Републиком Србијом је задатак да усвоји и примени Европску регулативу која се бави овом области и, користећи се већ развијеним препорукама, почне са развојем сопствене стратегије заштите целокупне критичне инфраструктуре. Званично, односно теоријски је та активност и реализована, а примена у пракси тек следи.

У Републици Србији, у складу са Одлуком о одређивању великих техничких система од значаја за одбрану („Службени гласник РС”, бр. 41 35, 86, 53), егзистирају следећи системи:

5.1.1. Акционарско друштво „Нафтна индустрија Србије”

Нафтна индустрија Србије бави се прерадом нафте и продајом нафтних деривата, експлоатише угљоводоник. На годишњем нивоу обим експлоатације износи око милион тона нафтног еквивалента.

НИС има рафинерије за прераду нафте у Панчеву и Новом Саду, укупног капацитета 7,3 милиона тона годишње. У саставу НИС-а налази се погон за производњу течног нафтног гаса у Елемиру.

Стратешки циљ компаније је регионално лидерство и његова реализација до 2020. године подразумева раст основних показатеља вредности компаније: увећање обима производње нафте и гаса до 5 милиона тона, завршетак пројекта модернизације прерађивачког комплекса у Рафинерији Панчево и повећање обима прераде до 5 милиона тона, повећање обима

продаје до 5 милиона тона, као и инвестиције у кључне правце бизниса до 2103. године у износу од 90 милијарди динара.

Подсећања ради, разарање постројења нафте у Новом Саду имало је размере еколошке катастрофе. Бомбардовање и разарање мостова, административних, стамбених и других објеката инфраструктуре у ванредним ситуацијама.

5.1.2. Јавно предузеће „Електропривреда Србије"

Јавно предузеће „Електропривреда Србије" (скр. ЈП „ЕПС") највећа је компанија у Србији, привредни и енергетски ослонац земље. Основне делатности ЈП „ЕПС" су производња, снабдевање и дистрибуција електричне енергије, као и трговина електричном енергијом. ЈП „ЕПС" је, у потпуности, посвећено остварењу своје мисије — снабдевање купаца електричном енергијом, под тржишно најповољнијим условима, уз стално подизање квалитета услуга, унапређење бриге о животној средини и увећање добробити заједнице у којој послује.

Делатност ЈП „ЕПС" је енергетска делатност: снабдевање електричном енергијом. Такође, ЈП „ЕПС" може, у складу са законом којим се уређује област енергетике, обављати и делатност јавног снабдевања електричном енергијом купаца на територији Републике Србије. Основна делатност ЈП „ЕПС" јесте:

– производња електричне енергије и производња електричне и топлотне енергије у комбинованом процесу,
– експлоатација лигнита,
– дистрибуција електричне енергије и управљање дистрибутивним системом.
– управљање економским субјектом,
– кабловске телекомуникације.

5.1.3. Акционарско друштво „Електромрежа Србије"

„Електромрежа Србије" (скр. „ЕМС АД")је оператор преносног система у Републици Србији и послује као акционарско друштво у државном власништву. Мисија овог друштва јесте сигуран и поуздан пренос електричне енергије, ефикасно управљање преносним системом повезаним са електроенергетским системима других земаља, оптималан и одржив развој преносног система у циљу задовољења потреба корисника и друштва у целини, обезбеђивање функционисања и развоја тржишта електричне енергије у Републици Србији и његово интегрисање у регионално и европско тржиште електричне енергије. „ЕМС АД" усвојило је десетогодишњи План развоја преносног система Републике Србије за период 2017—2026., са пројекцијама до 2031. године.

У складу са Стратегијом развоја енергетике Републике Србије, плановима развоја производног и дистрибутивног система Републике Србије, пословном стратегијом „ЕМС АД" као оператора преносног система Републике Србије, а на основу планираних улагања у унапређење и развој пословне активности, улагања у инфраструктуру за пренос електричне енергије усмерена су на следеће циљеве:

1) повећање поузданости преносног система и сигурности напајања потрошача, што је и законска обавеза „ЈП ЕМС";

2) повећање преносних капацитета/коридора (преко Републике Србије) који имају регионални и паневропски значај;

3) уравнотежен, одржив и благовремен развој преносног система с циљем прикључивања нових конвенционалних и обновљивих извора електричне енергије, објеката купаца и

4) развој тржишта електричне енергије на националном и регионалном нивоу.[17]

17 Подаци преузети са званичног сајта „ЕМС" а. д.

5.1.4. Јавно предузеће „Србијагас”

Јавно предузеће„Србијагас” обавља делатности од јавног значаја и општег интереса државе, основне обавезе су:

– сигурно снабдевање тржишта природним гасом,

– развој и безбедно функционисање транспортног, дистрибутивног и складишног система,

– развој могућности за успостављање нових праваца и извора снабдевања кроз повезивање са транспортним системима са земљама у окружењу,

– развој принципа рационалне и енергетски ефикасне примене природног гаса уз поштовање заштите животне средине и принципа одрживог развоја.

5.1.5. Јавно водопривредно предузеће „Србијаводе”

Делатност ЈВП „Србијаводе” од општег интереса утврђена Законом о водама је:

1) уређење водотока и заштита од штетног дејства вода:

– изградња, реконструкција, санација, одржавање и управљање регулационим и заштитним водним објектима у јавној својини и одржавање водотока,

– изградња, реконструкција, санација, одржавање и управљање водним објектима за одводњавање у јавној својини,

– изградња, реконструкција, санација, одржавање и управљање водним објектима за заштиту од ерозија и бујица у јавној својини и извођење радова и мера за заштиту од ерозије и бујица, у складу са законом,

– спровођење одбране од поплаве,

2) уређење и коришћење вода:

– израда биланса вода, контрола стања залиха водних ресурса и мере за обезбеђење њиховог рационалног коришћења и заштите,

– израда биланса подземних вода за појединачни ресурс, укључујући и расположиви ресурс, начин и динамику обнављања ресурса и мере за обезбеђење рационалног коришћења и заштиту ресурса,

– одржавање и управљање водним објектима за наводњавање у јавној својини,

3) заштита вода од загађивања:

– праћење хаваријских загађења, организација и контрола њиховог спровођења,

– уређење водног режима заштићених области из члана 110. овог закона и других подручја која на њих имају утицаја,

4) остали послови од општег интереса:

– израда и спровођење планских докумената, програма и нормативних аката,

– израда студија и извођење истражних радова за потребе интегралног управљања водама, израда техничке документације из области уређења водотока и заштите од штетног дејства вода, уређења и коришћења вода и заштите вода од загађивања,

– послови међународне сарадње у области вода,

– успостављање и вођење водне документације и водног информационог система,

– вршење поверених послова (припрема предлога водних јединица и њихових граница, плана управљања водама за водна подручја, посебног плана управљања водама за појединa питања управљања водама, плана управљања ризицима од поплава за водна подручја, оперативног плана за одбрану од поплава, израда карте угрожености и карте ризика од поплава, израда мишљења о оперативним плановима за одбрану од поплава за воде II реда, идентификација водних тела површинских и подземних вода која се користе или могу да се користе за људску потрошњу у будућности, вођење регистара заштићених области на водном подручју, вршење послова инвеститора у име Републике Србије, спровођење посту-

пака давања у закуп водног земљишта у јавној својини, издавање водних аката и вршење обрачуна и задужења обвезника плаћања накнада за воде).

Јавно водопривредно предузеће „Србијаводе" организовано је као јединствена пословна и економска целина. У оквиру предузећа је успостављена територијална и функционална организација, утврђена Статутом и Правилником о унутрашњој организацији и систематизацији послова. Унутрашњу организацију предузећа чине Дирекција, са седиштем у Београду, која координира и обједињује рад предузећа и три водопривредна центра (скр. ВПЦ). У Дирекцији предузећа и водопривредним центрима образоване су организационе јединице као сектори (Технички сектор, Сектор за економско-финансијске послове, Сектор за имовинско-правне и опште послове).

5.1.6. Јавно предузеће „Пошта Србије"

Статутом Јавног предузећа „Пошта Србије", уређују се: пословно име, седиште и правна форма Јавног предузећа „Пошта Србије", његова имовина, делатност, организација обављања делатности, органи, делокруг, одговорност и начин одлучивања органа, заступање, расподела добити, покриће губитака и сношење ризика, средства за обављање делатности, планирање рада и развоја, дужност чувања пословне тајне, заштита животне средине, јавност у раду, права, обавезе, одговорност и обавештавање запослених, обавезе запослених у случају штрајка, општа акта, као и друга питања значајна за рад, пословање и његов развој.

Претежну делатност ЈП „Пошта Србије" обавља на основу дозволе надлежног органа, односно Регулаторне агенције за електронске комуникације и поштанске услуге, у складу са законом који уређује област поштанских услуга. Делатност од општег интереса је универзална поштанска услуга, у смислу Закона о поштанским услугама („Службени гласник РС", бр. 18/05, 30/10 и 62/14). Поред претежне делатности, сагласно члану 13. Статута, „Пошта Србије", обавља: 1) поштанске активности комерцијалног сервиса које подразумевају посебне захтеве у погледу начина и квалитета преноса; 2) промет и дистрибуцију поштанских марака и вредносница, као и продаја марака у филателистичке сврхе; 3) монетарно посредовање, које обухвата делатност упутничког промета, платне и друге услуге и у оквиру финансијске делатности; 4) заступање и посредовање у осигурању; 5) телекомуникације (кабловске, бежичне, сателитске и остале телекомуникационе услуге), рачунарско програмирање, консултантске и сличне делатности, као и информационе услужне делатности повезане са телекомуникацијама; 6) поправке рачунара и периферне опреме; 7) брокерске послове с хартијама од вредности и берзанском робом који обухватају услуге мењачница; 8) штампање и издавање; 9) друмски превоз терета, укључујући све активности у вези с превозом терета друмом; 10) складиштење; 11) изнајмљивање властитих или изнајмљених некретнина и управљање њима; 12) истраживање и развој у природним и техничко-технолошким наукама; 13) делатност музеја, галерија и збирки; 14) друге делатности утврђене Статутом.

