УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

ВЛАДИМИР М. НИНКОВИЋ

ОТПОРНОСТ КРИТИЧНЕ ИНФРАСТРУКТУРЕ НА НЕРУТИНСКЕ РИЗИКЕ

Докторска дисертација

БЕОГРАД, 2024

UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

VLADIMIR M. NINKOVIĆ

RESILIENCE OF CRITICAL INFRASTRUCTURE TO NON-ROUTINE RISKS

Doctoral dissertation

BELGRADE, 2024

Ментор: Доктор Зоран Кековић, редовни професор, Универзитет у Београду, Факултет безбедности

- Чланови комисије:

Доктор Желимир Кешетовић, редовни професор, Универзитет у Београду, Факултет безбедности

Доктор Борис Кордић, редовни професор, Универзитет у Београду, Факултет безбедности,

Доктор Роберт Микац, ванредни професор, Универзитет у Загребу, Факултет политичких знаности.

- Датум одбране:

Изјаве захвалности

Захваљујем се ментору проф. др Зорану Кековићу на стрпљењу, драгоценим сугестијама и преданом менторском раду током израде ове докторске дисертације. Захвалност исказујем проф. др Желимиру Кешетовићу, проф. др Борису Кордићу, проф. др Роберту Микцу и др Дејвиду Рубенсу на саветима који су допринели унапређењу квалитета докторске дисертације. Такође, захвалност исказујем др Александру Узелцу за помоћ приликом лекторисања дисертације, као и проф. др Харису Дајчу на добронамерним саветима. Посебну захвалност изражавам породици и пријатељима на разумевању и подршци током писања докторске дисертације.

Отпорност критичне инфраструктуре на нерутинске ризике

Сажетак: Свет у којем живимо је све комплекснији, како са становишта безбедности, тако и са становишта зависности друштвених заједница од технологије и технолошких система који су и међусобно повезани комплексним везама. Неуобичајени, „нерутински“, ризици, окарактерисани ниском вероватноћом, а великим утицајем или последицама, као што су природне катастрофе, рат, терористички напад или пандемије могу узроковати значајне прекиде пословања критичне инфраструктуре, као и њихов спори или отежани опоравак, што угрожава националну безбедност и добробит грађана. Отпорности смо у овој дисертацији пришли кроз приступ Вилдавског (Wildavsky) према којем су антиципација (тј. традиционални, пробабилистички менаџмент ризиком) и отпорност две могуће стратегије менаџмента ризиком, од које је потоња адекватнија у условима високе неизвесности. Отпорност критичне инфраструктуре у овом раду посматрамо кроз призму организационе отпорности појединачних оператора критичне инфраструктуре у Републици Србији, Републици Хрватској и Босни и Херцеговини. Такође, сматрали смо да је неопходан темељни осврт на анализу односа концепата отпорности, кризног менаџмента и менаџмента континуитетом пословања, будући да су њихова разграничења магловита и да у литератури до сада није успостављен консензус о њиховим односима. За потребе истраживања креиран је интегративни аналитички модел организационе отпорности, комбинацијом постојећих аналитичких модела капацитета отпорности и модела „рибље кости“. У овом моделу анализирали смо четири капацитета отпорности (антиципативни, ресорптивни, ресторaторни и адаптациони) кроз индикаторе који припадају тврдом (активности, „шта се ради“ у циљу унапређивања отпорности) и меком (карактеристике, „како се те активности спроводе“) аспекту. Модел је пилотиран кроз теренско истраживање које је обухватило петнаест полуструктурисаних интервјуа са доносиоцима одлука, менаџерима безбедности и континуитета пословања у операторима критичне инфраструктуре у Републици Србији, Републици Хрватској и Босни и Херцеговини. Пилот студија резултирала је теоријским препорукама о могућим даљим токовима истраживања, као и практичним препорукама за операторе критичних инфраструктура у Републици Србији и региону.

Кључне речи: отпорност, ризик, критична инфраструктура, кризни менаџмент, континуитет пословања.

Научна област: друштвено-хуманистичке науке.

Ужа научна област: студије безбедности.

Resilience of critical infrastructure to non-routine risks

Abstract: The world we live in is becoming increasingly complex, both in terms of security and in terms of the dependence of social communities on technology and technological systems, which are interconnected through complex relationships. Unusual, "non-routine" risks, characterized by low probability but severe impact or consequences, such as natural disasters, war, terrorist attacks, or pandemics, can cause significant disruptions to the operations of critical infrastructure and impede or delay their recovery, thereby threatening national security and citizen welfare. In this dissertation, we approached resilience using Wildavsky's perspective, which posits that anticipation (i.e., traditional, probabilistic risk management) and resilience are two possible risk management strategies, with the latter being more appropriate under conditions of high uncertainty. This paper examines the resilience of critical infrastructure through the lens of organizational resilience of individual critical infrastructure operators in the Republic of Serbia, the Republic of Croatia, and Bosnia and Herzegovina. A combined analytical model of organizational resilience was created for research purposes by combining existing resilience capacity models and the "herringbone" model. In this model, we analyzed four resilience capacities (anticipatory, absorptive, restorative, and adaptive) through indicators belonging to both the hard (activities, "what is done" to enhance resilience) and soft (characteristics, "how these activities are implemented") aspects. The model was piloted through field research that included fifteen semi-structured interviews with decision-makers, security managers, and business continuity managers in critical infrastructure operators in the Republic of Serbia, the Republic of Croatia, and Bosnia and Herzegovina. The pilot study resulted in theoretical recommendations for potential further research directions, as well as practical recommendations for critical infrastructure operators in the Republic of Serbia and the region.

Keywords: resilience, risk, critical infrastructure, business continuity, crisis management.

Scientific field: Social and humanistic sciences.

Scientific sub-field: Security studies.

САДРЖАЈ:

СПИСАК ТАБЕЛА:

СПИСАК ГРАФИКОНА:

УВОД

Свет у којем живимо је све комплекснији, како са становишта безбедности, тако и са становишта зависности друштвених заједница од технологије и технолошких система који су и међусобно повезани комплексним везама. У том динамичном окружењу сведоци смо појављивања бројних безбедносних претњи који су се до јуче чинили занемарљивима, а данас представљају ризике са изузетно великим последицама. Неуобичајени, „нерутински“, ризици, окарактерисани ниском вероватноћом, а великим утицајем или последицама, као што су природне катастрофе, рат, терористички напад или пандемије могу узроковати значајне прекиде пословања критичне инфраструктуре, као и њихов спори или отежани опоравак, што угрожава националну безбедност и добробит грађана. Иако ће у овој дисертацији фокус бити на пандемију коронавируса тј. вируса COVID-19, бројни глобални и регионални системски шокови претходних година и деценија утицали су на наше поимање, разумевање и моделирање ризика. Сви ти поремећаји описивани су епитетима попут „без преседана“ или „неочекивани“. Другим речима, те претње су биле неидентификоване, или у ретким случајевима када су биле идентификоване, то јест када би се налазиле у регистру ризика, њихова вероватноћа или утицај су били потцењени. Укратко, приликом идентификације и процене ризика главни проблем је био висока неизвесност таквих догађаја.

Уколико је крај XX века с правом био назван „друштвом ризика“, данашње доба глобалне умрежености, међузависности и доминације информативне сфере можемо назвати „друштвом неизвесности“. Неизвесност се може јавити у два облика – квантитативном и квалитативном. Наиме, када вероватноћу, последице, па самим тим ни ризик од одређених опасности није могуће израчунати услед непостојања јасних историјских или статистичких података, као и високог степена варијабилности у том случају говоримо о квантитативној (алеаторној) неизвесности.

Када не можемо ни предвидети шта нас може у будућности задесити, тада се налазимо у домену квалитативне или епистемолошке неизвесности то јест, према бившем министру одбране САД, Доналда Рамсфелда, „непознатих непознаница“, (Department of Defense 2002) или „црних лабудова“ по речима Насима Талеба (Taleb 2015). Истраживања у области когнитивне психологије (Данијел Канеман, Амос Тверски, Барух Фишхоф, Пол Словик) указују на субјективну природу ризика и на ограниченост људских способности за предвиђање будућих догађаја, чак и релативно познатих феномена. Врло често су најозбиљније безбедносне, економске, политичке, па и корпоративне кризе и катастрофе управо последица таквих непредвиђених догађаја, непознатих претњи, лоше процењених ризика. Стога, суочени са могућношћу избијања нових „црних лабудова“ све више теоретичара и практичара даје предност оснаживању штићеног система, то јест јачању његове отпорности, пре него заштити - активном усмерењу ка безгрешној идентификацији безбројних извора ризика, њиховој анализи и успостављању конкретних процедура и мера за митигацију. Како Лагадек наводи, „више није довољно контролисати многобројне фронтове ризика, потребно је радити на чврстоћи ткива. Другим речима, треба развити отпорност – након што је наша логика ефикасности последњих деценија почивала на њеном уништењу. Уништење свих заштитних слојева био је тренутни извор профита, али нас је учинио запањујуће рањивима. Поновно откривање граница отпорности постало је кључно питање националне и међународне безбедности*“* (Lagadec 2012, 368).

Критичне инфраструктуре су од виталног значаја за нормално функционисање друштва и држава, што са друге стране подразумева да поремећаји у њиховом раду, инциденти или несреће могу оставити озбиљне последице по друштво и привреду, те ограничити или онемогућити рад инфраструктуре у дужем или краћем временском периоду. Самим тим, заштита и отпорност критичне инфраструктуре су од кључног значаја за добробит грађана сваке државе. Овај императив се намеће нарочито данас, како услед директних претњи (било оних индукованих климатским и геополитичким променама, или политичком и економском ситуацијом), али ништа мање ни услед индиректних претњи генерисаним све већим умрежавањем и међузависношћу критичних инфраструктура на националном, међународном и глобалном нивоу. Управо ова комплексност и међузависност доводе до све већих стања неизвесности, што је узроковало и померање приступа заштите критичне инфраструктуре од приступа оријентисаног на појединачне претње, преко свеобухватне листе претњи – природних и антропогених (*all hazard approach*), па до приступа оријентисаног ка отпорности система. Критична инфраструктура не само да може бити преферирана мета противправног деловања, подложна климатским промена и непогодама, већ и због својих иманентних особина, те карактеристика организационих система који чине систем критичне инфраструктуре на једној територији, она сâма може бити извор ризика по друштво и државу.

Критичну инфраструктуру у овој дисертацији посматрамо као скуп организација, оператора критичних инфраструктура, које чине међуповезану мрежу, или систем система, критичне инфраструктуре на једној територији. Према Митлтон-Келију, организације као социо-технолошко системи, инхерентно представљају комплексне адаптивне или еволутивне системе (Mittleton-Kelly 2003). Једно од основних својстава комплексних система јесте њихова способност адаптације на промене у окружењу, али и на промене унутар система, те је у литератури све присутнији појам „комплексних адаптивних система“ (КАС). Ово је од изузетног значаја за наш приступ промишљању отпорности критичне инфраструктуре. Наиме, у овој дисертацији адаптацију, посматрамо као један од капацитета отпорности. Поједини аутори блиски овој школи мишљења појам адаптације чак стављају у први план, као својеврстан „надкапацитет“ и поистовећују са отпорношћу. Према Милеру и Пејџу, адаптивно деловање индивидуалних агената удаљава систем од критичног режима функционисања и помера га ка стању равнотеже (Miller & Page 2007, 177).

Осим адаптације, унапређење отпорности организационог система оператера критичне инфраструктуре може се постићи јачањем преосталих капацитета отпорности – антиципативног, ресорпционог и ресторативног. Ови капацитети се у знатној мери подударају са фазама кризног одговора (приправности, одговора и опоравка), међутим у посматрању отпорности сматрамо да би потпуно везивање капацитета за темпоралне фазе (пре, током и после инцидента) могло негативно утицати на њихов експликативни потенцијал, о чему ће више речи бити у теоријском делу дисертације. Ово је нарочито важно уколико посматрамо адаптацију као један континуирани процес, који се одвија у свим фазама одговора на кризу.

Осим врсте неизвесности (квантитативне или квалитативне), природа и јачина инцидента играју велику улогу у способности организација за одговор, адаптацију и опоравак након прекида пословања узрокованог нежељеним догађајем (Riddle 2015, 12; Chaffee 2009). Наиме, одређени екстремни догађаји, као што су терористички напади утичу на физички ограничену територију, док епидемије и пандемије заразних болести могу имати шире и дугорочније последице, које утичу на способност организација и држава да наставе са нормалним функционисањем. Догађаји попут „Мајских поплава“ 2014. године у Србији, те урагана Сенди и Катрина у САД, терористичког напада на „Куле Близнакиње“ 2001. године, девастирања

нуклеарне електране Фукушима препречивања Суецког канала теретног брода „Евер Гивен“ које је пореметило трећину глобалног бродског транспорта, па до глобалне кризе узроковане пандемијом вируса COVID-19 резултирали су штетама које се мере милијардама и билионима долара, психолошким траумама становништва, као и значајним променама у политици и регулативи. Осим објективне јачине утицаја, важно је узети у обзир и перцепцију ризика која такође утиче на способност адекватног одговора организација и њихових запослених.

Отпорност је комплексан и, по много чему, вишезначан појам. Једно од сувислијих питања о отпорности тичу се врсте претњи са којима ће се систем суочити, односно какав је одговор на питање „на шта је систем отпоран“? Ми смо се у овој дисертацији одлучили да одговор контекстуализујемо у домену неизвесности, па смо отпорност система класификовали као отпорност првог реда (отпорност на познате претње или рутинске ризике – квантитативна неизвесност) и отпорност другог реда (отпорност на непознате претње или нерутинске ризике – квалитативна неизвесност).

У досадашњим студијама организационе отпорности, а нарочито оних који се тичу система критичне инфраструктуре присутна је усмереност на такозване „тврде аспекте“ отпорности, а који подразумевају присуство одређених ресурса, структура, имплементираних и сертификованих система менаџмента и документације (политика, планова и процедура). С друге стране когнитивни и бихејвиорални аспекти које, користећи терминологију из аналитичког модела „рибље кости“ (*Herringbone model*) Гибсона и Таранта, називамо „меким аспектима“ отпорности су углавном занемаривани (Gibson and Tarrant 2010). Ти аспекти се тичу менаџерских и комуникационих пракси, као и организационе културе. Како Гибсон и Тарант наводе, тврди аспект односи се на оно „шта се ради“, а меки аспект на оно „како се то ради“. Тврди аспект указивао би на усмереност на отпорност првог реда, док би присуство добре праксе у „меким аспектима“ указивао на усмереност и на постизање отпорности другог реда, то јест отпорности на нерутинске ризике и неизвесности.

У складу са овим, ова дисертација покушаће да примени комбинацију аналитичких модела капацитета отпорности и „рибље кости“ ради креирања новог, композитног аналитичког модела, који би могао да пружи прецизније и свеобухватније сагледавање тврдих и меких аспеката капацитета отпорности. Другим речима, истраживање ће покушати да установи „шта се ради“ и „како се то нешто ради“ у сваком од четири капацитета отпорности у организационим системима оператера критичне инфраструктуре у Републици Србији и суседним државама.

Како је приступ (то јест, стратегија, о чему ће бити речи у теоријском делу рада) отпорности, за разлику од приступа заштите углавном усмерен на догађаје и околности окарактерисане високим степеном неизвесности, у овој дисертацији испитани су утицаји догађаја ниске вероватноће, а високог утицаја који узрокују промене у режиму рада организација (а које у даљем тексту називамо нерутинским ризицима) на способност критичних инфраструктура у Републици Србији и суседним земљама да одговоре на поремећај, прилагоде се новонасталим околностима и наставе са испоруком критичних услуга и добара.

Као студија случаја узета је актуализација нерутинског ризика пандемије коронавируса (COVID-19) Истраживање је обухватило анализу различитих варијабли идентификованих у експертским интервјуима и њихову класификацију у једну од четири капацитета отпорности (антиципације, ресорпције, опоравка и адаптације) и два припадајућа аспекта (меки и тврди). Индикатори су идентификовани у складу са налазима бројних академских студија из области организационе отпорности и кризног менаџмента, узимајући у обзир и најновија истраживања из ових области. Нарочито су узети у обзир индикатори које су предложили Гибсон и Тарант у

свом моделу „рибље кости“, а које називају активностима (тврди аспект) и карактеристикама (меки аспект) (Gibson & Tarrant 2010). Поједини индикатори испитивани су посредно. На пример, индикатор суочавања са стресом идентификован од стране Гибсона и Таранта, посматран је кроз призму истраживачких питања покренутих у докторској дисертацији Лорне Ридл (Riddle 2015).

Први део ове дисертације посвећен је теоријском оквиру. Како би се темељно сагледала проблематика односа термина ризика, отпорности и критичне инфраструктуре потребно је било применити теоријска промишљања из различитих научних дисциплина. Прво потпоглавље овог дела дисертације посвећено је истраживањима о појму, природи, перцепцији и комуницирању ризика која представља основу за две могуће стратегије управљања ризиком – антиципацији (управљању ризиком у традиционалном смислу) и отпорности (управљању неизвесностима). Такође, дато је подробно објашњење термина „нерутински ризик“ и оправдање за његово коришћење у тексту ове дисертације. Друго потпоглавље бави се појмом отпорности отпорношћу, нарочито организационим, когнитивним и бихевиоралним аспектима овог термина. У оквиру овог потпоглавља анализирани су и односи појма организационе отпорности са појмовима кризног менаџмента и менаџмента континуитетом пословања. Треће потпоглавље теоријског дела укључује промишљања термина критичне инфраструктуре, њене заштите и отпорности. Како су заштита и отпорност критичне инфраструктуре препознати као изазови од високог значаја за националну безбедност, осим академских и стручних радова, у овом потпоглављу анализирани су и међународни и национални легислативни и стратегијски документи.

Други део дисертације представља истраживачки део. У њему прво износимо предмет, циљеве и хипотезу, као и методолошки оквир истраживања. Затим се у дисертацији излажу резултати теренског дела истраживања и њихово кодификовање у теоријски оквир, након чега следи дискусија, то јест поређење резултата добијених теренским истраживањем са теоријским оквиром и налазима добијеним из других истраживања спроведених у другим географским, темпоралним и организационим оквирима.

Последњи део ове дисертације представља закључак у оквиру кога се излажу препоруке за практичаре, затим ограничења истраживања, као и препоруке за даље истраживачке напоре.

На крају документа дат је списак коришћене литературе, као и прилози.

1. ТЕОРИЈСКИ ДЕО

Како би се темељно сагледала проблематика односа термина ризика, отпорности и критичне инфраструктуре било је потребно применити постулате теоријских промишљања из различитих научних дисциплина. Тематика је сагледана проблемски, анализом приступа различитих научних дисциплина феноменима ризика, отпорности и критичне инфраструктуре. Прва теоријска основа овог истраживања налази се у филозофским и социолошким изучивањима концепта ризика и неизвесности. Психолошка изучавања перцепције ризика могу расветлити ставове и мишљења људи о различитим типовима ризика као и потенцијалним бихејвиоралним одговорима у случајевима када би људи били изложени одређеном ризику. Литература из примењених научних дисциплина комуникације и управљања ризицима консултована је ради анализе начина којима се комуниколошки и организациони алати могу применити у циљу унапређења антиципације ризика, приправности и одговора на нежељени догађај.

Други кључни термин који је сагледан кроз мултитеоријску призму јесте отпорност. Анализиран је приступ отпорности у психологији, социологији, еколошким, политичким и организационим наукама. Затим је анализиран теоријски појам организационе отпорности као и његова операционализација у пракси кроз различите системе управљања. Како је истраживање капацитета и аспеката отпорности примарни фокус ове докторске дисертације, значајан сегмент теоријског оквира истраживања посвећен је овом проблему и његовој операционализацији у досадашњим истраживањима. Посебна пажња посвећена је адаптационом капацитету, или фази адаптације, као дистинктивног појма у еколошким приступима изучавања отпорности. Приликом изучавања организационе отпорности, нужно је било дотаћи се и теорија о организационом понашању и култури, као и о доношењу одлука које је анализирано и кроз призму теорије система, те постулата динамичког адаптивног планирања. Посебан осврт дат је на међународне стандарде који третирају организациону отпорност и кризни менаџмент, као примере најбоље праксе које се препоручују организацијама у циљу унапређења отпорности и кризног одговора.

Приликом расветљавања појма критичне инфраструктуре, њене заштите и отпорности, неопходно је било анализирати корпус правних и стратешких докумената из разних држава, као и теоријска промишљања из области наука о безбедности и стратешких студија. Напокон, научни напори у концептуализацији и операционализацији феномена отпорности у различитим секторима критичне инфраструктуре – транспорту, енергетици, здравству, финансијама били су предмет посебне пажње у припреми овог истраживања.

1.1. Ризик и управљање ризицима

Речник појмова ИСО 73:2009 ризик дефинише као „ефекат неизвесности на жељене циљеве“ (ISO 73:2009). Исти документ додатно појашњава ову врло широко постављену дефиницију, те наводи да је ефекат позитивно или негативно одступање од очекиваног, а да се ризик изражава као комбинација вероватноће догађаја и последица (Ibid). Према Мартину, безбедносни ризик јесте количина штете која може настати ако се не предузму никакве мере (Martin 2019, 11).

Кључни елемент ризика јесте вероватноћа. Укратко речено, вероватноћа представља могућност наступања одређеног догађаја (Кековић и сар. 2014, 27). Вероватноћа ризичног догађаја се може изразити на два начина, као објективна или као субјективна. Објективна

вероватноћа објашњава дугорочну учесталост неког догађаја, засновану на претпоставкама великог броја посматраних догађаја и непроменљивим условима или се израчунава на основу извршеног експеримента и прикупљених података (Ibid). Субјективна вероватноћа би значила властито уверење или личну процену исхода одређеног догађаја. Она се разликује од појединца до појединца и на њу утичу различити фактори, као што су искуство, старост, интелигенција, образовање и многе друге појединости и специфичности које обележавају појединца (Ibid).

Према Ортвину Рену (Renn 2008) постоје три суштинска елемента ризика. Прво, исход који утиче на оно што људи вреднују; друго, могућност догађаја (неизвесност), и треће, формула за комбиновањем ова два елемента у један појам. Сви постојећи приступи проблему ризика различито концептуализују ова три елемента. У природним и инжењерским наукама термин „ризик“ односи се на функционални однос између вероватноће и последица (Granger Morgan & Henrion 1990; Kolluru & Brooks 1995). У психологији, ризик се посматра као функција субјективно очекиваних корисности (Slovic et al. 1981). Културно и друштвено разумевање ризика усмерено је на менталне моделе према којима различите друштвене и културне групе приписују значење искуству штете и хазарда (Breakwell 2007).

Менаџмент ризиком је последњих деценија једна од најважнијих активности у корпоративној пракси. Готово да се не може замислити пословни систем који нема формализоване процедуре за идентификацију, процену, приоритизацију и управљање ризиком. Најбоља пракса менаџмента ризиком формализована је у међународним и националним стандардима од којих је свакако најпопуларнији и најзначајнији ИСО 31000. Методологија процене ризика усаглашена са ИСО стандардима 31000 и ИСО/ИЕЦ 31010:2019 (Менаџмент ризиком – Технике за процену ризика) примењиване су за процену пандемијског ризика, али и за хипотетичке пандемије и друге нерутинске ризике (Ewertowski & Butlewski 2021; Boldog et al. 2020; Chakraborty & Gosh, 2020).

Менаџмент ризиком најуспешнији и најефикаснији је онда када имамо на располагању поуздане податке о вероватноћи настајања нежељеног догађаја и последица његове актуализације. Што мање података имамо о тим варијаблама, процена ризика је непоузданија и повећава се могућност доношења неадекватних мера управљања ризиком, као и њихова економска оправданост. Другим речима, из домена ризика улазимо у домен неизвесности. Неизвесност је поменути ИСО речник појмова дефинисао као стање чак и делимичног недостатка информација, разумевања и знања у вези са догађајем, његовом последицом и вероватноћом (ИСО 73:2009). Неизвесност захтева интуитивно закључивање које је пре свега засновано на искуству, а мање на аналитици. Алесандри и сар. су установили да у околностима ризика, доносиоци одлука обично користе аналитички и квантитативни приступ у циљу доношења одлуке, док су у околностима неизвесности примењивали квалитативне и интуитивне процесе (Alessandri et al. 2004).

Многи аутори оспоравају могућност ефикасне примене техника и стратегија менаџмента ризиком на стања неизвесности (Wildawsky 1989; Taleb 2009; Aven 2011; Fjaeder 2014; Pate-Cornell 2014; Gibson & Tarrant 2020). С друге стране, Бојн и 't Харт истичу да већини „природних несрећа или насилних конфликата претходи период инкубације током којег креатори политика погрешно интерпретирају, игноришу предстојеће опасности“ (Boin & t'Hart 2003, 546). Сорнетова теорија о неочекиваним, али ипак предвидивим, догађајима „краљевима змајевима“ (Sornette 2009), као и теорија о „сивим носорозима“ (Wucker 2016) на трагу су ове тезе Бојна и 't Харта.