5.1.7. Јавно комунално предузеће „Београдски водовод и канализација"

Делатност водоснабдевања, одвођења и пречишћавања отпадних вода обавља око 100 јавних комуналних предузећа водовода и канализације у Републици Србији. Оснивачи ових предузећа су локалне самоуправе, које на основу Закона о комуналним делатностима, уређују њихове услове управљања, организације и пословања.

Сви ови системи су сложени, деценијама грађени и веома скупи. У њихово функционисање и развој се највише улагало 60-тих и 70-тих година прошлог века и многи од њих и данас раде са таквом превазиђеном технологијом и техником, инсталацијама, уређајима и

опремом. Након тог периода, много мање се улагало у одржавање постојећих и проширење и изградњу нових, углавном секундарних, уличних водовода и канализација, чему је допринела велика економска криза, крајем прошлог и почетком овог века.

Недостајала су улагања и модернизација технологија третмана пијаће и отпадних вода, реконструкција магистралне и колекторске водоводне и канализационе мреже, примена информатичких технологија у управљању техником, у пословању и односима са потрошачима. Ова огромна материјална улагања превазилазе могућности градова и општина као оснивача ових предузећа. Многи од система данас тешко излазе на крај са обезбеђењем неопходног квалитета услуга.

Цена воде није на тржишним основама, као у земљама транзиције и земљама у развоју; не обезбеђује ни просту репродукцију, а камоли средства за развој у складу с потребама и интересима садашњих и будућих потрошача. Њен садашњи ниво, у сиромашној земљи каква је наша, не подстиче потрошаче да се рационалније односе према потрошњи воде која није неисцрпан ресурс. Такође, такав однос према води доводи нас у ситуацију да улажемо велика средства у стално проширење капацитета, уместо да више пажње усмеримо ка систему управљања квалитетом производње, дистрибуције и другим услугама.

Између ових предузећа, која обављају исту делатност, раде у истим економско-социјалним условима и слично су организована, нема успостављене сарадње, нема размена информација, идеја, знања, метода и начина рада, коначно, нема ни заједничког наступа пред надлежним државним органима, организацијама и институцијама. То је нарочито значајно када се доносе кључна стратешка документа и закони, везани за ову област. Ово је значајно и због тога што је потребно на јединствени начин, на националном нивоу, постићи и придржавати се норми и стандарда које су, у области водовода и канализације, прописани регулативом ЕУ; те норме и стандарди допринеће ефикаснијем и квалитетнијем обављању ових делатности.

5.1.8. Јавно предузеће „Путеви Србије"

ЈП „Путеви Србије основано је сходно Закону о јавним путевима („Службени гласник РС", број 101/05) и обавља стручне послове који се односе на трајно, непрекидно и квалитетно одржавање и заштиту, експлоатацију, изградњу, реконструкцију, организацију и контролу наплате путарине, развој и управљање државним путевима I и II реда.

Путна мрежа је једна од највећих капиталних вредности у Републици Србији, на чијој територији има **16.221,125 км** државних путева I и II реда и њихова вредност се процењује на око 4,5 милијарде евра.

На државним путевима Републике Србије тренутно је евидентирано 2960 мостова (377 на ауто-путевима) укупне површине преко 1.000.000 м^2 чија је вредност око 900 милиона евра.

Република Србија на државним путевима има 14 великих мостова и то осам мостова преко реке Дунав и шест мостова преко реке Саве. Мостови су различите старости, најразличитијих облика и начина градње, од дрвета, камена, бетона, преднапрегнутог бетона, челика и различитих статичких система, распона и дужина од 5 до 2212 м, колико је дугачак мост преко реке Дунав код Бешке.

На државним путевима у Србији изграђено је 85 тунела, укупне дужине 14 километара. На ауто-путевима налази се шест тунела (два још увек нису пуштена у саобраћај). Тунели су различите старости, различите технологије градње у зависности од геолошких срединама у којима се налазе. Најдужи тунел је Шарган, на правцу од Кремне ка Вишеграду, дужине 775 м. Највећа концентрација ових објеката је на Ђердапској магистрали — 26. Укупно 39 путних тунела у Србији је дуже од 100 м.

Основни циљ ЈП „Путеви Србије" је спречавање пропадања путева, очување вредности мреже путева и њено побољшање, одржавање путева, улагања у изградњу, рехабилитацију, реконструкцију, као и израду студија и пројеката. Сва улагања су у складу са стратешким опредељењем Републике Србије у сектору друмског транспорта да се функционално интегрише у европску мрежу путева. ЈП „Путеви Србије" брине и о безбедности саобраћаја кроз отклањање опасних места, као и о заштити животне средине кроз елиминисање или смањење штетних утицаја путева и саобраћаја на животну средину, поштујући све прописане процедуре у складу са важећом законском регулативом.

Побољшање саобраћајних веза ЈП „Путеви Србије" постиже кроз квалитетно, ефикасно и равномерно повезивање привредних подручја, покрајина и региона Републике Србије, с акцентом на побољшању транспортних веза између развијених и мање развијених привредних подручја. Истовремено се ради на ефикаснијем повезивању Републике Србије са окружењем, пре свега са суседним земљама, повећањем протока саобраћаја отклањањем уских грла у пограничним зонама. Саобраћајна и економска валоризација географског, међународног и саобраћајног положаја Републике Србије у окружењу постиже се активним учешћем у интегративним процесима региона Западног Балкана, Југоисточне Европе и Дунавске регије. Истовремено, води се рачуна о укључивању у систем брзих саобраћајница европског значаја, намењених првенствено транзитном и туристичком саобраћају, пре свега на Коридору 10.

ЈП „Путеви Србије" тежи смањењу степена задужености и рационализацији трошења на свим нивоима. Веома су важни сарадња са међународним финансијским институцијама и повећање прихода по основу накнаде за употребу државног пута, изградњом и укључивањем свих новоизграђених деоница ауто-пута у систем наплате путарине. Такође, тежи се увођењу система наплате за све кориснике путног земљишта.

ЈП „Путеви Србије" настоји да побољша квалитет услуга које се пружају корисницима путева, као и унапређењу информисања, управљања квалитетом и контроле квалитета. Упошљавањем капацитета предузећа за путеве и грађевинских предузећа подстичу се укупни привредни токови.[18]

5.1.9. Јавно предузеће „Железнице Србије" а. д.

Српске железнице од 2015. године наставиле су да постоје као четири акционарска друштва: „Железнице Србије", Друштво за управљање железничком инфраструктуром „Инфраструктура железнице Србије", Друштво за железнички превоз робе „Србија карго" и Друштво за железнички превоз путника „Србија воз".

Делатности „Железница Србије а. д. су: инжењерске делатности и техничко саветовање, консултантске делатности у области информационе технологије и остале услуге информационе технологије, куповина и продаја властитих некретнина, као и изнајмљивање властитих или изнајмљених некретнина и управљање њима, рачуноводствени, књиговодствени и ревизорски послови, пореско саветовање, техничко испитивање и анализе, изнајмљивање и лизинг осталих машина, опреме материјалних добара, делатност музеја, галерија и збирки.[19]

Делатности „Инфраструктуре железница Србије" а. д. су услужне делатности у копненом саобраћају. Делатност обухвата управљање јавном железничком инфраструктуром, у делу одржавања јавне железничке инфраструктуре, организовања и регулисања железничког саобраћаја, обезбеђења приступа и коришћења јавне железничке инфраструктуре свим заинтересованим железничким превозницима, као и правним и физичким лицима која обављају превоз за сопствене потребе, као и заштита јавне железничке инфраструктуре.

18 Подаци преузети са званичног сајта ЈП „Путеви Србије".
19 Подаци преузети са званичног сајта „Железнице Србије" а. д.

Мисија овог Друштва јесте управљање јавном железничком инфраструктуром у Републици Србији, организовање и регулисање железничког саобраћаја, обезбеђење приступа и коришћења јавне железничке инфраструктуре свим заинтересованим железничким превозницима, као и правним и физичким лицима који обављају превоз за сопствене потребе, а који испуњавају прописане услове, изградња и реконструкција јавне железничке инфраструктуре, успостављање стандарда пословања, хармонизација са важећим стандардима и прописима у међународном железничком саобраћају, успостављање стандарда понашања запослених као и обезбеђивање рационализованог, компетентног и мотивисаног особља.

На основу дефинисане визије и мисије, као и започетог корпоративног реструктурирања железнице, одређени су основни циљеви Друштва:

– успостављање оптималне структуре пословања,
– повећање интерне ефикасности,
– оптимизација трошкова,
– спровођење активности у циљу успостављање принципа тржишног пословања,
– подизање квалитета инфраструктуре кроз реализацију плана инвестиција,
– повећање профитабилности.[20]

5.2. ПРЕДЛОГ КРИТИЧНИХ СЕКТОРА У РЕПУБЛИЦИ СРБИЈИ

Као земља која претендује да постане пуноправна чланица Европске уније, Република Србија има обавезу да усвоји и примени Европску регулативу из ове области и да уз већ прихваћене препорукама, почне са развојем сопствене стратегије заштите система критичне инфраструктуре.