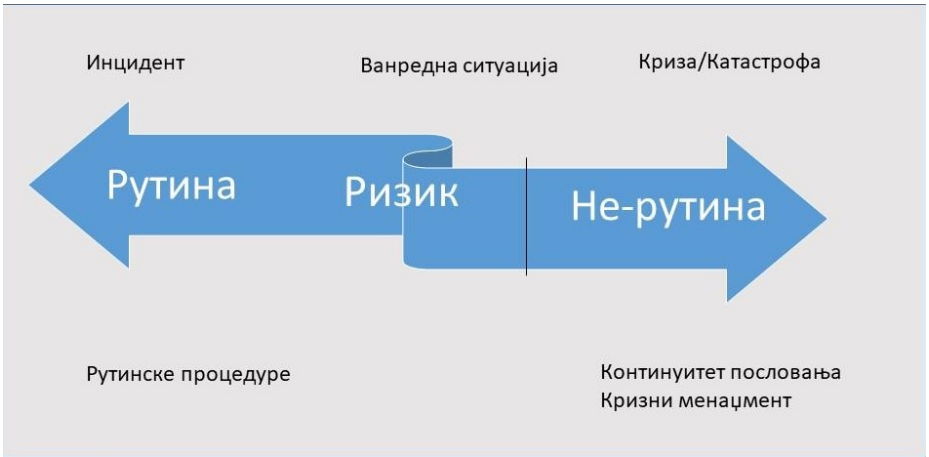
Класични приступа менаџмента ризиком у смислу идентификације претњи, процене вероватноће настајања нежељеног догађаја и јачине утицаја или последица, те оцене и приоритизације ризика и одређивања мера за управљање тим ризицима уважавајући анализу „цена-корисност“, Арон Вилдавски назива антиципаторном стратегијом. „*Антиципација је модус контроле коју врши централизовани ум; улаже се труд да се предвиди и спречи потенцијална опасност пре него што се штета начини*“ (Wildawsky 1991, 77). Према Вилдавском овај приступ има смисла уколико можемо да извршимо прецизну процену ризика, тј. вероватноће настајања нежељеног догађаја и последица. Вилдавски сматра да се у случајевима када немамо довољно података, проактивни, антиципаторни приступ може причинити више штете него користи, те да је у тим случајевима чак боље не чинити ништа. Да би била успешна, антиципација се мора вршити у окружењу које одликује стабилност и ниска варијанца, односно ниска неизвесност о будућности, другим речима када се пројекције на основу историјских података могу тачно извести (Ibid, 79). Као примере оваквих ризика можемо навести повреде на раду, пожаре, имовински криминалитет у одређеном окружењу, престанак рада техничких средстава усред дотрајалости или нестанка електричне енергије итд. Да би се донела одлука да је антиципација стратегија избора, потребно је показати да су највећи ризици са којима се сусрећемо они који се могу предвидети са великом вероватноћом (Ibid, 80). Напокон, у примени антиципаторне стратегије, морају се узети у обзир трошкови њене примене, ако покушамо да је применимо на све идентификоване ризике, цена би била превелика за било који систем (Ibid, 85). За неизвесности као и ризике са ниском вероватноћом али високим последицама (које ћемо у даљем тексту називати нерутинским ризицима), друга могућа стратегија управљања ризиком – отпорност, би, према Вилдавском, требало да буде стратегија избора.

Напокон, према Дејвиду Рубенсу, менаџмент ризиком може се посматрати и као поддисциплина футурологије, будући да се не заснива само на идентификацији постојећих претњи, већ пре свега на што прецизнијим промишљањима са каквим се будућим претњама можемо суочити (Rubens 2023, 11).

1.1.2. Нерутински ризик

Нерутински ризик је термин који се већ деценијама користи у академској и стручној литератури за означавање оних ризика које карактеришу ниска вероватноћа, или ниска предвидљивост, а изузетно високе последице. Термин је, према истраживању извора, први пут употребљен у зборнику „Управљање неизвесностима“ (Management of Uncertainty) Вилкина и Сатона из 1986. године (Wilkin & Sutton 1986), док се конструкције попут нерутинских догађаја могу наћи још у извештајима Нуклеарне регулаторне комисије САД из седамдесетих година прошлог века (U.S. Nuclear Regulatory Comission 1975). Иначе, термин је конструисан по аналогији са нерутинским проблемима у математици, које карактерише могућност више тачних одговора, процедуре које на први поглед нису довољно јасне, а чије решавање захтева креативност и иновативно размишљање (Polua 1957).

Велики допринос у савременом промишљању овог проблема дао је Мајкл Тарант. Према Таранту, појава нерутинских ризика наводи организације да предузимају нерутинске активности како би дале адекватан одговор (Tarrant 2010). Менаџмент ризика у нерутинском контексту разликује се од менаџмента рутинским ризицима. Нерутински део спектра ризика укључује оне ризике који имају потенцијал да значајно измене начин на који организација функционише, то јест да је приморају на функционисање у нерутинском моду. (Ibid) Графички се то може приказати на следећи начин:



Графикон 1. Приступи управљања ризиком (Нинковић, 2019; према Tarrant, 2010)

Дакле, на једном крају континуума налазе се уобичајени ризици нижег интензитета којима се управља кроз рутинске процесе, док су на другом крају катастрофални ризици. Можемо приметити да актуализација оваквих ризика одговара ономе што Насим Талеб назива статистичка дистрибуција „дебелих репова“ (fat-tail distribution), која одступа од стандардне гаусовске криве. Наиме, крај нормалне криве је неочекивано „дебео“ у поређењу са нормалном дистрибуцијом, што указује на високу вероватноћу катастрофалних догађаја. Талеб закључује да „ *у дистрибуцији „дебелих репова“, екстремни догађаји удаљени од центра криве играју веома велику улогу. Црни лабудови нису чешћи, али носе знатно веће последице*“ (Талеб 2019,8).

Нерутински ризици могу бити идентификовани, тј. могу фигурирати у регистру ризика, дакле они нису једнаки епистемиолошким неизвесностима. Праг који раздваја рутинске од нерутинских ризика дефинисан је променама у функционисању система, а не апсолутним вредностима. Једна ситуација у малој организацији може узроковати њено функционисање у нерутинском моду, док за велики систем та ситуација може представљати мањи инцидент који се може решити применом рутинских процедура.

Према Бировој и сарадницима (Bier et al. 1999, 17)[1] учестали догађаји налазе се унутар нормалног спектра искуства, те је за њих систем већ развио механизме одбране, премда се они могу разликовати од организације до организације. Нерутински ризици постављају више проблема пред доносиоце одлука. Прво, озбиљност последица може организацији отежати суочавање са тим догађајима када се јаве. Услед њихове реткости, организационо учење о тим догађајима је отежано – било да се учи из личног искуства, било из секундарних извора. При том, људи, технички системи и организације могу се понашати другачије приликом ретких, нерутинских догађаја него у нормалним околностима, а то понашање се неће увек правилно предвидети. Коначно , и када екстремни догађаји нису карактерисани високим нивоом статистичке неизвесности, могу бити тешки за разумевање и стављање у перспективу услед озбиљности њихових последица и непостојања личног искуства (Bier 2018, 17).

[1] Неки аутори (Bier, Haimes, Lambert, Mathalas & Zimmerman 1999; Cox and Bier 2018; Goble 2018) користе термин „екстремни“ ризици за означавање оних ризика који изазивају екстремне последице, а ретко се јављају. Међутим, овај термин је у колизији са терминологијом ИСО/ИЕЦ Стандарда 31010 и техником матрице последица/вероватноћа. Наиме , према овој методологији, преузетој и у српском стандарду СРПС. А .Л .2 .003 - Процена Ризика, да би се ризик окарактерисао као екстремни, производ вероватноће и последица мора бити изнад 20, што значи да и вероватноћа и последице морају бити, у најмању руку, врло високе (СРПС А.L2.003:2017).

Тарант примећује пораст интересовања за организационе одговоре на нерутинске ризике које се у пракси огледа у повишеној важности које се у организацијама дају приступима попут организационе отпорности, континуитетом пословања и кризног менаџмента и комуницирања (Tarrant 2010, 16). Тарант сматра да кризни планови и планови континуитета пословања управо служе као припрема за ефикасно функционисање организације у нерутинском моду (Ibid).

Фундаментални изазов за организације јесте како да се прилагоде измењеном окружењу уз одржавање кључних функција. Ипак, у случајевима екстерних шокова тешко је очекивати да ће то прилагођавање тећи у савршеном реду. Нерутински ризици генеришу услове у којима организације и заинтересоване стране морају радити заједно на нерутински начин. Распон задатака, циљева и радног окружења може бити значајно различит од свакодневних услова. „*Од виталног је значаја да особе укључене у одговор имају довољно прилике у фази планирања да успоставе ефикасне односе са оним особама са којима ће их ванредно стање довести у додир, како унутар, тако и изван организације*“ (Crichton, Ramsay & Kelly 2009, 33).

Иако излази изван оквира овог истраживања треба напоменути да организације морају имати свест да ће током криза и катастрофа изазваних нерутинским ризицима, очекивања јавности и њена толеранција на ризик бити измењена у односу на редовне околности. Тзв. „Блекетов извештај“, написан на захтев Кабинета Премијера и Министарства одбране Велике Британије из 2012, ради анализе најбољих приступа за идентификовање, анализу и управљање нерутинским ризицима, истиче следеће: „Код многих ризика који могу резултирати високим последицама ми не разумемо шта јавност заправо очекује у случају њихове актуализације, нити колико може бити толерантна на 'абнормалне' ризике током криза. Истраживање тих питања може помоћи приликом одлучивања о комуницирању тих ризика према јавности“ (Blackett Review 2012). Водећи се налазима истраживања Ридлове (Riddle 2015), можемо констатовати да ће се у случају нерутинских, „абнормалних“ ризика запослени понашати као „општа јавност“, јер ће се у слућају да не добију веродостојне информације од својих организација, информисати преко средстава јавног информисања и друштвеног мрежа.

Водећи се овим коментаром и чињеницом да организације често не планирају одговоре на догађаје ниске вероватноће, можемо закључити да је укључивање запослених у планирање организационих одговора, те разумевање одговора запослених као и њихових очекивања у случају актуализације нерутинских ризика од великог значаја за отпорност и безбедност како критичних инфраструктура, па тако последично и за националну безбедност.

1.1.1. Перцепција и комуникација ризика

Процес идентификације претњи, сачињавање регистра ризика, те њихова приоритизација у великој мери зависи од перцепције ризика доносиоца одлука, нарочито када је реч о нерутинским ризицима. Перцепција ризика укључује људска веровања, ставове, судове и осећања, као и шире друштвене или културне вредности и диспозиције које људи усвајају према хазардима и користима које од њих могу добити (Pidgeon 1992, 89)[2]. У неким околностима,важни аспекти перцепције и прихватљивости ризика укључују расуђивања не само о физичким карактеристикама и последицама неке активности, већ и о друштвеним и организационим факторима, као што су кредибилитет и веродостојност извора информација, доносиоца одлука у организацијама и надлежних институција (Кешетовић, Кековић & Нинковић 2009).

[2] Перцепција или опажање у овом смислу има шире значење од уобичајеног које се ограничава на „сазнање спољашње средине путем чула“ (Видановић 2006).

Према Стару, перцепција ризика може бити условљена степеном до којег се сматра да је ризик узрокован самим субјектом, односно спољним утицајем ван његове контроле (Starr 1969). Старови налази наишли су на широку примену у каснијим истраживањима који су их даље продубили. Фон Винтерфелт и сарадници установили су да се ризици које одликује ниска вероватноћа и високе последице обично перципирају као веће претње него ризици са вишом вероватноћом а средњим последицама (von Winterfeldt, John & Borcherding 1981). Затим, према Рену, главне контекстуалне варијабле које утичу на перципирану озбиљност ризика су веровања о узроку ризика и потенцијал за катастрофу (Renn 1992, 65). Извештај британског Краљевског друштва из 1992. године сумирао је, на основу до тада објављених студија, једанаест „негативних хазардних атрибута“ који могу утицати на људску перцепцију ризика (Report of a Royal Society Study Group 1992, 101).

У студији Бернса и Словика, терористички напад биолошким оружјем (вирусом антракса) заузео је прво место на листи од деведесет шест сценарија, који су се разликовали по домену (тероризам – остало), механизму (извору ризика – нпр. антракс, резервоар пропана), мети (званичници – „обични људи“), намери (намеран-ненамеран), што даље потврђује раније претпоставке и негативне атрибуте хазарда (Burns & Slovic 2009). Ипак , треба узети у обзир и историјски моменат Бернсове и Словикове студије, будући да је писана у тренутку када су сећања на панику изазвану слањем писама у којима се налазио вирус антракса и даље била свежа (Demidov 2002, Fahmy & Johnson 2007, Mason & Lyons 2003, Glass & Schoch-Spana 2002).

Дакле, узевши у обзир наведене студије, теорија нас наводи на закључак да се одређени нерутински ризици високо котирају на лествици неприхватљивости.

Осим ставова јавности, тј. „лаика“, за ово истраживање значајни су ставови доносилаца одлука и стручњака у области безбедности и управљању ризицима. Наиме, уврежена је претпоставка да се једино лаици руководе хеуристикама, тј. „пречицама “ приликом процене ризика, односно хазарда, међутим ни експертске процене ни у ком случају нису имуне на субјективна расуђивања. Расуђивање се може јавити у одабиру индекса ризика, у процени последица и неизвесности, као и у почетном структурисању проблема. Претпоставке експерата су често опште раширене у одређеној научној или експертској заједници, пошто су њени чланови изложени заједничком корпусу усвојеног знања и сличним методама обуке (Кешетовић, Кековић и Нинковић 2009, 550-551).

У контексту овог истраживања, претпоставка је да лаичка јавност, односно запослени који нису укључени у планирање одговора на ризик и кризу и планирање континуитета пословања, сасвим легитимно може желети да сазна више о хазардима којима су окружени, нарочито уколико су ти хазарди окарактерисани неким од горепоменутих хазардних атрибута. С друге стране, менаџери корпоративне безбедности, континуитета пословања и други доносиоци одлука, такође могу имати погрешне претпоставке о ризицима, али и о перцепцијама ризика својих запослених.

За ово истраживање најважнија је била стратегија доношења одлука која се назива хеуристика заснована на доступности (Kahneman & Tversky 1973). У овој стратегији, процена ризика условљена је лакоћом побуђивања примера из дуготрајне меморије. Менаџери и други доносиоци одлука могу преценити вероватноћу одређеног догађаја који је тренутно доступан у медијима или уочљив. С друге стране, вероватноће догађаја за које не постоји тренутно доступан пример, или је сећање на пример далеко, могу бити потцењене (Simola 2005). Лично искуство доносиоца одлуке са одређеним догађајем је такође од велике важности за његову доступност (Dunaway 2010, 52).

Такође, очекивана вероватноћа такође утиче на закључивање и доношење одлука. Према теорији изгледа (енг. Cumulative Prospect Theory; Tversky & Kahneman 1992), вероватноће 0 и 1 се опажају објективно, док се ниске вероватноће прецењују или занемарују. Вероватноћа ретког догађаја који је лако доступан нашем уму ће бити прецењена, док ће вероватноћа ретког догађаја који није „засићен“ у нашем уму бити игнорисана. Средње и високе вероватноће ће, пак, бити потцењене. Идентификације могућих претњи као и њихове вероватноће могу бити условљене личним искуством, корпоративном историјом, или упозорењима и алармима (нарочито када је реч о лажним узбунама).

Релевантност хеуристике засноване на доступности и теорије изгледа за ову дисертацију огледа се у њиховој примени на процесе одлучивања менаџера безбедности, континуитета пословања и других доносиоца одлука у идентификацији ризика, сачињавању регистра ризика и њиховој приоритизацији. Ово је значајно за анализу антиципаторног капацитета отпорности организације критичне инфраструктуре, о чему ће даље бити речи у поглављу о капацитетима отпорности.

Бројне студије су показале да негативни атрибути хазарда могу бити ублажени адекватном комуникацијом ризика. Према Бороџичу, у сфери управљања ризицима, допринос комуникације ризика треба да буде смештен у контекст смањења друштвених конфликата кроз процес међусобног разумевања и уважавања мишљења (Borodzicz 2001, 135). Проучавање и пракса комуникације ризика треба да у обзир узме различите перцепције ризика и тиме фундаментално смањи могућност настајања конфликта. Четири кључна аспекта за постизање овог циља су: информисање и едукација, утицање на промену понашања, обезбеђивање упутстава приликом инцидената и обезбеђивање решења конфликата (Ibid). Главна сврха комуникације решења није да произведе неко свеважеће решење, већ да унапреди дијалог и сарадњу успостављањем заједничких циљева за људе са различитим очекивањима (Кешетовић , Кековић и Нинковић 2009, 525).

Организације често праве претпоставке о понашању запослених током и након екстремних догађаја, слично као и владе и хитне службе о понашању грађана. Роџерс и Пирс истичу да је неповерење јавности према ауторитетима делимично резултат задржавања информација према јавности у протеклим инцидентима (Rogers & Pearce 2011). Могући разлог за овакво поступање јесте што надлежне особе формулишу материјале за комуникацију ризика под претпоставком да би потпуно упознавање са ситуацијом изазвало панику у јавности, а што је претпоставка која је данас оповргнута у литератури. Наиме, студије потврђују да јавност није склона паници у ванредним ситуацијама (Drury, Cocking & Reichel 2009a; Drury, Cocking & Reichel 2009b; Sheppard, Rubin, Waldman & Wessely 2006). Подаци прикупљени од особа са личним искуством ни у којем случају не поткрепљују тезу о „масовној паници“, а учесталост антисоцијалног понашања је веома ретка (Sheppard et al. 2006; Drury et al. 2009a). Штавише, истраживања показују да људи показују алтруистичне реакције чак и према потпуним странцима, и то у ситуацијама опасним по живот (Cocking, Drury & Reichel 2009).

Упркос оваквим налазима, у литератури је забележено да хитне службе често полазе од погрешне претпоставке да ће јавност паничити у ванредним ситуацијама и да неће пратити упутства (Carter, Drury, Rubin, Williams & Amlot 2014; Pearce, Rogers, Rubin & Wessely 2011). Ове нетачне претпоставке утичу негативно на кризно планирање и комуницирање, тј. непружање свих потребних информација може резултирати неефикасним одговором (Rogers & Pearce 2011). Ови налази имају импликације за начин на које организације комуницирају са својим запосленима током ектремних догађаја. Ускраћивање информација од стране организација према својим запосленим и другим заинтересованим странама може довести до

мање ефикасног одговора као и до губитка поверења и статуса поузданог извора информација (Riddle 2015, 38). Према Друрију у ванредним ситуацијама особе би требало да имају што тачније информације како би што боље реаговале на претњу (Drury 2009). Ови савети иду насупрот традиционалним уверењима да људи под стресом недовољно добро процесуирају информације, те да би ускраћивање информација утицало на смањење стреса и омогућило им да ефикасније реагују. Претпоставка, коју је Ридл потврдила у својој докторској дисертацији, да би искрено и прецизно извештавање запослених о озбиљном инциденту, нарочито о оном који је окарактерисан негативним атрибутима хазарда, као што су непостојање личног искуства с ризиком и тешкоће у поимању изложености и будућих ефеката ризика, (нпр напади биолошким агенсима), могло повољно утицати на спремност запослених да дођу на посао и тиме у знатној мери унапреде континуитет пословања, а у случају критичних инфраструктура и позитивно утичу на националну безбедност и отпорност (Riddle 2015). Ридл је такође идентификовала утицај различитих извора информисања на перцепције и понашање запослених, као и друге факторе који утичу на њихове потенцијалне бихевиоралне одговоре: веровања о озбиљности претње, и веровање о њиховој могућности да учине нешто што би их заштитило од те претње (Ibid).

Један од модела који је примењиван у досадашњим истраживањима перцепције ризика и одговорима на ризик јесте Проширени модел паралелних процеса (ПМПП). Овај модел је примењен у више студија које су проучавале како перцепција претњи и ефикасности здравствених установа може утицати на њихову спремност за рад током пандемије грипа (Witte 1992; Barnet et al. 2009; Balicer et al. 2010; Barnet et al. 2010). Модел сугерише да када појединци уоче претњу, они процењују 'перципирану озбиљност', која је њихово уверење о озбиљности претње и 'перципирану подложност', што је њихово веровање о њиховим сопственим шансама да доживе претњу (Witte 1992). Ефикасност у оквиру овог модела је сложен концепт који се дели на „уочену ефикасност одговора“, што је веровање појединца да ли одговор може спречити претњу, и „перципирану самоефикасност“, што је веровање у њихову сопствену способност да примене препоручени одговор.

ПМПП је првобитно замишљен као теорија која објашњава зашто нека упозорења на претње не успевају; било када упозорења не изазивају жељено здравствено понашање у јавности или када јавност једноставно одбија поруке (Riddle 2015,40). Према ПМПП, када особа верује да је претња озбиљна и да их лично угрожава, страх ће је мотивисати на акцију (Witte & Allen 2000). Ипак, вероватноћа да ће предузети одређену акцију зависи од тога да ли сами верују да су способни да је предузму. Ако сматрају да нису способни да предузму одговарајуће деловање или да ће оно бити неефикасно, тада је вероватније да ће покушати да контролишу страх путем стратегија превладавања као што су негација (тј. веровање да претња неће баш њих задесити), избегавање (тј. особа ће избегавати да мисли о претњи јер јој је превише застрашујућа) или реактивна формација (нпр. особа може игнорисати званично упозорење услед веровања да је манипулисана) (Ibid). У студији из 2009. године, Барнет и сар. су показали да су локални здравствени радници који су перципирали опасност од пандемије као високу, као и своју ефикасност, били значајно спремнији да пруже одговор на пандемију грипа него они који су опасност и своју ефикасност препознали као ниску (Barnet et al 2009). Аутори истичу да је ефикасност одговора чак јачи предиктор спремности него јачина претње, а неке студије чак напомињу да перципирана јачина претње није значајан предиктор спремности (Balicer et al. 2010).

Теоријски постулати утемељени у перцепцији ризика у овој дисертацији послужили су за одабир сценарија екстремних догађаја насталих актуализацијом нерутинских ризика, то јест

пандемије. Претпоставка је да услед недостатка личног искуства и корпоративне историје суочавања са овим ризиком, ова претња није идентификована или је врло ниско приоритизована пре избијања пандемије, те самим тим кризни планови и планови континуитета пословања нису третирали овај сценарио који је узроковао глобалне последице и највећи број организација приморао на функционисање у нерутинском режиму пословања. Пропусти у идентификацији и приоритизацији ризика указују на недостатке у антиципаторном капацитету отпорности организације.

Комуникација ризика утиче на све фазе, односно капацитете отпорности. Приликом антиципације неопходно је комуницирати оправданост укључивања идентификоване претње у регистар ризика, како би се извршила квалитетна приоритизација, те самим тим обезбедили ресурси за третман ризика. Приликом ресорпције, адаптације и опоравка нужна је двосмерна комуникација са доносиоцима одлука и запосленима како би се пружио адекватан одговор, обезбедили ресурси за опоравак и прихватили аранжмани о функционисању у нерутинском режима, а у складу са измењеним окружењем.

У складу са ПМПП теоријом, квалитет одговора запослених, а нарочито спремност за извршавање радних задатака у околностима неизвесности и повишеног ризика, зависиће од њихове сопствене перципиране способности за извршавање задатака као и од уверења у ефикасност организационог одговора. У овом истраживању имплицитно смо повезали квалитет одговора запослених са присуством на радним местима током пандемије вируса COVID-19. Квалитет одговора запослених од значаја је за ресорпциону и ресторациону фазу, односно капацитет, отпорности критичне инфраструктуре.

1.2. Отпорност

1.2.1. ***Појам отпорности***

Последњих деценија отпорност[3] је постала свеприсутан термин у академском и професионалном дискурсу. Вокер и Купер примећују да се пролиферација коришћења овог термина јавља од оснивања Министарства за отаџбинску безбедност САД и њихове Националне стратегије отаџбинске безбедности 2002. године (Walker & Cooper 2011). Према Гибсону, примена термина „отпорност“ учестала је у поводу глобалне финансијске кризе када је велики број организација настојао да осмисли оквир за превазилажење перципираних заблуда стандардних менаџерских алата, попут менаџмента ризиком и менаџмента континуитетом пословања (Gibson 2020, 1). Дакле, популарност овог термина може се приписати имплицитном или експлицитном препознавању недостатака традиционалних приступа заштите , превенције и пробабилистичке процене ризика. С друге стране, поглед на друштво и природу као системе који теже равнотежи замењен је динамичким погледом који наглашава комплексне, не-линеарне односе између јединица које се налазе у стању континуиране промене и система који се суочава са дисконтинуитетима и неизвесностима (Dahlman 2011).

Сам термин отпорност, „резилијентност“, изведен је од латинског глагола resilire који значи „скочити уназад“. Ране студије овог феномена, према којима систем „ускаче“ у стање равнотеже које је заузимао пре поремећаја, повезивале су отпорност са стабилношћу и

[3]Постоје несугласице око адекватног превода термина „resilience“ на српски језик. Два најприхваћенија су „отпорност“ и „резилијентност“, од којих аутор овог текста даје предност првом, у складу са терминологијом српских стандарда.

капацитетом за симултану апсорпцију шока и одржавање виталних функција. Доцније се термину придодаје значење способности система да се суочи и адаптира на промену (Fraccascia, Giannoccaro & Albino 2018).