Будући да у Републици Србији до пре само пар дана није постојао Закон о критичној инфраструктури и она није била јасно дефинисана предложен модел заснован је 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 Републици Србији.

Као што је већ речено, критична инфраструктура је релативно нов појам у Србији, будући да се као термин први пут помиње тек 2011. године у Уредби о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама („Службени гласник РС", бр. 8/2011). Наиме, чланом 8 истиче се процена критичне инфраструктуре са гледишта елементарних непогода и других већих несрећа, али не тумачи се дефиниција овог појма.

Приликом идентификације критичних инфраструктура и сектора критичних инфраструктура пожељно би било кренути од међународног, у најмању руку, од регионалног нивоа. Иако један број развијених земаља идентификује преко десет сектора (укључујући Републику Хрватску, која је идентификовала једанаест сектора) треба бити реалистичан и не правити превише детаљан попис објеката услед ограничености буџета и његовог оптималног коришћења. У наредном кораку, практично би било идентификовати КИ на различитим нивоима, осим регионалног и националног. КИ се могу идентификовати и на градском, локалном, па и на секторском нивоу. Прелиминарну идентификацију и класификацију КИ могуће је урадити и без важећих законских аката, уколико се дефинишу критеријуми и ресорне секторске анализе.

Издвајањем оних инфраструктура које се појављују у скоро свим земљама са дефинисаном политиком заштите критичне инфраструктуре добија се предлог ширег списка критич-

20 Подаци преузети са званичног сајта „Инфраструктура железнице Србије" а. д.

них инфраструктура и у Србији. Сектори у којима се врши идентификација и одређивање критичне инфраструктуре у складу са Законом о критичној инфраструктури јесу:

1) енергетика,
2) саобраћај,
3) снабдевање водом и храном,
4) здравство,
5) финансије,
6) телекомуникационе и информационе технологије,
7) заштита животне средине,
8) функционисање државних органа.

Критична инфраструктура може се одредити и у другим секторима, на предлог министарства надлежног за одређену област, у складу са овим законом. („Службени Гласник РС", бр. 87/2018-41.)

Различита министарства, сектори и ресори поседују засебне критеријуме и класификације објеката под њиховом ингеренцијом. Закон о одбрани („Службени гласник РС", бр. 116/2007, 88/2009 – др.закон, 104/2009 – др.закон. 10/2015 и 36/2018) дефинише објекте од посебног значаја за одбрану: велике техничко-технолошке системе, објекте у којима се производе, складиште предмети или врше одређене услуге, објекте у којима су смештени државни органи и правна лица, као и одређени инфраструктурни објекти од посебног значаја за одбрану земље.

Стога је могуће да се будући планови заштите критичних инфраструктура уврсте у планове одбране. Поред закона и планова одбране за будућу идентификацију и класификацију КИ у Србији релевантна су и следећа подзаконска акта:

– Одлука о објектима од посебног значаја за одбрану („Службени гласник РС", бр. 112/2008),

– Одлука о одређивању великих техничких система од значаја за одбрану („Службени гласник РС", бр. 41/2014 и 35/2015),

– Одлука о одређивању производа и услуга од посебног значаја за одбрану Републике Србије („Службени гласник РС", бр. 58/2008),

– Одлука о врстама инвестиционих објеката и просторних и урбанистичких планова значајних за одбрану земље („Службени гласник СРЈ", бр. 39/95).

– Закон о приватном обезбеђењу („Службени гласник РС", бр. 104/2013), у члановима 4 и 5 дефинише појам „обавезно обезбеђених објеката", као „објеката од стратешког значаја за Републику Србију и њене грађане, као и објеката од посебног значаја, чијим оштећењем или уништењем би могле наступити теже последице по живот или здравље људи или који су од интереса за одбрану земље". Такође, под обавезно обезбеђеним објектима подразумева се и простор на коме се они налазе, као и пратећи објекти. Поред ова два закона, други најважнији закони и стратешки документи којима се директно и индиректно штити КИ су: Национална стратегија заштите и спасавања у ванредним ситуацијама, („Службени гласник РС", бр. 86/2011), Закон о заштити животне средине („Службени гласник РС", бр. 135/2004, 36/2009, 36/2009 - др. закон, 72/2009 - др. закони 43/2011 — одлука УС), Закон о тајности података („Службени гласникРС", бр. 104/2009), Закон о планирању и изградњи („Службени гласник РС", бр. 72/2009), Закон о водама („Службени гласник РС", бр. 30/10, 93/12) и други релевантни документи.

Наведена документа, пре свега, помињу одбрамбену (наменску) индустрију Србије, али и друге индустријске и инфраструктурне објекте који за време ратног или ванредног стања, као и при мобилизацији Војске Србије првенствено врше услуге које утврди Министарство одбране.

Следећи поменуту добру праксу, Република Србија би свој систем заштите КИ могла да осмисли и примени у складу са досадашњим искуствима Словеније и Бугарске. Тим пре

што се Република Србија, исто као и Републике 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, с друге стране, не могу преузети и имплементирати у Републици Србији без одређених модификација, јер свака држава има своје специфичне особености. Објекти КИ асиметрично су дистрибуирани у оквиру Словеније - КИ у већој мери су смештене у урбаним срединама.

Посебно су критичне мултиинфраструктурне 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 Републици Србији су, пак, објекти критичне инфраструктуре равномерно дистрибуирани на целој територији државе. Да бисмо били сигурни на који садржај појма КИ се ослањамо и које су његове оквирне границе, потребно је било донети Закон о критичној инфраструктури, чиме се успоставио нормативни оквир за дефинисање, идентификацију, одређивање и заштиту националне и европске критичне инфраструктуре, али и подзаконских аката који ће обезбедити практична решења и критеријуме за идентификацију КИ. Доношење Закона о критичној инфраструктури обавеза је Републике Србије у процесу придруживања Европској унији, Акциони план о поглављу 24 за придруживање ЕУ. Овим законом уређује се идентификација и одређивање критичне инфраструктуре Републике Србије, принципи и планирање заштите критичне инфраструктуре, надлежност и одговорност органа, организација у области критичне инфраструктуре, информације, извештавање, пружање подршке одлучивању, заштита података, управљање и надзор у области КИ. Имајући у виду најбољу европску праксу, израђена је анализа стања (гап анализа). Последњих година, Република Србија улаже значајне напоре у стварање интегрисаног система заштите и спасавања који би адекватно одговорио у условима угрожавања, пре свега људских живота, али и критичних националних ресурса.

Такође, Упутством о методологији за израду процене угрожености и планова заштите и спасавања утврђују се критеријуми за процену десет сектора КИ са становишта њихове угрожености од елементарних непогода и других несрећа. Иако методологија садржи најсвеобухватнији приступ у заштити КИ у домаћем законодавству, он је оријентисан на идентификовање извора опасности и последица које поремећаји и прекид у функционисању инфраструктура имају по економију и екологију.

Приступ садржан у методологији не обухвата процену рањивости и отпорности КИ на све врсте претњи, као и мере повећања отпорности које треба да умање штетне последице елементарних и других несрећа на саме инфраструктуре, укључујући и ефекте међузависности.

Посебно се указује потреба да се развију модели и методе за подизање отпорности система КИ с циљем унапређења капацитета којима се амортизују ефекти претњи на штићене вредности. Због тога је потребно дефинисати критеријуме за идентификацију потенцијалних претњи, тј. опасности и генерисање опасности и међузависности прилагођених различитим секторима КИ у складу са међународним, европским и националним стандардима.

Треба напоменути и да је јачање јавно-приватног партнерства један од битних чинилаца процеса заштите критичне инфраструктуре. Закон о јавно-приватном партнерству и концесијама донет је 2011. године са изменама 2016. године. Према члану 7 овог Закона јавно-приватно партнерство (скр. ЈПП) означава дугорочну сарадњу јавног и приватног партнера ради обезбеђивања финансирања, изградње, реконструкције, управљања или одржавања инфраструктурних и других објеката од јавног значаја и пружања услуга од јавног значаја, које може бити уговорно или институционално.

Према Шкеру кораци које очекују Републику Србију у процесу придруживања Европској унији, а које Директива предвиђа, подразумевају:

– идентификовање националне и европске КИ,

– анализу ризика, односно разматрање могућих сценарија или претњи како би се оценила рањивост и могући учинак поремећаја у раду КИ или њеног уништења,

– успостављање система међусекторских мерила, као скупа општих мерила/правила на основу којих се процењује ризик за поједине системе и мреже КИ у свим секторима,

– успостављање система секторских мерила, као скупа специфичних мерила/правила на основу којих се процењује ризик за системе и мреже критичних инфраструктура у поједином сектору,

– дефинисање поверљивих података који се односе на националну и европску КИ, начин њихове размене са државама чланицама ЕУ и другим државама, као и систем њиховог пријема, експлоатације и архивирања,

– одређивање контакт тачке, која у име државе спроводи комуникацију и координацију са надлежним телима ЕУ и других држава, ради размене информација о КИ и спровођењу утврђених активности у њиховој заштити и осигурању непрекидног функционисања,

– одређивање сигурносног координатора за КИ – особу која је надлежна за питања у вези са заштитом КИ између власника/оператора и централних тела државне управе надлежних за поједини сектор КИ,

– успостављање плана сигурности власника/оператора који осигурава поверљивост, целовитост и расположивост организационих, кадровских, материјалних, информационо-комуникационих и других решења и сталних и степенованих безбедносних мера потребних за непрекидно функционисање КИ,

– уређивање поступања са осетљивим подацима који се односе на заштиту КИ. (Шкеро, Атељевић, 2015: 192–207)

НЕКА ИСТРАЖИВАЊА ВЕЗАНА ЗА СТАЊЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

6

Уопштено посматрајући, мисао везана за критичну инфраструктуру на подручју Републике Србије није још увек у довољној мери развијена у складу са потребама. Наравно, не сме се занемарити чињеница да и те како постоји добра воља и намера да се овој области посвети посебна пажња која се огледа у напору да се успостави адекватан систем КИ, што потврђују бројни академски доприноси области, али и велики број конференција и радионица на ту тему као и захтевна истраживања. Треба напоменути да је Факултет безбедности Универзитета у Београду као референтна институција из ове области учествовао у реализацији активности на пројекту „Resilience of Critical Infrastructure Protectionin Europe" (скр. RECIPE). Координатор пројекта који је трајао од јануара 2015. до јуна 2016. године била је Државна управа за заштиту и спашавање (скр. ДУЗС) из Републике Хрватске, док су партнери у пројекту били Факултет безбедности Универзитета у Београду, Велеучилиште Велика Горица (скр. ВВГ), Република Хрватска и Шведска агенција за ванредне ситуације (енг. Swedish Civil Contingencies Agency).