Популарност овог вишезначног термина узроковала је и велики број покушаја за дефинисањем концепта „отпорности“ у академској и стручној литератури, као и у званичним законским и стратешким документима. Отпорност се у дефиницијама посматра као капацитет, тј. својство система, процес којим се „оснажује“ систем, али и као стратегија за управљање ризицима. Преглед дефиниција дат је у табели бр. 1.:

Табела 1: Преглед дефиниција отпорности из постојеће литературе

Аутор	Година	Дефиниција	Капацитет / процес / стратегија	Рутински/нерутински ризици (отпорност првог или другог реда)	Антиципаторни	Ресорпциони	Реституциони	Адаптациони
Холинг	1973	Мера издржљивости система и способност за ресорпцију промене и поремећаја уз задржавање истих односа између популација или варијабли система.	Капацитет	Оба	Не	Да	Да	Да
Вилдавски	1985	Капацитет за суочавање са неантиципираним опасностима након њихове манифестације	Стратегија и капацитет	Нерутински	Не	Да	Да	Да
Мастен и сар.	1990	Процес, капацитет за или исход успешне адаптације упркос изазовима или претећим околностима.	Процес и капацитет	Оба	Не	Не	Не	Да
Тилман и Даунинг	1994	Брзина којом се систем враћа у јединствену тачку равнотеже након поремећаја.	Процес	Оба	Не	Да	Да	Не
Хорн и Ор	1998	Фундаментално својство за продуктивни одговор на значајну промену која ремети очекивани след догађаја не укључујући продужени временски период регресивног понашања.	Капацитет	Оба	Не	Да	Да	Не
Гундерсон	2000	Магнитуда поремећаја коју систем може да ресорбује пре него што му се структура редефинише променама варијабли и процеса који	Капацитет	Оба	Не	Да	Не	Не

		контролишу његово понашање						
Патон и сар.	2000	Отпорност описује активни процес самопотврђивања, научене сналажљивости и раста. Концепт се односи на способност функционисања на вишем психолошком нивоу узимајући у обзир индивидуалне способности и претходно искуство.	Процес	/	Не	Да	Да	Да
Карпентер и сар.	2001	Магнитуда поремећаја коју систем може да толерише пре него што се пребаци у друго стање које је контролисано другим сетом процеса.	Капацитет	Оба	Не	Да	Да	Не
Вокер и сар.	2002.	Способност за одржавање функционалности система приликом поремећаја или способност одржавања елемената потребних за обнављање или реорганизацију система уколико поремећај измени структуру функције система	Капацитет	Оба	Не	Да	Да	Да
Бруно и сар.	2003	Способност друштвених јединица за умањење хазарда, задржавање ефеката катастрофа када се десе и извршавање активности опоравка које минимизирају друштвене поремећаје и умањују ефекте будућих земљотреса.	Капацитет	Оба	Не	Да	Да	Не
Хамел и Валикангас	2003	Отпорност се односи на капацитет за континуирану реконструкцију	Капацитет	Оба	Не	Не	Не	Да
Вокер и сар.	2003	Капацитет система за ресорпцију поремећаја и реорганизовање приликом промена а задржавајући исту функцију, структуру, идентитет и повратне спреге	Капацитет	Оба	Не	Да	Да	Да
IRGC	2005	Нормативни циљ система	Стратегија +	Нерутински	Не	Да	Да	Да

		управљања ризиком за третирање неизвесности и изненађења. Својство система који ресорбују ризик да би издржали поремећај (објективна отпорност), али и поверење актера управљања ризиком да су у стању да савладају кризне ситуације (субјективна отпорност).	капацитет					
Холнагел и сар.	2006	Способност за предосећање, препознавање, адаптирање и ресорбовање варијација, промена, поремећаја, дисрупција и изненађења.	Капацитет	Оба	Да	Да	Не	Да
Мекдоналд	2006	Отпорност садржи својства способности за адаптирање на захтеве окружења и способности да се управља различитостима у окружењу	Капацитет	/	Не	Не	Не	Да
NIAC	2009	Способност за редукцију јачине и/или трајања реметилачких догађаја. Ефикасност отпорности инфраструктуре или организације зависи од њихове способности да предвиде, ресорбују, адаптирају се и/или брзо се опораве од потенцијално реметилачког догађаја	Капацитет	Оба	Да	Да	Да	Да
Лонгстаф и сар.	2010.	Капацитет система за ресорбовање поремећаја и промене уз задржавање истих есенцијалних функција, структуре, идентитета и повратних веза.	Капацитет	Оба	Не	Да	Не	Да
Линенлуке и Грифитс	2010	Способност за ресорбовање утицаја и опоравак	Капацитет	Оба	Не	Да	Да	Не
DHS	2010a	Способност система, инфраструктуре, владе, пословних организација и грађана да се одупру, ресорбују,	Капацитет	Оба	Не	Да	Да	Да

		опораве се или адаптирају на негативни догађај који може проузроковати штету, уништење или губитак од националног значаја						
DHS	2010б	Капацитет организације да препозна претње и хазарде и прилагоди им се у циљу унапређења будућих напора за заштитом и мера редукције ризика	Капацитет	Оба	Да	Не	Не	Да
УК Стратегија националне безбедности	2010	Способност за прилагођавање измењеним околностима и приправност за одбијање и брз опоравак након ремећења	Капацитет	Оба	Да	Да	Да	Да
US Quadrennial Defense Review Report	2010	Робусност, прилагодљивост и капацитет за брз опоравак	Капацитет	/	Не	Да	Да	Да
Бојн, Комфорт и Демчак	2010	Капацитет друштвеног система (организације, града или заједнице) да се проактивно прилагоди и опорави након поремећаја који су унутар система препознати као поремећаји који су ван домета нормалног и очекиваног ремећења	Капацитет	Нерутински	Не	Да	Да	Да
Баум	2015	Оквир за управљање системским ризицима и онима које је немогуће квантификовати путем повећања способности система да задржи критичну функционалност ресорбујући поремећај, прилагођавајући му се или се лако опорављајући	Стратегија	Нерутински	Не	Да	Да	Да
ИСО 22316	2015	Организациона отпорност је исход адаптивног капацитета организације у комплексном и променљивом окружењу. Организације са вишим нивоима отпорности имају капацитет да антиципирају и	Капацитет	Оба	Да	Да	Не	Да

		одговоре на претње и прилике и да се измене у условима неизвесности како би постигле своје стратешке и операционе циљеве						
АСИС ОРМ-1	2017	Ресорптивни и адаптивни капацитет организације у комплексном и променљивом окружењу	Капацитет	Оба	Не	Да	Не	Да
Директива 2022/2557/ ЕК		Способност критичног ентитета да спречи, заштити, реагује, одупре се, ублажи, апсорбује, прилагоди и опорави се од инцидента.	Капацитет	Оба	Да	Да	Да	Да

Како Шо и Мејторн наводе, у постојећим дефиницијама постоји контраст између оних дефиниција које су усмерене на опоравак и оних усмерених на адаптацију (Shaw & Maythorn 2013). У приступу отпорности усмереном на опоравак, фокус је на отпор ка спољним утицајима и ефикасан повратак на стање пре поремећаја у што краћем року. У приступу усмереном на адаптацију полази се од тога да утицај ремећења може да буде већи него што постојеће структуре могу да издрже, те је у случају немогућности да се утицај ресорбује, систем приморан на адаптацију (Shaw & Theobald 2011).

Сличну дистинкцију уочава и Пол Мартин, за кога су усмереност на опоравак и усмереност на адаптацију два облика отпорности – пасиван и активан. Пасивна отпорност је способност за ресорпцију поремећаја, опоравак и повратак у нормални режим функционисања. Пасивна отпорност је усмерена на умањење утицаја реметилачког догађаја или напада смањивањем обима или трајања његових негативних последица (Martin 2019, 76). Активна отпорност је према Мартину једнака Талебовом концепту „Антикрхкости“ (Taleb 2019). Наиме она означава јачање система путем учења и извлачења поука из нежељених догађаја и унапређивање спремности на будуће поремећаје (Ibid).

Према Бамри и сарадницима (Bhamra et al. 2011, 7) литература о отпорности може бити широко класификована у три опште области које корелирају са елементима отпорности које су идентификовали Пономаров и Холкомб (Ponomarov & Holcomb 2009):

- Спремност и приправност;
- Одговор и адаптација;
- Опоравак или прилагођавање.

Следеће важно питање које се поставља када се говори о, не само организационој, отпорности јесте отпорност на шта? (Martin-Breen & Anderies 2011). Да ли је систем отпоран или не генерално закључујемо из суда да је систем опстао, или је чак ојачао, упркос отежавајућим околностима који су представљали претњу по позитиван исход (Sutcliffe & Vogus 2003). Бојн, Комфорт и Демчак се питају о интензитету нежељеног, реметилачког догађаја или хроничне претње: да ли је отпорност капацитет за суочавање са ретким, потенцијално катастрофалним

догађајима, или је то капацитет за адресирање много ширег дијапазона поремећаја и дисрупција који се налазе ван оквира поремећаја за које је систем предвиђен да пружи одговор (Boin, Comfort & Demchak 2010, 8).

Напокон, долазимо до онога што Бојн, Комфорт и Демчак називају „моментом отпорности“ (Ibid, 7). То јест, да ли отпорност долази пре или после почетка нежељеног догађаја? Према Бојну и сар. ако отпорност посматрамо као исход, у складу са перспективом посматрања кризе-као-догађаја[4], онда би природно отпорност наступила након догађаја, а њена основна одлика била би способност опоравка. С друге стране, ако отпорност посматрамо као процес, у складу са концептом кризе-као-процеса, отпорност би временски била смештена у ранији период (Ibid 2010, 8).

Услед усмерености овог истраживања на нерутинске ризике, који се одликују потенцијално изузетно високим, екстремним утицајима, од значаја је и примена концепта отпорности у управљању катастрофама. Велики допринос развоју концепта у овој сфери дао је проф. Слободан Симоновић. Према проф. Симоновићу, отпорност представља „способност система и његових компонената да антиципирају, ресорбују, прилагоде или опораве се од ефеката хазардног догађаја у кратком року и на ефикасан начин, укључујући очување, ресторацију или унапређење његових кључних базичних структура и функција“ (Simonovic & Peck 2013; Simonovic 2016). Отпорност на катастрофе постиже се укључивањем опција за адаптацију које омогућавају систему да се адаптира на утицаје догађаја и унапреде способност физичких, друштвених и економских сектора да фукнционишу након катастрофе. Ове опције за адаптацију помажу компонентама система да се суоче са и опораве од утицаја догађаја како би се вратиле у стање пре поремећаја што је брже могуће (Simonović 2020, 25).

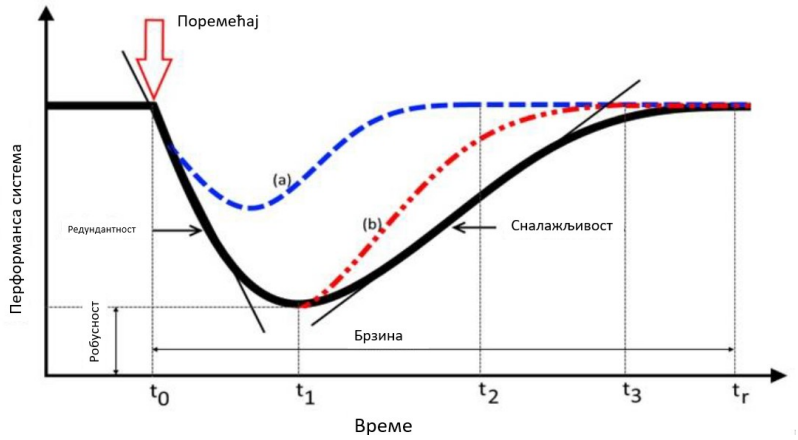
Симоновић сматра да се опције за адаптацију могу груписати у четири категорије:

1. Робусност (*robustness*) – снага или способност система да се одупре поремећајима (нпр. Мере заштите од поплава);
2. Редундантност (*redundancy*) – способност система да омогући непрекинуте услуге у случају поремећаја (нпр. дупли проводници);
3. Сналажљивост (*resourcefulness*) – коришћење ресурса (монетарних, технолошких, информационих и људских) ради успостављања, приоритизовања и постизања циљева (нпр. мобилизација фондова за управљање катастрофама);
4. Брзина (*rapidity*) – капацитет за повратак на ниво од пре поремећаја што је брже могуће. (Ibid)

Генерички приказ перформансе система који Симоновић и сар. користе за квантификацију динамичке отпорности приказан је на графикону 2 у наставку. Линија представља последицу интегрисане перформансе система након реметилачког догађаја са постојећим адаптивним капацитетом. Опадајући нагиб омогућава увид у редундансу система, док секција раста кривуље показује сналажљивост система. Робусност система и брзина су јасно илустроване нивоом перформансе система у временској тачки *t1* и временској разлици између *t0* и *tr*. Имплементација различитих адаптивних мера резултира променама у облику кривуље перформансе. На пример, проактивне мере ће резултирати кривуљом *a*, а реактивне мере

[4] Типологија криза и термини „криза-као-догађај“ и „криза-као-процес“ биће детаљније објашњена у делу о кризном менаџменту.

кривуљом *b*. Адаптивни капацитет одређује облик кривуље отпорности кроз четири припадајуће вредности – робусности, редундантности, сналажљивости и брзине (Ibid).



Графикон 2 Динамичка отпорност система (Simonović 2020)

1.2.1.1. Отпорност комплексних система

Као што је приказано у прегледу дефиниција концепта, отпорност омогућава системима способност да истрпе и преживе шокове и потресе, а такође и претпоставља способност система за опоравак. У савременим промишљањима овог концепта отпорност се препознаје као кључно својство комплексних адаптивних система (Barasa, Mbau & Gilson 2018).

Премда термин „отпорност“ има дуг историјат коришћења у психологији и антропологији[5], можемо са сигурношћу тврдити да је коначно утемељен 1973. године у кључном раду еколога Крофорда Холинга „Resilience and Stability of Ecological Systems“ (Отпорност и стабилност еколошких система). Холинг је тврдио да је одређени атрактор око кога се систем организује само једно од могућих стања која се појављују и нестају током времена (Holling 1973). Холинг супротставља појмове отпорности и стабилности. За Холинга, ***отпорност је мера издржљивости система и способност за ресорпцију промене и поремећаја уз задржавање истих односа између популација или варијабли система***. Стабилност, с друге стране, наглашава одржавање равнотеже унутар предвидивог света и акумулирање сувишних ресурса уз минималну флуктуацију система, а дефинише је као способност система да се врати у стање равнотеже након поремећаја (Ibid). Према Холингу ниска стабилност система сразмерна је његовој отпорности, што пореди са особинама траве и дрвећа приликом ветра. Дрво задржава стабилност, али је склоно пуцању, док се трава повија, али се, колико год удар ветра био јак, враћа у претходно стање (Ibid).

Холингово дело има значајне импликације по доносиоце одлука. Како Вилдавски истиче одржавање континуираног стања безбедности (тј. стабилности, према Холингу) може бити изузетно опасно на дуге стазе по опстанак система, пошто подрива капацитет система да се суочи са неочекиваним хазардима (Wildavsky 1989).

Концепт отпорности утемељен је у системском приступу, који укључује концепте комплексности, самоорганизације, функционалног диверзитета и не-линеарног понашања, па је према томе сачињен од комплексног сета интеракција и понашања које дозвољавају елементима

[5]За детаљан приказ академске примене термина „resilience“кроз историју види Alexander, 2013.

да се опораве и поврате функцију (Bhamra et al. 2011, 18). Сви системи су оријентисани ка остваривању циљева (Kast and Rosenzweig 1972; Skyttner 2005), међутим неизвесност игра кључну улогу у понашању система и може представљати претњу систему да постигне номиноване циљеве (Holling 1973).

У еколошкој литератури постоје многе расправе о реметилачким догађајима, тј. поремећајима (Holling 1973; Walker et al. 2004; Scheffer et al. 2001). Поремећаји значајне величине могу померити путању система у наизглед супротан домен (Scheffer et al. 2001). Сваки динамички систем поседује један или више домена, који се називају басени привлачности (Holling 1973), који се могу представити као „простор" који одређени систем заузима (Walker et al. 2004). Ти домени привлаче систем ка одређеном обрасцу понашања (Walker et al. 2004). На основу претпоставке да је циљ система опстанак, сваки систем може поседовати бројне басене привлачности који могу довести до опстанка или пропасти система (May 1977), са прагом који постоји између ова два пројектована исхода (Walker et al. 2004). Постојање бројних басена атракција је резултат нелинеарности између огромног низа неизвесних догађаја и интеракција њихових компоненти (Levin 1998). Различите одлуке могу довести ка привлачењу у басен поремећаја, или привлачењу у басен преживљавања (Mackay et al. 2020, 15).

На путању ка датом басену често утиче интеракција између система и његовог егзогеног (екстерног) окружења. Унутар сваког отвореног система (укључујући критичне инфраструктуре) пропусне границе су подложне и егзогеним и ендогеним (интерним)поремећајима (Kast and Rosenzweig 1972).

Теорија комплексних адаптивних система (КАС) произашла је из открића динамике хаоса у понашању система. Теорија хаоса се развила у две димензије.[6] Експериментализти су пронашли начине да открију дубоке и сложене обрасце у наизглед случајним или „хаотичним" подацима (Dooley 1997, 76). Пригожин и Стенгерсова, између осталих, користе хаос да опишу како поредак може настати из комплексности кроз процес самоорганизације (Prigogine & Stengers 1984).

Док су концепти хаоса и самоорганизације еволуирали из физике, појам КАС има своје корене у биолошким наукама (Gell-Mann, 1994). Док се теорија хаоса односи на одређено понашање сложених система, теорија КАС омогућава анализу организационог система са холистичке тачке гледишта: КАС се и самоорганизује и учи; примери КАС-а укључују друштвене системе, организације, екологије, економије, културе, политику, технологије, саобраћај, временске прилике итд (Dooley 1997, 77).

[6] Дули и сар. наводе следеће карактеристике система описаних теоријом хаоса: (а) наизглед случајно понашање може бити резултат једноставних нелинеарних система (или линеарних система повезаних повратном спрегом), (б) хаотично понашање се може открити путем различитих тополошких пресликавања, (ц) нелинеарни системи могу бити подложни осетљивој зависности од почетних услова — ова осетљивост приморава на преиспитивање узрочности — која се сада мора сматрати вишеслојном и вишедефинираном, (д) системи који су гурнути далеко од равнотеже (на ивици хаоса) могу спонтано да се самоорганизују у нове структуре, и (е) промене у суштинској природи система се дешавају када контролни параметар пређе критични праг — тачку бифуркације. (Dooley et al. 1995)

КАС су сачињени од међусобно повезаних елемената који чине мрежу у којој елементи често интерагују нелинеарно. Ова интеракција узрокује емергентно понашање[7] услед дејства повратних информација унутар мреже. Ова повратна информација ствара спрегу и јача узрочно-последичне односе између елемената система. Како би се одржала интерна комплексност система, потребна је константна енергија и интеракција између система и екстерног окружења. Услед оваквог понашања, комплексни системи су еволуциони, реагују на локалне информације и самим тим су способни за самоорганизовање (Andriani 2003).

Уколико применимо теорију КАС на организационе системе, или уже на операторе критичне инфраструктуре можемо закључити да интеграција у окружење и инхерентна међузависност критичних инфраструктура чини актере рањивим на ендогене и егзогене (локалне, регионалне и глобалне) поремећаје, а нарочито на системске, нерутинске ризике услед фактора као што су:

- озбиљност последица која може организацији отежати суочавање са тим догађајима када се јаве;

- реткости, која отежава организационо учење из личних и секундарних искустава;

- тешкоће предвиђања понашања организација, запослених и техничких система (Bier 2017,17).

1.2.1.2. Управљање ризицима – стратегија отпорности

Један од централних проблема праксе безбедности у комплексним окружењима и адаптивним системима јесте немогућност предвиђања и идентификације претњи и правовременог реаговања. Каплан и Гарик (1981) су тврдили да се управљање ризиком састоји од три главна питања: (1) шта може причинити штету, (2) колика је вероватноћа да ће се то десити и (3) које су последице? (Kaplan & Garrick 1981). Литература о ризику довела је у питање корисност квантитативних примена овог приступа због нетачних прорачуна (Haimes 2009) и ризика од пристрасности доносиоца одлука (Tversky, Kahneman, and Slovic 1982; Slovic 1987). Како неизвесност најчешће не може бити умањена, организације морају да се суоче са нежељеним догађајима тек када се они материјализују (Kahneman & Tversky 1982, 4).

Поље отпорности настало је као допуна традиционалном приступу пробабилистичке процене ризика, који има снажна ограничења у анализи комплексних система које карактеришу висока неизвесност и потенцијал за изненађења (Aven 2019, 1196). Према Дан Кавелтијевој и сар. отпорност пружа одговор на овај проблем и нову основу за суочавање са неизвесношћу (Dunn Cavelty, Kaufmann & Soeby Kristensen 2015, 5). Дакле, по овим ауторима отпорност представља стратегију менаџмента ризиком пре него стање система (Wildawsky 1985, Renn 2008, Longstaff et al. 2010, Aven 2019). Аутори ову стратегију супротстављају антиципацији

[7] Емергентност се односи на настајање нових и кохерентних структура, образаца и својства током процеса самоорганизације у сложеним системима. Овај феномен настаје када целина, односно систем, има одлике које немају њени појединачни саставни делови, односно када својства или понашања настају унутар система услед интеракције елемената. Емергентни феномени су концептуализовани као догађаји на макро нивоу, за разлику од елемената на микро нивоу, и процеса из којих настају. (Goldstein, Jeffrey. (1999). Emergence as a Construct: History and Issues. Emergence, 11: 49–72)

(Wildawsky 1985), пробабилистичком приступу управљања ризиком (Aven 2019) или безбедности, односно заштити (Fjäder 2014).

Слично томе, Баум наводи да су појмови ризика и отпорности повезани, али истиче да приступу отпорности треба дати предност за управљање системским ризицима и онима које је немогуће квантификовати (Baum 2015). Дакле, отпорност је важна парадигма за одлучивање у случају неизвесности. Поредећи парадигме управљања ризиком и отпорности, Баум каже да отпорност наглашава повећање способности система да задржи критичну функционалност ресорбујући поремећај, прилагођавајући му се или се лако опорављајући (Ibid).

Терје Авен, председник Удружења за анализу ризика (Society for Risk Analysis) уочава да постоји недовољно истраживања која тематизују однос ризика и отпорности, упркос томе што се ова поља у великој мери преклапају (Aven 2019, 1196). Неразумевање односа између ова два појма и скроман корпус интегрисаних истраживања довело је до позива на померање фокуса са ризика на отпорност међу доносиоцима одлука и међународним институцијама, укључујући Европску Унију и Уједињене Нације (Ibid, 1197). Јачањем отпорности безбедност система се унапређује без потребе за математичким рачунањем ризика (Ibid, 1196). Другим речима, отпорност умањује ризик појаве нежељених последица.

У свом капиталном делу „Трагање за безбедношћу“ (*Searching for Safety*) Арон Вилдавски разликује две могуће стратегије управљања ризицима: антиципацију и отпорност (Wildavsky 1989). Ставови Вилдавског заслужују детаљнији осврт, будући да је ово дело увело термин отпорности у друштвене науке (Darkow 2018, 1), као и приступ отпорности као стратегији управљања ризицима које се налази у темељу овог истраживања.

Према Вилдавском, антиципација је начин контроле централног ума - напори се усмеравају ка предикцији и превенцији потенцијалних опасности пре него што је штета начињена. С друге стране отпорност је капацитет за суочавање са неантиципираним опасностима након њихове манифестације (Wildavsky 1989, 77).

Даље, „организам или друштвени систем који мора да одржава пун репертоар одговора на будуће поремећаје ниске вероватноће схвата да је његов инвентар стандардних одговора скуп и, прилично вероватно, неприкладан. Предвиђање будућности је, као и тачно предвиђање кретања на финансијским берзама, изузетно редак случај. С друге стране, организам или друштвени систем који може, из својих стандардних залиха ресурса, синтетизовати шта му је потребно када год се појави нова опасност је у много бољој позицији да се суочи са неочекиваним последицама или хазардима који се само повремено појављују. Пошто му није неопходно да држи при руци репертоар свих могућих одговора, такви респонзивни системи су способни за конвертовање доступних генеричких ресурса, као што је богатство, знање и техничке вештине у прикладна решења ако му и када буду потребна“ (Wildavsky 1989, 71).

Вилдавски истиче да су отпорност и антиципација две стратегије које, када се уравнотежено користе, могу довести до оптималног нивоа безбедности. „Ниједна стратегија није инхерентно боља. Окружење са периодичним екстремима кореспондира са ситуацијом високих неизвесности (тј. покушај екстраполирања будућности полазећи од постојећих услова обично испадне погрешан), док би услови чврсте, непроменљиве стабилности кореспондирали са ситуацијама ниске неизвесности о будућности (тј. пројекције су обично тачне). Према томе, у условима неизвесности стратегији отпорности треба дати предност. У условима значајне извесности, антиципација (те самим тим заштита система од предвидивих облика претњи и грешака) има смисла. Стратегија антиципације није универзално примењива, јер је будућност нужно неизвесна што се тиче великог броја хазарда. Наиме, многи хипотетички хазарди су увек

могући, иако се највероватније неће материјализовати. Према томе, антиципаторно потрошени ресурси у циљу спречавања тих хазарда могу бити узалуд протраћени (Wildavsky 1989,79-80).

Дакле, свака стратегија има своју примену. Централни проблем у одређењу коју стратегију применити јесте да се анализирају ризици са којима се суочавамо. Уколико најозбиљнији ризици потичу од непредвидих извора или извора ниске вероватноће, тада је најбоље применити стратегију отпорности (тј. очување ресурса који се могу пребацивати и користити по потреби). Ако опасност долази из поуздано предвидих извора, тада антиципација има смисла. Реалне ситуације обично укључују мешавину познатог и непознатог; према томе постоји компромис – највероватније велике опасности, ако су познате и можемо им се супротставити, а да тиме нећемо погоршати ситуацију, могу и треба да буду спречене.[…] Да бисмо одабрали антиципацију као најбољу могућу стратегију за одређену ситуацију, морамо прво доказати да су највећи ризици са којима се сусрећемо они које можемо предвидети уз високу вероватноћу“ (Wildavsky 1989, 80).

Као што смо у уводним пасусима овог потпоглавља видели, идеје Вилдавског су присутне и у савременој литератури. Одјеке Вилдавског можемо видети код Фједера, за кога су појмови отпорности и безбедности супротстављени, тј. безбедност је оно што Вилдавски назива антиципаторном стратегијом: „суштинска природа безбедности је превентивна и проактивна, […] док је отпорност комбинација проактивних и реактивних мера усмерених на умањење последица, али не на превенцију претњи као таквих. Сасвим супротно, појам отпорности сугерише да превентивне мере нису имале пуног ефекта, и да се последично фокус помера на минимизирање ремећења критичних функција, када се догађај упркос свему десио“ (Fjäder 2014).