С обзиром на то да критична ифраструктура чини саставни део система развоја друштва, циљ пројекта огледа се у оснаживању отпорности система заштите КИ на националном и европском нивоу побољшањем начина управљања и заштите КИ.

Кроз заједничке радионице, међународне конференције омогућена је размена мишљења, искустава, потешкоћа и тиме су се створиле смернице за боље и ефикасније управљањем КИ. Не постоји јединствено упутство за успостављање система КИ што не искључује сагледавање модела, нпр. у земљама у окружењу и могућност прилагођавања уз одговарајуће модификације и корекције нашем систему.

Такође, простор за нова истраживања постоји који би омогућио и помогао да се створи јасна слика и идентификује КИ у Републици Србији.

Занимљива је чињеница да су поједни резултати истраживања које су организовале и реализовале колеге са Факултета безбедности Универзитета у Београду за потребе РЕЦИПЕ (Отпорност заштите критичне инфраструктуре у Европи) пројекта готово идентични као и подаци које је аутор спознао добио након обраде анкете у свом истраживању.

У оквиру међународног пројекта обухваћена је земља учесница у пројекту (Србија) и три суседне земље региона (Босна и Херцеговина, Црна Гора и Македонија). Циљ истраживања био је да се идентификују нормативно-правни аспекти организације заштите КИ и најзначајнији практични проблеми у овој области. Истраживањем су обухваћене релевантне установе и испитаници су одговарали на питања сврстана у неколико целина почев од законодавства и праксе заштите КИ у РС, процене рањивости и идентификације ризика и претњи КИ у РС, преко анализе међузависности КИ у РС, успостављања и унапређења сарадње између националних субјеката па до предлога модела ефикасне размене знања и искуства између субјеката.

Резултати овог истраживања веома значајни за даља истраживања, унапређења и побољшања у овој области у РС. Закључено је да:

– не постоји политика заштита КИ,

– наша домаћа регулатива није усклађена са правилима ЕУ,

– није идентификована КИ,

– не постоји тело за координацију активности спровођења политика заштите националне КИ,

– нису идентификовани ризици и претње КИ,

– није урађена анализа рањивости.[21]

Посебно треба пажњу обратити на угроженост објеката КИ у следећим областима:

– производња и дистрибуција електричне енергије (хидро и термо електране, далеководи, трафостанице),

– производња и снабдевање енергентима (рафинерије, налазишта нафте, складишта гаса, нафтних деривата, магистарални нафтоводи и гасоводи),

– телекомуникације (преносни путеви, фиксна и мобилна телефонија, централе),

– производња и снабдевање питком водом (изворишта и фабрике воде, дистрибутивни центри,

– производња и снабдевање храном (погони за производњу хране),

– здравствена заштита (здравствене установе и објекти),

– материјална и културна добра (музеји, позоришта, културно-историјски споменици) и

– национални паркови.[22]

Свеукупни очекивани резултати пројекта су:

– континуирана и свеобухватна размена знања и искустава кроз активну промоцију примера добре праксе између земаља,

– унапређење знања, ставова и понашања у односу на ризике који прете КИ,

– широка база знања о превенцији катастрофалних догађаја,

– унапређена комуникација између националне и међународних страна,

– обезбеђивање узајамне подршке и развијање нових механизама сарадње свих релевантних партнера из јавног и приватног сектора,

– омогућавање бољих услова за подршку научној и истраживачкој активности у подручју управљања ризицима КИ,

– смернице за успостављање оптималног система управљања ризиком КИ у државама партнерима,

– смернице стављене на располагање Европској комисији за даљу дисеминацију и употребу,

– повећана отпорност и ниво заштите европских КИ као резултат побољшане координације и сарадње учесника,

– успостављена методологија процене заштите система на темељу системског приступа,

– дефинисана дугорочна стратегија о управљању КИ у обухваћеним државама,

– утврђене и дефинисане потребе за даљим образовањем и обуком јавног и приватног сектора (образовни програми, размена стручњака).[23]

Резултати до којих је ауторка монографије дошла спровевши истраживање имају готово идентичне закључке по питању извесних недостатака и мањкавости у области КИ у Републици Србији.

Занимљива је чињеница да су анкетирана лица са дугогодишњим радним искуством чији је радни ангажман директно у вези са КИ која је тема истраживања. У истраживању је учествовало 94 испитаника, 64 мушкарца и 30 жена. (Мићовић, 2016)

21 Ово су званични подаци истраживања у оквиру РЕЦИПЕ пројекта, анализу резултата анкете на панел-дискусији представила је проф. др Јасмина Гачић, ванредни професор на Факултету безбедности, Универзитета у Београду.

22 Исто.

23 Предлог националних становишта - Resilience of Critical Infrastructure Protection in Europe (RECIPE), 2015.

Табела 3. *Радно ангажовање на пословима заштите и спасавања*

Р. бр.	Број година	Број лица	Проценат (%)
1.	до 5 година	28	29,8
2.	од 5 до 10 година	6	6,3
3.	од 10 до 20 година	31	32,9
4.	од 20 до 30 година	20	21,4
5.	више од 30 година	9	9,6

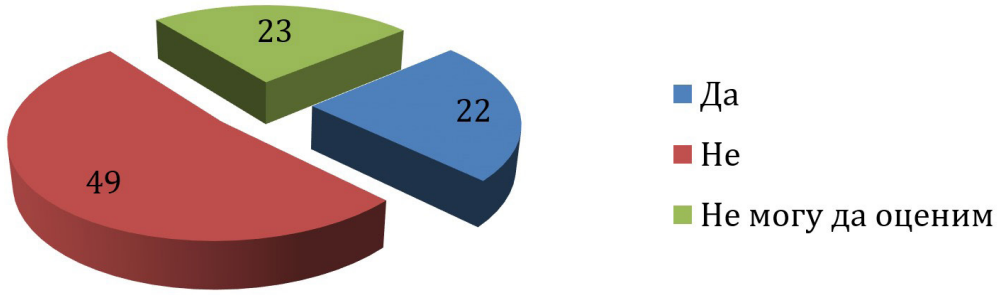
Као основно питање и основа за успостављање адекватног система КИ намеће се нормативно-правно регулисање КИ у ванредним ситуацијама.

Готово половина анкетираних лица одговорило је негативним одговором, што је сасвим и очекивано ако се зна да до недавно уопште није постојао Закон о критичној инфраструктури у Републици Србији.

Институције у којима је спроведено истраживање су: Сектор за ванредне ситуације МУП РС, Јавно предузеће „Железнице Србије" а. д., Јавно комунално предузеће „Београдски водовод и канализација", Јавно предузеће „Пошта Србије", Јавно предузеће „Електропривреда Србије", Акционарско друштво „Нафтна индустрија Србије", Јавно предузеће „Електромрежа Србије".

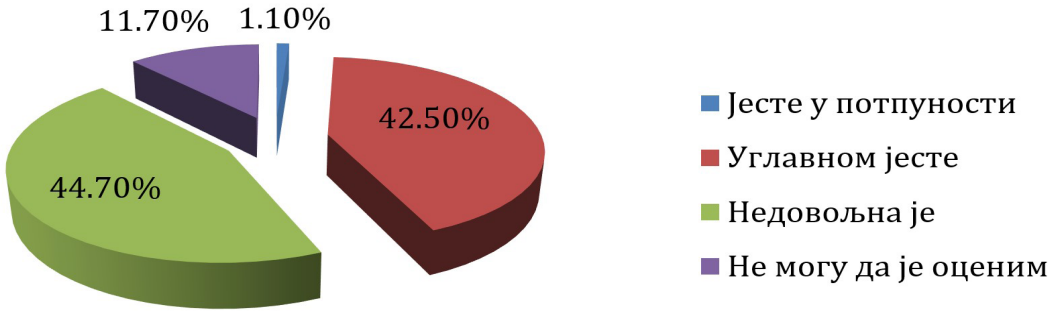
Графикони приказују одговоре испитаника на питања:

1) Да ли сматрате да су КИ и њено функционисање у условима ванредне ситуације довољно нормативно-правно регулисани?



Графикон 1. *Мишљење о функционисању КИ у условима ванредних ситуација*

2) Да ли је, према Вашем мишљењу, постојећа законска регулатива адекватна савременим опасностима и потребама заштите и спасавања у условима ванредних ситуација?