Повезујући учења о КАС и идеје Вилдавског, Комфортова и сар. наводе да у случају повећања комплексности окружења, углавном услед високог утицаја реметилачких догађаја, перформанса система опада. Опадање се дешава јер систем није у могућности да обради потребан обим и количину информација како би адекватно успоставио неопходну координацију између компонената система за одговор. Као резултат, у циљу успостављања стратегије за умањење ризика у неизвесностима, Комфорт и сар. даље сугеришу да би систем требало да створи баланс између антиципације или приправности и отпорности (Comfort 2001). Позитивна последица овог приступа јесте да систем на тај начин еволуира и учи. Нове структуре, обрасци и својства могу спонтано настати а да нису есктерно наметнути систему (Bhamra et al 2014, 18).

За ово истраживање веома су значајни ставови Ортвина Рена о отпорности као кључном приступу управљања ризицима (*risk governance*) (Renn 2008, 2015; Renn & Klinke 2015). Оквир управљања који је предложио Међународни савет за управљање ризицима (IRGC 2005) описује отпорност као ***нормативни циљ система управљања ризиком за третирање неизвесности и изненађења***. Отпорност је својство система који ресорбују ризик да би издржали поремећај (објективна отпорност), али и поверење актера управљања ризиком да су у стању да савладају кризне ситуације (субјективна отпорност). Рен примењује концепт отпорности који је развио Лоренц 2010. године, а према којем три капацитета отпорности (адаптивни менаџмент, капацитет за суочавање са нежељеним догађајем и партиципативни капацитет) одговарају трима карактеристикама ризика – комплексности, неизвесности и вишесмислености (Lorenz 2010). Рен, дакле, отпорност посматра као инклузивни и дискурзивни приступ управљању ризиком који укључује јаке везе са заинтересованим странама и општом јавношћу при чему квалитет размене информација игра одлучујућу улогу (Renn 2015).

Слично Талебовој илустрацији „антикрхкости“, а у складу са ставовима Вилдавског, Мекдоналд наводи да предузимање приступа отпорности у суочавању са поремећајима (у смислу прихватања реметилачких догађаја нижег интензитета) може омогућити адаптацију организације на нове ризике и обезбедити платформу за ефективно управљање варијабилностима и неизвесностима које долазе из окружења (McDonald 2006).

Дакле, за све ове ауторе, отпорност је стратегија избора у менаџменту оних ризика које карактеришу висока неизвесност (или ниска вероватноћа) и високе последице, то јест онима који се налазе на, по Талебовим речима, „дебелим реповима“ нормалне гаусовске расподеле вероватноће. Према овим ауторима, претње генерисане комплексним феноменима окарактерисане су ниским нивоом предвидљивости, али са потенцијално екстремно високим последицама (нерутински ризици). Ако не можемо да предвидимо долазећу опасност, превенција и заштита постају изузетно тешке и са ниским односом између цене коштања и ефикасности.

Узевши у обзир све наведено, у овој дисертацији отпорност дефинишемо као ***стратегију управљања нерутинским ризицима и неизвесностима, усмерену на јачање капацитета система за антиципацију (предвиђање) и ресорпцију (одговор) догађаја, адаптацију (прилагођавање) на догађај и , и рестаурацију (опоравак) након догађаја***.

1.2.2. ***Организациона отпорност***

Академско интересовање за отпорност организација допунило је ранија истраживања о узроцима организационих криза усмеравањем пажње на питања како и зашто организације напредују упркос неизвесностима и комплексностима, те како подносе екстерне шокове, уче из нежељених догађаја и прилагођавају се динамичном окружењу (Lee, Vargo & Seville, 2013). Као и друге врсте, КАС организациони систем се мора мењати и прилагођавати као одговор флуктуацијама и поремећајима у окружењу како би одржао своју структуру и функције. Да би преживеле у волатилном окружењу, организације морају развити способност да успешно одговоре на различите манифестације неизвесности, према одређеним процедурама (Seville et al. 2006).

Како Комфорт и сар. наводе, организационе перформансе опадају у окружењу повишене комплексности, јер повећања организационе комплексности захтевају значајна повећања у току информација, комуникацијама и координацији како би се интегрисали различити нивои функционисања и различити захтеви за одлучивање у кохерентан програм деловања (Comfort et al. 2001, 144).

Корпус литературе о организационој отпорности је веома обиман, а у последњих неколико година приметан је напор за систематизацију литературе у великом броју прегледних студија које тематизују различите аспекте организационе отпорности приказаних у табели 2.

Табела 2 – Тематизација организационе отпорности у прегледним студијама

Аутор	Година	Тема	Резултати

Lienenlueke	2017	Перспективе истраживања организационе отпорности	1. Одговор на нежељене догађаје и/или способност за опоравак након инцидента и повратак у стање „нормалности“ 2. Унапређивање организационих капацитета и адаптација 3. Антиципација и осмишљавање
Lienenlueke	2017	Нивои организационе отпорности	1. Организациони (стратегијски) 2. Тимски (тактички) 3. Индивидуални (оперативни)
Williams et al.	2017	Елементи организационе отпорности у емпиријским студијама	1. Располагање ресурсима, 2. Организационе праксе, 3. Посткризни одговор
Conz & Magnani	2018	Концептуализација организационе отпорности у литератури из области менаџмента	Темпорално одређење 1. (t-1) – пре догађаја – антиципација/приправност 2. (t) – током догађаја - ресорпција 3. (t+1) – након догађаја – опоравак и адаптација 4. Континуум
Darkow	2018	Доминантне парадигме отпорности у новијој литератури	1. Планирање за супротстављање 2. Задржавање кризе
Dutchek	2020	Категорије дефинисања организационе отпорности	1. Исход 2. Процес 3. Капацитети
Hillmann & Guenther	2020	Хронолошки развој концептуализације организационе отпорности	1. Специфично понашање отпорних организација 2. Ресурси потребни за постизање отпорности 3. Инжењерски приступ отпорности 4. Капацитети отпорности 5. Типологије отпорности 6. Еколошки приступ - адаптација
Hillmann	2020	Перспективе различитих научних дисциплина	1. Екологија 2. Безбедност (укључује менаџмент ризиком, кризни менаџмент и управљање ванредним ситуацијама), 3. Инжењерске науке, 4. Психологија 5. Организационо понашање, 6. Стратегијски менаџмент

У наставку ћемо се детаљније осврнути на прегледне студије Линенлукеове (Lienenluecke 2017), Даркова (Darkow 2018), Дучекове (Duchek 2020), и Хилманове (Hillman 2020) као најзначајнијих за утемељивање истраживања у оквиру ове дисертације, док ће прегледна студија

Вилијамса и сар. (Williams et al. 2017) бити изложена у потпоглављу о односу између кризног менаџмента и организационе отпорности.

Прегледна студија Дучекове (Duchek, 2020) идентификује три главне категорије дефиниција организационе отпорности – отпорност као исход, отпорност као процес и отпорност као сложен концепт сачињен од чинилаца - капацитета.

Прва, и најшира, укључује студије које отпорност посматрају као исход. Оне су углавном усмерене на идентификовање карактеристика отпорних организација: ресурса, стратегија и понашања. Емпиријске студије често ретроспективно испитују организационе одговоре на кризу како би идентификовале факторе који су могли имати позитивне или негативне утицаје. Дучекова наводи да иако те студије имају важан допринос у идентификовању карактеристика или атрибута организација које су ефикасно одговориле на промене и кризе, оне не пружају довољан увид у интерну динамику отпорности.

Друга концептуализација посматра отпорност као динамички процес укључивањем временске перспективе и усмерена је на идентификацију фаза отпорности. На пример, за Сатклифа и Вогуса отпорност је процес суочавања са неповољним догађајима који коначно доводи до отпорности као исхода (Sutcliffe & Vogus 2003). Исти аутори наводе да се појам отпорности односи на способност за препознавање претњи и адаптирање на претње и дисконтинуитете, као и на развој способности за опоравак и ефикасан повратак функција након нежељеног догађаја (Ibid). Ипак, Бојн и ван Етен сматрају да је концептуализација отпорности као процеса проблематична јер је сам процес отпорности „црна кутија“, а такође је мерење успешности процеса отежано јер се може мерити само *ex-post* у случају да је процес био успешан (Boin & van Eeten 2013). Слично томе, за Бамру и сараднике организациона отпорност је исход функционисања организације пре, током и након догађаја. (Bhamra et al. 2011). Бојн и ван Етен додају да постоје два типа отпорности – прекурсорска (превентивна) отпорност и отпорност опоравка, те наглашавају да ова два типа треба јасно разликовати. За прекурсорску отпорност наводе пет антецедената: 1) висока техничка компетентност у целој организацији; 2) постојање свести о кључним догађајима који морају бити спречени; 3) процедуре и праксе које подржавају спречавање тих догађаја; 4) формалне структуре у смислу улога, одговорности и ланца комуницирања које могу бити трансформисане у ванредним ококлностима у децентрализоване структуре и тимски приступ решавању проблема; 5) „култура поузданости“ (Boin & van Eeten 2013).

Последња концептуализација, према Дучековој, усмерена је на идентификовање капацитета отпорности, то јест специфичних способности организације које су у основи отпорности[8]. Капацитети се широко дефинишу као операциони и стратегијски, али се понекада и специфично идентификују као рутине и праксе које чине организацију отпорном. Овај приступ је заинтересован за операционализацију отпорности у пракси. Морамо приметити да Дучекова не укључује концептуализацију отпорности као стратегије менаџмента ризиком, будући да су консултовани радови из области стратегијског менаџмента, не консултујући радове из области управљања ризицима. Аутор ове дисертације је адаптирао приступ Дучекове у категоризацији дефиниција отпорности изложеној на претходним страницама (табела 2), заменивши категорију исхода, са категоријом стратегије.

[8] Треба напоменути да у литератури није јасно објашњена разлика између капацитета и способности , па се та два термина се често користе као синоними (Hillman & Guenther 2020, 2). Рихтнер и Лефстен појашњавају да „имати способност значи имати и капацитет и знање, те само онда када се капацитет за отпорност преточи у дело у организацији онда отпорност постаје организациона способност“ (Richtner & Löfsten 2014, 138).

Линенлуке (2017) разликује три главне перспективе академских истраживања организационе отпорности. Прва група истраживача приступа организационој отпорности као способности организације да преживи нежељене ситуације и/или способности да се опораве након инцидента и врате у стање „нормалности“ (нпр. Horne 1997; Horne and Orr 1998; Robert 2010). Друга група је усмерена на унапређивање организационих процеса и капацитета, и указују на потребу за прилагођавањем променама како би организација из кризе изашла јача него што је била (Lengnick-Hall and Beck 2005; Lengnick-Hall et al. 2011). Према овој перспективи организациона отпорност подразумева активно и смислено суочавање са неочекиваним догађајима (Duchek 2020). Напокон, за трећу групу истраживача организациона отпорност укључује и идеју антиципације (Rerup 2001; McManus, Seville, Vargo & Brunsdon 2008; Somers 2009). За Сомерса је отпорност чак „више од пуког опстанка, она укључује идентификацију потенцијалних ризика и предузимање проактивних корака како би се обезбедио успех организације упркос непогоди“ (Somers 2009). Дакле, према овој перспективи отпорност се приближава Талебовој идеји „антикрхкости“ (Taleb 2019). Студија Линенлукеове такође је примењена на анализу дефиниција отпорности у Табели 2, идентификовањем усмерености концептуализација на капацитете и фазе антиципације, ресорпције, рестаурације и/или адаптације.

Прегледна студија Хилманове анализирала је перспективе различитих научних дисциплина које су утицале на разумевање организационе отпорности: екологије, безбедности (а међу које укључује менаџмент ризиком, кризни менаџмент и управљање ванредним ситуацијама), инжењерских наука, психологије, организационог понашања, стратегијског менаџмента наука (Hillman 2020). Према Хилмановој разумевање појма отпорности у свакој од набројаних научних дисциплина разликује се по онтологији, разумевању потреба за отпорношћу и понуђеним решењима за постизање отпорности (Hillman 2020, 42).

Теоријске идеје из екологије као што је метафора о адаптивном циклусу (Holling 1973) пружају нова и кориснија објашњења организационог понашања (Clement & Rivera 2017). Идеја да организације пролазе кроз адаптивне циклусе рефлектована је у перспективама менаџмента ризика и криза, те теорије комплексних система и организација високе поузданости (High Reliability Organizations - HRO), а она гласи да организације треба да примењују стратегију отпорности ако функционишу на граници хаоса без постојања стабилних или постојања искључиво краткотрајних равнотежа (Hillman 2020, 46). Међутим, за разлику од екосистема, организације могу применити проактивне мере за изградњу отпорности (Ibid). Еколошке студије и теорија комплексних система утицале су на схватање отпорности као својства које укључује адаптацију и трансформацију кроз емергентно понашање, то јест настајање нових структура и функционалности. У организационој пракси, то подразумева развој и измену политика, процеса и организационе културе које омогућавају организацији да настави да врши своју функцију упркос изазовима (Barasa et al. 2018; Pike, Dawley & Tomaney 2010).