Графикон 2. *Усклађеност законске регулативе са савременим опасностима и потребама заштите и спасавања у условима ванредних ситуација*

Већина испитаника је одговорила да постојећа законска регулатива није у складу са савременим опасностима и реалним потребама заштите и спасавања у условима измењених околности. Република Србија се суочава са застарелом законском регулативом, што ће се вероватно отклонити у блиској будућности, доношењем подзаконских аката и изменама већ постојећих.

3) Да ли израда нормативно-правне регулативе у области заштите и спасавања треба да буде заједнички посао субјеката различитих профила (нпр. стручно-оперативни органи из области заштите и спасавања, здравствене службе, ватрогасно-спасилачких јединица МУП, Војске, стручњака из области заштите животне средине, радника државних органа управе и безбедносних структура БИА, ВБА или ВОА)?

Готово сви испитаници су сагласни да је потребна сарадња и мултидисциплинарни приступ у успостављању адекватног нормативно-правног оквира у области заштите и спасавања како људи, животне и радне средине тако и објеката критичне инфраструктуре (табела 4).

Табела 4. *Потреба за сарадњом у процесу израде нормативно-правне регулативе*

Р. бр.	**Заједничка израда нормативно-правне регулативе**	**Број лица**	**Проценат (%)**
1.	Неопходна је сарадња међу њима.	93	98,9
2.	Сарадња није неопходна.	/	/
3.	Немам мишљење о овом питању.	1	1,1

Испитаници су истакли да будући Закон о заштити КИ треба преузети одредбе о заштити КИ из Директиве ЕУ (Директива 2008/114/ЕЦ). У том смислу, неопходно је извршити измене и допуне Стратегије заштите и спасавања у ванредним ситуацијама. Такође, у постојеће референтне законе и подзаконска акта треба укључити нови термин 'критична инфраструктура' и ускладити их са Законом о критичној инфраструктури када буде ступио на снагу.

Највећи број анкетираних лица (око 70 %) је КИ дефинисао као објекте који су најугроженији од ванредних ситуација (електроенергетски објекти, саобраћај, ПТТ саобраћај, војни објекти, водовод и канализација итд).

Када је у питању значај КИ за управљање и превазилажење последица ванредне ситуације, испитаници су одговорили да КИ има изузетно велики значај (64,9%), а велики значај (30,9%) испитаника.

4) Који од објеката критичне инфраструктуре су најугроженији у условима ванредне ситуације?

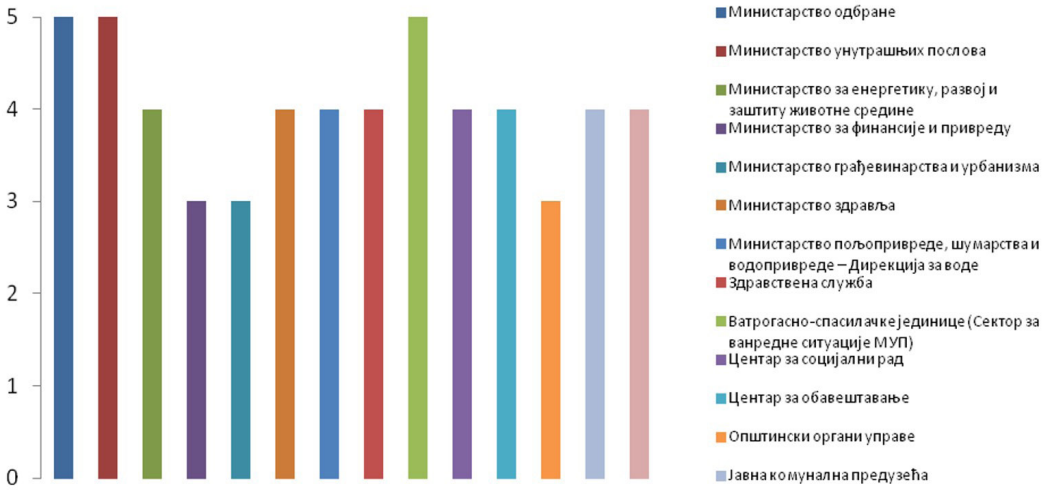
Добијени резултати су приказани на графикону 3.

Анализом резултата истраживања може се закључити да су испитаници изразили позитивне ставове о квалитету људских ресурса, а да су оцене о квалитету материјалних и финансијских ресурса незадовољавајуће. Када су у питању људски ресурси оцене су доста високе, међутим, оне се морају узети са резервом јер сви ти кадрови нису уско специјализирани за област заштите КИ, већ су им ти послови придодати у склопу редовних активности. Такво стање захтева јачање квалитета људских ресурса и прилагођавање система образовања будућих стручњака области заштите КИ у Републици Србији. Испитаници потенцирају ограниченост финансијских ресурсашто може бити значајан фактор за нормалан развој система заштите КИ.

Графикон 3. *Најугроженији објекти критичне инфраструктуре*

По питању сардње са институцијама, највишом оценом је оцењена сарадња са Министарством одбране, Министарством унутрашњих послова и Сектором за ванредне ситуације МУП РС (графикон 4).

Највећи број испитаника одговорио је да Министарство унутрашњих послова Републике Србије треба да чини окосницу планирања и управљања системом интегрисане заштите, што се у пракси и потврдило.



Графикон 4. *Оцена сарадње са институцијама Републике Србије*

5) Каква је стручна оспособљеност чланова Вашег стручно-оперативног органа из области цивилне заштите?

Највећи број испитаника је констатовао да стручно-оперативни органи који реализују активности из домена цивилне заштите поседује задовољавајућу оспособљеност за обављање свих послова. Највећи број одговорних лица поседује одговарајуће дипломе, сертификате о завршеним курсевима/усавршавању.

Да је пожељно сагледати и размотрити страна искуства и моделе заштите КИ јасно указује резултат одговора испитаника на питање: *Да ли управљање системом интегрисане заштите у отклањању последица напада на критичну инфраструктуру треба да се заснива на (дати одговор)?*

Табела 5. *Интегрисана заштита КИ*

Р. бр.	Интегрисана заштита КИ	Број лица	Проценат (%)
1.	Сопствени модел заштите и спасавања	9	9,6
2.	Страним искуствима у овој области	2	2,1
3.	Комбиновању страних искустава са сопственим	76	80,8
4.	Не знам	7	7,5

Највећи број испитаника је, као своју личну сугестију, навео да је потребно унапредити превентивно деловање у области заштите и спасавања, планско деловање снага за интервенцију, увести обавезну обуку омладине у школама и да се обезбеде већа финансијска средства за јачање целокупног система.

Досадашња емпиријска истраживања јасно указују да је стање у погледу функционисања и заштите критичне инфраструктуре у Републици Србији незадовољавајуће.

Доношење Закона о критичној инфраструктури обавеза је Републике Србије у процесу придруживања Европској унији. Акциони план о поглављу 24 за придруживање ЕУ препознаје Министарство унутрашњих послова Републике Србије као носиоца будућег закона. У оквиру Сектора за ванредне ситуације Републике Србије је тело које координира активности на успостављању међуресорне радне групе која ће имати за циљ дефинисање националне политике у области заштите критичне инфраструктуре.

Испитаници су указали на ризике којима су изложени критични инфраструктурни системи, превенцију и процену ризика КИ. То је сасвим оправдано ако се зна да отпорност критичне инфраструктуре означава способност система да настави извршавање критичних функција неопходних за испуњавање своје мисије у случају ванредних ситуација.

Незадовољавајуће стање је показано и у делу који се односи на планске активности и међуресорну сарадњу. Стога је неопходно у наредном периоду успоставити одговарајући систем јасног дефинисања надлежности и одговорности у области заштите КИ. Поред тога, веома битним се чини и успостављање адекватног система јавно-приватног партнерства и поверења између свих актера у области заштите КИ.

ЗАКЉУЧАК

Неопспорна је чињеница да ефикасан систем КИ представља основ за несметано функционисање како појединца тако и друштва у целини. Током низа последњих година схватање значаја и заштите КИ значајно се променило. Раније се рањивост КИ везивала за проблеме који се односе на функционисање високоризичних технологија, док данас КИ и њена заштита представљају питање веома значајно како за националну тако и за међународну безбедност.

Природни, друштвени ризици, ванредне ситуације и катастрофе постали су саставни део свакодневног живота, и остављајују веома озбиљне последице (људске жртве, материјални губици, деградација животне средине). Ови догађаји захтевају максимално ангажовање расположивих ресурса, од локалне заједнице преко региона до државног нивоа, стављајући на озбиљан испит политичке лидере и њихову способност да што ефикасније врате друштво у стање нормалног функционисања. Посматрано у контексту савремених глобалних претњи и ризика, управљање ванредним ситуацијама и успостављање заштите критичних инфраструктура представља приоритетан задатак како заједница локалне самоуправе, сваке државе, тако и наднационалних творевина. Област критичне инфраструктуре постаје последњих неколико година незаобилазна у стручној и научној литератури, од превенције ризика и катастрофа до могућих штетних последица људске активности. С елементима критичне инфраструктуре срећемо се у свим сферама наших свакодневних активности. Уколико се не препозна важност и значај великих техничких система, страх од недовољног улагања у критичну инфраструктуру биће оправдан, а привреда изложена великом ризику. Основни елемент државне безбедности сваке земље је заштита КИ. То су индустрија и институције, зграде и дистрибутивна мрежа која је основа за свакодневни живот. Њихова улога досеже од националне безбедности и јавних предузећа до функционисања државне управе и благостања њених грађана. Сваки поремећај континуираног функционисања ових делова друштва може да буде катастрофалан по само друштво.

На међународном нивоу, Европска унија има кључну улогу придајући велики значај овом питању. Државе чланице Европске уније су покренуле низ иницијатива и истраживачких програма како би се испитали различити аспекти заштите и претњи по КИ, као и утицаји који оштећење КИ може имати на образовање, привреду, здравство, систем комуникација и друге сегменте људске делатности.

Анализом међународних искустава у области идентификовања и заштите КИ утврђено је да дефиниција КИ и њен садржај не могу бити идентични у свакој држави понаособ па је логично да се та дефиниција и садржај морају утврдити на националном нивоу што важи и за Републику Србију.

С обзиром на тода је Република Србија земља која је била изложена процесу транзиције, процес дефинисања, идентификицаје, анализе критичних сектора и подсектора ће, свакако,

бити отежан. Том приликом, највећи проблем представља комплексност инфраструктурних система и идентификовање специфичних ризика и претњи којима су они изложени. Једно од главних питања тиче се одређивања редоследа спровођења радњи током израде адекватног система заштите КИ. Наиме, најпре треба утврдити ризике, претње и рањивости којима је одређени систем изложен, након чега се приступа идентификовању критичних сектора и изради специфичне класификације.

Такође, потребно је инвестирати у застареле инфраструктурне објекте што представља велику инвистицују и финансијску потрошњу.

Област заштите КИ тек што је нормативно уређена и створен је правни оквир за дефинисање, идентификацију, одређивање и заштиту националне и европске критичне инфраструктуре. Сада након усвајања закона о КИ биће потребно усвојити и подзаконска акта која ће обезбедити практична решења и критеријуме за идентификацију КИ и сектора КИ. Доношењем Закона о критичној инфраструктури нису решени проблеми и недостаци у области КИ, потребно је радити на развијању свести власника и оператора КИ, јачати јавно-приватно партнерство у заштити и отпорности КИ, као и размена искустава и знања са домаћим и међународним институцијама.

Потребно је одредити приоритете код идентификовања КИ, а затим регулисати оне аспекте заштите КИ који су се у досадашњој домаћој и међународној пракси показали као нарочито проблематични, а то су јавно-приватно партнерство и размена осетљивих информација.

Анализом међународних искустава у области идентификовања и заштите КИ утврђено је да дефиниција КИ и њен садржај не могу бити идентични у свакој држави понаособ, па је сасвим оправдано да се та дефиниција и садржај морају утврдити на националном нивоу, што важи и за Републику Србију.

Република Србија, у односу на земље из непосредног окружења, ужива доста висок степен безбедности у релативно нестабилном регионалном и међународном окружењу.

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 Републици Србији.

У погледу мера заштите критичне инфраструктуре све државе, укључујући и Републику Србију, првенствено треба да дефинишу редослед поступака:

– идентификација КИ,
– израда мапа КИ,
– размена информација,
– оспособљавање особља ангажованих на пословима и задацима у системима КИ,
– увежбавање система за заштиту КИ или опоравак у случају ванредне ситуације.

Уз организовану и планирану реализацију реформи у систему управљања ванредним ситуацијама, у складу са развијеним европским земљама, Република Србија мора изградити сопствени приступ управљања ванредним ситуацијама у заштити критичних инфраструктура, узимајући у обзир расположиве капацитете и могућности. Искуства других земаља могу бити корисна, али их увек треба прилагодити сопственим интересима, с крајњим циљем заштите грађана и државе од ризика и опасности.

ЛИТЕРАТУРА

I Монографије и научностручни радови

1. Adger, W. N. (2006). Vulnerability. *Global Environmental Change*, 16, 268—281.
2. Andreas, W., Metzger, J., Dunn, M., eds. (2004). *International CIIP Handbook center for security studies at the Swiss federal institute of technology*. Zurich: Center for Security Studies..
3. Annual Information Society Report 2007 — *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. Brussels, 30th March 2007.
4. Архипова, Н. И., Кульба, В. В. (1998). *Управление чрезвичайных ситуациях*. Москва: РГУ.
5. Assante, J. M. (2009). Infrastructure Protection in the Ancient World. Proceedings of the 42nd Hawaii International Conference on System Sciences. *HICSS-42*. 1—10. doi: 10.1109/HICSS.2010.442.
6. Baker, G. H. (2005). *A vulnerability assessment methodology for critical infrastructure sites*. Boston, Massachusetts: Department of Homeland Security symposium: R&D partnerships in homeland security.
7. Bankoff, G. (2004). The Historical Geography of Disaster: 'Vulnerability' and 'Local Knowledge' in Western Discourse.In: Bankoff, G., Frerks, G., Hilhorst, D. (eds.). *Mapping Vulnerability: Disasters, Development and People*. Routledge.
8. Bartlett, H., Holman, G., Somes, E. T. (2004). *The art strategy and force planning, Strategy and force planning, Bartlett model*. Newport: Naval War College Press.
9. Bimal, K. P. (2012). *Environmental Hazards and Disasters Contexts, Perspectives and Management*. Wiley — Blackwell.
10. Blagojevic, M., Nikac, Ž. (2010). Legal and security aspects of engagement of the Ministry of interior of the Republic of Serbia in emergency situations. Second International scientific conference *Transport of dangerous goods and risk management*, INTERNATIONAL THEMATIC ISSUE (dr Marija Vukić, ed.). Belgrade: "Kirilo Savić" Institute a. d.
11. Благојевић М. (2011) Безбедност, заштита и спасавање у ванредним ситуацијама, монографија, Задужбина Андрејевић, ISSN 1450-653X;261 ISBN 978-86-7244-970-9 COBISS.RS.ID 186116620
12. Брзаковић, М. (2009). *Интероперабилност и безбедност информација у организацијама од стратешког значаја у ванредним ситуацијама* (докторска дисертација). Београд: Факултет безбедности.

13. Brown G., Carlyle M., Salmer J., Wood K. (2005). Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses. *INFORMS Tutorials in Operations Research*. Hanover: Institute for Operations Research and the Management Sciences, 102–123.

14. Buzan, B., Waiver, O., Wilde, de J. (1998). *Security: A New Framework For Analysis*. Boulder, Colorado: Lynne Rienner Publishers, Inc.

15. Whale, T., Beaty, G. (2004). *Emergency Management Guide for Business Industry*. Federal Emergency Management Agency (FEMA), Internet edition (https://www.fema.gov/media-library/assets/documents/3412).

16. Garb, G. (2009) *Varnostno upravljanje kritične infrastrukture*. Magistrsko delo. Celje: Fakulteta za logistiko.

17. Гаћиновић, Р. (2013). Спољни оружани облици угрожавања капацитета безбедности државе. *Политичка ревија*, Vol. 35 No. 1/2013, 183—201.

18. Goetz, E., Shenoi, S. (eds.) (2008). *Infrastructure Protection*. , Boston: Springer a.g.. Library of Congress Control Number 2007938897, ISBN 978-0-387-75461-1.

19. Gospić, G., Murić, D. (2012). *Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia*. International Conference on Applied Internet and Information Technologies, Zrenjanin.

20. Деканић, И. (2008). Положај Хрватске у могућим енергетским и геополитичким кризама. *Хрватска — како сада даље*, Загреб: Центар за демократију и право „Мико Трипало".

21. Dembskey, J. E. (2009). *The Aqueducts of Ancient Rome*, University of South Africa.

22. Dunn, M., Mauer, V. (2006). International critical information infrastructure protection handbook, Zurich: ETH Center for conflict studies, Vol. I, .

23. Ђукић, С. (2006). Савремени организовани криминалитет као облик угрожавања националне безбедности. *Економски изазови*, бр. 9/2016.

24. Edward, B. (2005). *Natural Hazards*, 2nd Edition, Cambridge: University Press.

25. Engelbrekt, K., Förberg, M. (2005). *Managing Crises in Bulgaria* Stockholm: Elanders Gotab.

26. Egan, M. J. (2007). Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *Journal of Contingencies and Crisis Management*, Vol. 15 No. 1, 4—17.

27. Europe 2020 – A strategy for smart sustainable and inclusive growth, Communication from the Commision. Brussels, 3 March 2010.

28. Executive Order 13010 — Critical Infrastructure Protection. *Federal Register*, Vol. 61, No. 138 (1996), 37347—37350.

29. Ezell, B. C. (2007). Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*, 27(3), 571—583.

30. Зутер, Б. (2011) Стратешки кризни менаџмент Швајцарске ‑ Поређење швајцарског модела са девет страних референтних држава. *Војно дело*, Београд, стр. 37, 2011.

31. Јаковљевић, В. (2010). Ресурси критичне инфраструктуре и њихов значај за управљање ванредним ситуацијама. *Годишњак Факултета безбедности*, Београд: Факултет безбедности, 63—81.

32. Jopling, L. (2007). *The protection of critical infrastructure*. Special Rapporteur (United Kingdom).

33. Kash, Toby J., Darling, John R. (1998). Crisis management: prevention, diagnosis and intervention. *Leadership & Organization Development Journal*, Vol. 19, Issue: 4, pp.179—186.

34. Кекић, Д., Млађан, Д. (2007). Ванредна ситуација – прилог концептуалном одређењу безбедности (Emergency – a contribution toward conceptual determination of security). НБП НАУКА • БЕЗБЕДНОСТ • ПОЛИЦИЈА, XII. 61—83.

35. Кековић, З., Савић, С., Комазец, Н., Милошевић, М., Јовановић, Д. (2011). *Процена ризика у заштити лица, имовине и пословања*. Београд: Центар за анализу ризика и управљање кризама.

36. Кљајић, С. М. (2010). *Примјена ICT у управљању критичном инфраструктуром утранзицијским земљама*. Београд: ЕЛФОР.

37. Комарчевић, М. (2018). *Увод у критичну инфраструктуру*, Београд: Академска мисао.

38. Koubatis, A., Schonberger, J.Y. (2001). Risk management of complex planning framework. *Internatinal Journal of Critical Infrastructures*, Vol. 1, Nos. 2/3, 195–215.

39. Кулишић, Д. (2008). Мјере сигурности од терористичких и иних злонамјерних угроза критичне инфраструктуре (I дио). *Сигурност*, 50, 3 (2008): 201–226.

40. La Porte, T. R. (2007). Critical Infrastructure in the Face of a Predatory Future: Preparing for untoward surprise. *Journal of Contingencies and Crisis Management*, Vol. 15, No.1, 60–64..

41. Lewis, G. T. (2006). Critical Infrastructure Protection in Homeland Security - Defending and Networking Nation. New Jersey: Wiley-Interscience.

42. Liscouski, R. (2004). *Infrastructure Protection*, Dept. of Homeland Security, Testimony before the House Select Committee on Homeland Security; Infrastructure and Border Security Subcommittee.

43. Ljuština, A., Mališ Sazdovska, M., Knezević Lukić, N, (2014). *Safety in emergency situations caused by natural disasters*. Thematic Conference Proceedings of International Significance, Vol. 2, Scientific Conference „Archibald Reiss Days", Belgrade,3—4 march, Academy of Criminalistic and Police Studies.

44. Медаковић, Р. (2005). ИКТ индустрија као доминантна привредна грана у Србији. *Е-волуција*, бр. 8. (http://old.bos.rs/cepit/evolucija/html/8/ikt-granaindustrije.htm).

45. Милашиновић, Р., Мијалковић, С. (2011). Тероризам као савремена безбедносна претња. Зборник радова *Супротстављање тероризму – међународни стандарди и правна регулатива*. Бања Лука: Висока школа унутрашњих послова Република Српска.

46. Мићновић, М., Никач, Ж., (2012). *Фактори заштите критичне инфраструктуре у ванредним ситуацијама*, *Супротстављање савременом организованом криминалу и тероризму*. Едиција ΑΣΦΑΛΕΙΑ, Књига IV, Београд: Криминалистичко-полицијска академија.

47. Mićović, M., Jakovljević, V. (2014). *The system of critical infrastructure of the Republic of Serbia in response to emergencies - Opportunities and perspectives*, V međunarodni stručno-znanstveni skup „Zaštita na radu i zaštita zdravlja". Zadar: Veleučilište u Karlovcu, .

48. Мићновић, М. (2014). Специфичности заштите критичне инфраструктуре. *Безбедност*, 3/2014, 165—173.

49. Мићновић, М., Цветковић, Д. (2014). Последице загађења животне средине на људску популацију. *Ecologica*, No. 74, 317-321.Мићновић, М., Цветковић, Д. (2015). Угрожавање инфраструктурног система природним катастрофама услед климатских промена. *Ecologica*, No. 78, 333—337.

50. Мићовић, М. (2016). *Безбедносни аспекти функционисања критичне инфраструктуре у ванредним ситуацијама*. Докторска дисертација, бр. 63/7-11 од 23.02.2016, УДК: 614.8:351.78(043.3). Београд: Факултет безбедности.

51. Moteff, J., Copeland, C., Fischer, J. (2003). *Critical Infrastructures: What Makes an Infrastructure Critical?* Washington: Congressional Research Service (The Library of Congress).

52. Moteff, D. J., Parfomak, P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification*. CRS Report for Congress, Congressional Research Service, Library of Congress.

53. Murray, A. T., Grubesic, A. (2012). Critical infrastructure protection: The vulnerability conundrum. *Telematics and Informatics*, Vol. 29, No. 1, 56—65.

54. Nickolov, E. (2005). Critical information infrastructure protection: Analysis, evaluation and expectations - study case of Bulgaria. *Information & Security: An International Journal*, Vol. 17, 116—117.

55. Papa, M., Shenoi, S. (2008). *Critical Infrastructure Protection II – Emergent Commission of the European Communities, Critical infrastructure protection in the fight against terrorism* (Brussels, 20 October 2004), COM(2004)702 final.

56. Papa, M., Shenoi, S. (2008a). *Risks in Critical Infrastructures*. New York: International Federation for Information Processing.

57. Peerenboom, J. P. (2001). *Infrastructure Interdependencies: An Overview of Concepts and Terminology*. NSF Workshop. June 2001. www.pnwer.org/pris/peerenboom_pdf.pdf. Перинић, Ј. (2007). Кризно комуницирање на случају трагедије ватрогасаца на Корнату. *Медианали*, Свеучилиште у Дубровнику, год. 1, 47—66.

58. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructure*, 1997.

59. Prezelj, I. (2008). Role of the European Union in the Fight against International Terrorism. In: I. Prezelj (Ed.), *The Fight Against Terrorism and Crisis Management in the Western Balkans*, IOS Press 16—34.

60. Prezelj, I., Kustec Lipicer, S. (2010). *Public and policy management of critical infrastructure: Lessons from Integral Nations Cross-Sectoral Scanning in Slovenia*. IRSPM Conference, Panel: Risk and crisis management in the public sector, Berne, 15.

61. Предог Националних становишта. Назив пројекта: *Resilience of Critical Infrastructure Protection in Europe (RECIPE)*. Финансијер пројекта: Механизам Уније за цивилну заштиту, пројекте приправности и превенције у цивилној заштити и загађењу мора, 2014.

62. Radvanovsky, R., McDougall, A. (2010). *Critical Infrastructure, Homeland Security and Emergency. Preparedness*. Boca Raton, FL: CRC Press/Taylor & Francis Group.

63. Rashed, T., Weks, J. (2003). Assessing vulnerability to earthquake hazards through spatial multicriteria analysis of urban areas. *International Journal of Geographical Information Science*, Vol, 17, Issue 6, 547—576.

64. Ribeiro, S. L., Bezerra, E. K., Nakamura, E. T. (2005). *Critical Infrastructure in Brazil*. 1st IEEE International Workshop on Critical Infrastructure Protection, 3-4th Nov 2005, Darmstadt.

65. Rinaldi, S. M. (2004). *Modeling and simulating critical infrastructures and their interdependencies*. Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS'04). 8 pp. 10.1109/HICSS.2004.1265180.

66. Roper, C. (1999). *Risk Management for Security Professionals*, Butterworth-Heinemann.

67. *Словарь виталитской социологии* (ред. Григориев С. М.), Гардарики, Москва, 2006.

68. Smedts, B. (2010). *Disruptions of gas supply from Russia to East Europe during the winter of 2008-2009. Critical Infrastructure Protection Policy in the EU: state of the art and evaluation in the (near) future*. Royal High Institute for Defense, Center for Security and Defense Studies, Focus paper 15.

69. Solano, E. (2010). *Methods for Assessing Vulnerability of Critical Infrastructure*. Institute for Homeland Security Solutions.

70. Stanković, M. (2006). *System Risk Engineering the Basis of Integrated Management System*. Plenary paper, Proceedings of 9th International Conference *Dependability and Quality Management* DQM-2006, Prijevor, Čačak.

71. Stoimenov, L., Predić, B., Mihajlović, V., Stanković, M. (2005). *GIS Interoperability Platform for Emergency Management in Local Community Environment*. Proceedings printed as book (Eds. Fred Toppen, F., Painho, M.), AGILE 2005, 8th AGILE Conference on GIScience, Estoril, Portugal, 26—28. 5. 2005.

72. Tagarev, T., Pavlov, N. (2007). *Planning measures and capabilities for protection of critical infrastructures - study case of Bulgaria*.

73. Tagarev, T. (2006). The Art of Shaping Defense Policy: Scope, Components, Relationships (but no algorithms). *Connections: The Quarterly Journal* 5(1), Spring-Summer15—34.

74. The Clinton Administration's Policy on Critical Infrastructure Protection: *Presidential Decision Directive No. 63*, White Paper, May 22, 1998.

75. Таталовић, С. (2008). *Енергетска сигурност и критична инфраструктура*. Загреб: Политичка култура.

76. Trim, Peter, R. J. (2004). An integrative approach to disaster management and planning. Disaster Prevention and Management: An International Journal, Vol. 13 Issue: 3, pp.218—225,

77. Twigg, J., Bhatt, M.R. (1998). Understanding Vulnerability: South Asian Perspectives.. *Disaster Prevention and Management: An International Journal*, Vol. 8 Issue: 5, 370‑452.

78. Commission of the European Communities, *Green Paper on a European Programme for Critical Infrastructure Protection* (Brussels, 17. 11. 2005.), COM(2005) 576 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576.

79. *Critical Infrastructure and Key Resources*, Cansas City Regional Tew, Interagency Analisys Center.

80. Цветковић, В. (2014). *Заштита критичне инфраструктуре од последица природних катастрофа*. VIII међународна конференција Дани кризног управљања. Велика Горица: Велеучилиште Велика Горица, 1281—1293.

81. Цветковић, В. (2015). Феноменологија природних катастрофа теоријско одређење и класификација природних катастрофа. Безбједност — Полиција – Грађани. година XI број 3–4, 311–333.

82. Цветковић, В., Вучић, С., Гачић, Ј. (2015). Климатске промене и национална одбрана. *Војно дело*, 5/2015, 181–203.

83. Цветковић, В., Филиповић, М. (2017). Последице природних катастрофа — фактори утицаја на перцепцију грађана Србије. *Ecologica*, Vol. 24, No. 87, 1—6.

84. Harrington, L. S. B. (2005). Vulnerability and Sustainability Concerns for the US High Plains. *Rural Change and Sustainability: Agriculture, the Environment and Communities* (eds. Essex, S.J., Gilg, A.W., Yarwood, R.). Cambridge, MA: CABI Publishing.

85. Херга, М. (2010). *Национална критична инфраструктура*. Менаџмент и сигурност - M&C 2010: Планирање и сигурност.

86. Zimmerman, R. (2004). Decision-making and the Vulnerability of Interdependent Critical Infrastructure. *IEEE Control Systems Magazine*, pp. 23.

87. Чемерин, Д., Трут, Д. (2010). Критерије за утврђивање хрватске критичне инфраструктуре. Зборник радова *Хрватска платформа за смањење ризика од катастрофа*, Државна управа за заштиту и спашавање, Загреб.

88. Чемерин, Д. (2011). Управљање критичним инфраструктурама. Зборник радова са IV међународне конференције *Дани кризног управљања*. Велика Горица: Велеучилиште Велика Горица.

89. Шкеро, М., Атељевић, В. (2015). Заштита критичне инфраструктуре и основни елементи усклађивања са директивом Савета Европе 2008/114/ES. *Војно дело*, бр. 3, 192—207.

II Законски и подзаконски прописи

1. Закон о критичним инфраструктурама Републике Хрватске (*Народне новине*, бр. 56/13); Правилник о методологији за израду анализе ризика пословања критичних инфраструктура (*Народне новине* , бр. 128/13); Одлука о одређивању сектора из којих средишња тијела државне управе идентificирају националне критичне инфраструктуре те листе редосљеда сектора критичних инфраструктура *Народне новине* , бр. 118/13).

2. Закон о критичним инфраструктурама Републике Хрватске, *Народне новине*, бр. 56/13.

3. Закон о одбрани Републике Србије, *Службени гласник Републике Србије*, бр. 116/2007, 88/2009 – др. закон, 104/2009 – др. закон, 10/2015 и 36/2018).

4. Закон о полицији, *Службени гласник Републике Србије*, бр. 6/2016, 24/2018 и 87/2018.

5. Zakon o kritični infrastrukturi, *Uradni list RS*, št. 75/17.

6. Национална стратегија заштите и спасавања у ванредним ситуацијама (усвојена на седници Скупштине Републике Србије 18. новембра 2011.).

7. Статут Јавног предузећа „Пошта Србије", од 23. фебруара 2017, године доступан је на званичном сајту Јавног предузећа „Пошта Србије".

8. Стратегија националне сигурности Републике Хрватске, *Народне новине* , бр. 32/2002.

9. Стратегија развоја друмског, железничког, водног, ваздушног и интермодалног транспорта у Републици Србији 2008–2015.

10. Стратегија развоја информационог друштва у Републици Србији до 2020, Влада Републике Србије.

11. Устав Републике Србије (чл. 97), *Службени гласник Републике Србије*, бр. 83/06, Београд, 8. новембар 2006.

12. 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, L 345/75-L 345/82, 2008.

13. The Structure, Role and Mandate of Civil Protection in Disaster Risk Reduction for South Eastern Europe South, „South Eastern Europe Disaster Risk Mitigation and Adaptation Programme".

III Интернет сајтови

1. http://www.economy.rs/finansije/9790/Poslovanje-finansijskih-institucija
2. http://www.otvoreniparlament.rs/akt/3781.
3. http://www.oecd.org/dataoecd/2/41/40700392.pdf
4. http://www.cad.gov.rs
5. http://prezentacije.mup.gov.rs/svs/
6. http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/javne_objave/2018/MORS_Zgibanka_kriticna_infrastruktura_v3_splet.pdf
7. http://www.economy.rs/finansije/9790/Poslovanje-finansijskih-institucija-u-Republici-Srbiji-2012-odine.html.
8. http://www.posta.rs/
9. http://www.ems.rs/index.php?lang=2
10. http://eps.rs/
11. http://www.zeleznicesrbije.com/
12. https://www.bvk.rs/home/
13. http://www.srbijavode.rs/
14. https://www.nis.eu/lat/

РЕЗИМЕИ

Савремене друштвене промене усложњавају динамику идентификације, планирања, финансирања, изградњу и заштиту КИ. Прилагођавање новим изазовима и ризицима, окружењу у коме функционише КИ, захтева осмишљавање новог концепта планирања система КИ који ће омогућити отпорност критичних система на елементарне непогоде, катастрофе и друге непредвиђене намерне или ненамерне активности.

Усвајање нормативног оквира везаног за КИ, усклађеног са елементима Директиве Европског савета 2008/114/ЕС један је од важних задатака Републике Србије на путу европских интеграција. Директива Савета Европе 2008/114/ЕС из 2008. године дефинише КИ, представља основу за наредне кораке у дефинисању критеријума за КИ, потом заједничке процедуре за идентификацију и означавање европске КИ и заједнички приступ у процени потреба за побољшавање заштите. Међутим, доношењем закона не решава се процес успостављања система КИ у Републици Србији, већ следе захтевни поступци и планске активности с циљем дефинисања и мапирања КИ као отпорног система који ће одолети изазовима и ризицима што могу угрозити његово безбедно функционисање.

Република Србија је усвојила Закон о КИ који је ступио на снагу 2018. године. У наредном периоду следе планске мере и активности у оквиру којих ће се имплементирати норме прописане наведеним законом.. Такође, полазну основу у изради модела и решења Република Србија може поставити сагледавањем решења и модела земаља у окружењу, која могу применити или не применити.

Успостављање механизама јавно-приватног партнерства у заштити и отпорности КИ нарочито је значајно јер ће у процесу либерализације све више објеката КИ бити у приватном власништву, а, с друге стране, у заштити КИ све важнију улогу има сектор приватне безбедности.

Идентификација сектора КИ, идентификација и приоритизација објеката КИ, усвајање методологија за процену ризика у КИ, јавно-приватно партнерство у заштити КИ, размена осетљивих података, јачање отпорности КИ, као и евентуално успостављање нису једини изазови са којима ће се заинтересоване стране у Србији суочити у наредном периоду. Изазови се могу превазићи доношењем подзаконских аката, хармонизацијом других релевантних закона (нпр. Закон о тајности података, Закон о јавно-приватном партнерству, Закон о одбрани итд), затим едукацијом и подизањем свести власника и оператора КИ, усвајањем и применом међународних стандарда и бољом сарадњом са академским институцијама.

SPECIFICITIES OF CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF SERBIA

Contemporary social changes, an environment in which society lives, complicate the dynamics of identification, planning, financing, construction and protection of a critical infrastructure. Adapting to new challenges and risks, as well as the environment in which critical infrastructure operates requires of us all a new concept of planning a critical infrastructure system that will allow critical systems to be resilient to natural disasters, catastrophes and other unforeseen intentional or unintentional activities.

One of the most important tasks of the Republic of Serbia in the path of European integration is the adoption of a normative framework related to critical infrastructure, which is in line with the elements of the Council of Europe Directive 2008/114/EC, which defines critical infrastructure, common procedures for the identification and designation of European critical infrastructure, common approach in assessing the needs for protection improvement. It is the basis for next steps in defining the criteria for critical infrastructure. However, passing laws does not resolve that the process of establishing a critical infrastructure system in the Republic of Serbia, so it must be followed by demanding procedures and planning activities with the aim of defining and mapping the critical infrastructure as a resistive system that will resist challenges and risks that could threaten the safe functioning of the critical infrastructure system.

The Republic of Serbia adopted the Law on Critical Infrastructure, which came into force in 2018. In the following period, the planned measures and activities will be taken within which the prescribed norms will be implemented. Also, the Republic of Serbia can look at the solutions and models of countries in the environment that can serve as a starting point, but not to apply them, which is quite justified taking into account the specifics each state has.

The establishment of public-private partnership mechanisms for protection and resilience of CI is particularly important because in the process of liberalization more and more critical infrastructure facilities will come into private ownership, and on the other hand the private security sector has an increasing role in the protection of critical infrastructure.

Critical infrastructure sector identification, identification and prioritization of CI objects, adoption of methodologies for risk assessment in CI, public-private partnership in CI protection, sensitive data exchange and strengthening resilience of CI are not the only challenges that will be faced by stakeholders in Serbia in the next period. These challenges can be overcome by passing bylaws, harmonizing other relevant laws (eg. the Law on Data Secrecy, the Law on Public-Private Partnership, the Law on Defense, etc.), then by educating and raising the awareness of owners and operators of critical infrastructures, by adopting and applying the international standards and better cooperation with academic institutions.

РЕГИСТАР ПОЈМОВА

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

711.7/.8(497.11)(0.034.4)
351.78(497.11)(0.034.4)

БЛАГОЈЕВИЋ, Марија, 1980-
Специфичности критичне инфраструктуре у Републици Србији [Електронски извор] / Марија Д. Мићовић. - Београд: Криминалистичко-полицијски универзитет, 2020 (Београд : Криминалистичко-полицијски универзитет). - 1 електронски оптички диск (CD-ROM) ; 12 cm. - (Едиција Монографије / [Криминалистичко-полицијски универзитет] ; књ. 42)

Системски захтеви: Нису наведени. - Насл. са насловне стране.- Тираж 100. - Напомене и библиографске референце уз текст. - Библиографија: стр. 93-99. - Регистар.

ISBN 978-86-7020-441-6

а) Техничка инфраструктура - Безбедносни аспект - Србија

COBISS.SR-ID 16041481