Инжењерски приступ настоји да идентификује сет индикатора којима би се оценила отпорност организације, како би се даље унапређивала и оптимизовала (Pellisier 2011). Кључно питање јесте опоравка и повратка у нормални режим функционисања (Martin-Breen and Anderies 2011), што је у колизији са еколошком и организационом теоријама. Систем може превазићи поремећај и пребацити се у другачије стање (тј. адаптирати се на новонастале услове, према еколошким теоријама), или се чак унапредити упркос неповољним околностима (психолошка перспектива). Међу аспектима или индикаторима отпорности присутним у инжењерским перспективама најчешће се налазе флексибилност и редундантност. (Hillman 2020, 48)

Идеје потекле из психологије и организационог развија анализирају односе на нивоу појединаца и тимова и повезују их са организационом отпорношћу (Hillman 2020, 47). Инжењерски приступ је утолико сличан њима јер наглашава значај запослених и њихове улоге у суочавању са неочекиваним реметилачким догађајима. Ипак, док је инжењерска перспектива усмерена на комуницирање и безбедносне процедуре, психолошке и организационе теорије додају значај односа унутар организације, те индивидуалне отпорности запослених (Hillman 2020, 47). Ове теорије постављају следећа питања:

- Какав тип организовања би допринео унапређењу отпорности?
- Можемо ли обучити и образовати менаџере за показивање позитивнијег понашања и перципирања претњи као прилика?
- Како ћемо их за то обучавати? (Ibid)

Проучавање отпорности у области менаџмента ризика и криза потиче од истраживања Вилдавског (1988), које је већ детаљно изложено, те теорија нормалних акцидената (Perrow, 1984) и теорија високе поузданости (High Reliability Theory - HRT). Теорија нормалних акцидената претпоставља да су у високо комплексним системима грешке и акциденти неминовни и инхерентни тим системима, те се према њима треба односити нормално, као неизоставном делу функционисања тих система (Perrow 1999, Sagan 2004). Грешке се акумулирају услед људских грешака и ограничене рационалности (Perrow 1994). С друге стране, према теорији високе поузданости могуће је организацију учинити скоро савршено безбедном (Clarke 1993, La Porte & Consolini 1991), јер одређене стратегије могу резултовати готово оптималним исходима (Rijpma 1997, Roberts 1993). Теорија високе поузданости сматра да применом доброг организационог дизајна и управљања, грешке и акциденти могу бити превенирани, умањени или задржани (Weick & Sutcliffe 2007). Ипак, треба напоменути да су теорије високе поузданости и нормалних акцидената превасходно усмерене на ендогене претње, то јест на оне претње које потичу из саме организације.

Истраживања отпорности у области менаџмента ризиком и кризама усмерени су на два аспекта – организациона отпорност као заштита и превенција, те организациона отпорност као интегрисани систем менаџмента (Hillman 2020, 11-16). У изучавању организационе отпорности као аспекта интегрисаног система менаџмента посебно се наглашава значај система менаџмента континуитетом пословања (Herbane 2010; Sawalha 2013, 2015; Foster & Dye 2005). Однос организационе отпорности и интегрисаних система менаџмента – кризног менаџмента и менаџмента континуитетом пословања биће детаљно описан у потпоглављима 1.1.3.2 и 1.1.3.3.

Хилманова наводи да је допринос изучавања отпорности у области менаџмента ризиком и кризама вишеструк. Прво, отпорност је генеричка карактеристика организација која се може унапређивати на континууму, тј. савршена отпорност је идеалан концепт који је у пракси недостижан. Отпорност се имплицитно посматра као организовање за безбедност и поузданост, јер, следећи теорију високе поузданости, структуре и процедуре које обезбеђују поузданост једнаке су онима које обезбеђују отпорност – пре свега функционална децентрализација и редундантност. Напокон, према овој перспективи култура поузданости је битна за организациону отпорност током криза. Наиме, када се нежељени догађај деси, отпорна организација ће га прихватити и брзо решити проблем због постојања контингентних планова који ће одлучивање делегирати на ниво и особу која може најбрже и најефикасније реаговати (Hillman 2020, 16). Како Севил и сарадници примећују велика већина организација данас поседује планове континуитета пословања и опоравка, међутим, уколико те процедуре и

планови не могу бити интуитивно примењени током криза, они неће имати ефекта (Seville et al. 2006).

Дарков разликује две доминантне парадигме у литератури о организационој отпорности - прва која посматра отпорност као план за суочавање са нежељеним догађајима путем управљања ризицима и избегавања кризних ситуација (а која корелира са стратегијом "антиципације" Вилдавског) и отпорности као начина за заустављање, то јест управљања кризама (Darkow 2018). Дарков примећује да се организације високе поузданости (High Reliability Organizations - HRO) узимају као пример отпорних организација, будући да упркос својој комплексности успешно избегавају "нормалне акциденте" којима су инхерентно изложени. Главни фокус HRO јесте спречавање избијања проблема, јер се оне, по својој природи, не могу ослањати на принцип учења из грешака, будући да и мали проблем може значити губитак критичних функција друштва и узроковати тешке последице, потенцијално хиљаде људских живота (Boin & Van Eeten 2013, 432). Дарков истиче да се разлика између отпорности и поузданости огледа у односу према фази/капацитету опоравка (а који, опет, према аутору подразумева и способност адаптације), те тако наводи да се нису све HRO успешно и ефикасно опоравиле и прилагодиле новом окружењу након нежељеног догађаја, узимајући за пример нуклеарну електрану Фукушима (Darkow 2018, 5).

1.2.2.1. Међународни стандарди

Налази поменутих академских студија практично су примењени у стандардима о организационој отпорности, пре свега ISO:22316-2015 и ASIS ORM.1-2017. О директивама Европске Уније биће речи у поглављу о критичној инфраструктури.

Према ИСО стандарду 22316-2015, организациона отпорност је исход организационе способности за антиципирање и одговор на поремећаје узроковане ризицима и капацитета организације за даптацију на комплексне и променљиве околности у условима неизвесности (ISO 22316: 2015, 8). Високо отпорне организације отпорности имају капацитет да антиципирају и одговоре на претње и прилике и да се измене у условима неизвесности како би постигле своје стратешке и операционе циљеве. Капацитет је овим стандардом дефинисан као комбинација свих доступних снага и ресурса унутар организације, заједнице или друштва који могу умањити ниво ризика или ефекат кризе (ISO 22316: 2015, 7).

Ове функционалне способности отпорности су од виталног значаја за организације, међутим саме по себи нису довољне за осигурање будућности организација током периода промена и треба да буду подржане вредностима које једнако доприносе отпорности. Оне укључују поверење, лојалност и посвећеност изградњи морала запослених и заштити репутације организације (ISO 22316:2015, 4).

Стандард наводи да су три главна елемента отпорности принципи, атрибути и стратешки циљеви, те да организациона отпорност зависи од тога од степена до којег се ови елементи комбинују и формирају јединствен систем менаџмента како би се унапредио адаптивни капацитет за антиципацију и одговор на претње и прилике (ISO 22316:2015, 5).

Према стандарду Америчког удружења за индустријску безбедност (ASIS) о Безбедности и отпорности организација и њиховог ланца снабдевања – Захтеви и смернице (ASIS ORM.1-2017), отпорност је превасходно усмерена на континуирану изградњу капацитета система. Организациону отпорност одликују:

- Ресорптивни, ресторативни и трансферабилни капацитети који омогућавају отпорност на нежељене догађаје, или способност повратка на прихватљив ниво перформанси у прихватљивом временском оквиру након нежељеног догађаја;
- Капацитет система да одржи своје функције и структуре у поводу интерних и екстерних промена како би се искористиле прилике и/или управљало деградацијом активности и функција;
- Проактивно планирање у циљу умањења магнитуде и/или трајања нежељених, реметилачких догађаја унапређењем способности антиципације, ресорпције, адаптације и опоравка;
- Оснаживање запослених да одговоре на промене, прилике или нежељене догађаје на информисан начин.

ASIS ORM.1-2017 стандард посматра организациону отпорност као ***исход и функцију менаџмента ризиком, нарочито при стањима повишене неизвесности***.

Отпорност није инхерентна организацијама, већ се развија како организације сазревају, уче из успеха и грешака, унапређују вештине управљања и одлучивања, стичу боље увиде и сазнања о интерним и екстерним факторима који могу утицати на њу. Она такође произлази из односа са другим системима, културних перспектива и способности појединаца да се суоче са стресом и потешкоћама.

Стандард даље наводи да отпорне организације, између осталог, препознају да је ризик константа, интегришу проактивно управљање ризиком у све процесе одлучивања, промовишу способност праћења ситуације и надзор са нагласком на идентификовање индикатора промена, уче из свог и туђег искуства у циљу јачања за будуће догађаје, негују вештине решавања проблема на свим нивоима организације и прихватају да не могу све неизвесности и с њима повезани исходи бити квантификовани.

1.2.2.2. Структурне и формалне карактеристике отпорних организација

Истраживачи су указивали на формалне и структурне карактеристике отпорних организација. Ово укључује:

- хоризонталну хијерархију која омогућава брзе и флексибилне реакције на реметилачке догађаје и промене у окружењу,
- разноврсне слободне генеричке ресурсе и вештине за повећање шанси да систем може да пружи *ad-hoc* одговор,
- поверење унутар организације али и однос поверења са екстерним субјектима;
- лабаво повезане подсистеме који онемогућују каскадне ефекте, одржавање резервног капацитета за амортизовање неочекиваних поремећаја, и
- функционалну редундантност у критичним системима како би се осигурало да се основне функције могу одржати чак и под условима делимичног слома система (Godschalk, 2003; Lee et al., 2013; Longstaff, 2005, 2010; Parker, 2010; Wildavsky, 1989).

Као што је већ наведено, Вилдавски (Wildavsky 1989) је сматрао да је располагање слободним, генеричким ресурсима од кључног значаја за одговор на неизвесности и нерутинске ризике. Студије о организацијама високе поузданости (High Reliability Organizations – HRO)

показују да оне улажу ресурсе у превенцију и третман одређених ризика, али и успостављају организационе праксе за импровизацију и употребу слободних ресурса када и како су им потребни, иако претходно нису имали сазнања да ће им бити потребни (Wildavsky 1989, 433). У складу са становиштем Вилдавског, Вилијамс и сарадници такође истичу да према перспективи HRO отпорност укључује импровизовање и коришћење генеричких ресурса (Williams et al. 2017, 746).

Вајк и Сатклиф наводе пет одлика HRO које их чине отпорнима:

- Сталожено и поуздано функционисање у условима високог стреса, уз истицање важности надзора над ситним грешкама, чиме се избегава опуштање, а што је нарочито важно у дужим успешним периодима организације (Weick & Sutcliffe 2007, 9).
- Значај нижег, оперативног, особља и њихова техничка компетентност, којима се дају довољни ресурси и приоритизују упозорења која стижу од њих (Weick & Sutcliffe 2007, 12).
- Спречавање уских перцепција стварности путем инсистирања на "широком скенирању хоризонта" и контекстуалним интерпретацијама опаженог што доприноси бољем процесу одлучивања (Weick & Sutcliffe 2006, 516). Концептуални вишак доприноси дивергентним перспективама чиме се избегавају „слепе тачке" (Schulman, 1993).
- Способност импровизације, за коју је неопходно лично искуство и прећутно знање (Weick 1993, 638; Bechky & Okhuysen 2011).
- Брзе измене у хијерархији, стандардним оперативним процедурама и пребацивање ауторитета на функционалне експерте (Darkow 2018, 4).

Дискурс о организацијама високе поузданости се последње деценије помера ка мрежама високе поузданости (HRN) (Berthod et al. 2017), што отвара нови скуп проблема, пошто сви елементи мрежа високе поузданости не морају нужно бити организације високе поузданости (Berthod et al. 2015), а такође комплексне међузависности међу елементима могу утицати на повишену интерну неизвесност (Sydow et al. 2013).

Прегледна студија Вилијамса и сар. идентификује финансијске, когнитивне (знања, вредности, култура), бихејвиоралне (организациони дизајн, дифузија доношења одлука, сарадња и координација), релационе (поверење, умреженост) и емоционалне (емоционална чврстина, оптимизам) ресурсе од значаја за отпорност (Williams et al 2017). Ленгник-Холова описује организациону отпорност као, „јединствену смешу когнитивних, бихејвиоралних и контекстуалних својстава који поспешују способност организације да разуме своју тренутну ситуацију и да развије прилагодљиве одговоре који рефлектују то разумевање" (Lengnick-Hall et al. 2011, 244).

Когнитивни и бихејвиорални ресурси укључују снажан фокус на учење и размену искустава путем интерне комуникације (Weick & Sutcliffe 2007; Weick et al. 1999), пажљиву алокацију и дистрибуцију пажње, знања и ресурса на нивоу организације како би се олакшали препознавање и тумачење потенцијалних проблема (Marcus & Nichols 1999), фокусирало на истакнутост сигнала и смањиле тензије између организационих структура и ширег контекста у којем се организација налази (Barton et al 2015; Roberts et al. 1994; Bierly & Spender 1995).

У складу са Вилдавским (1988) и Вајком (Weick 1993), Сатклиф и Вогус наглашавају значај слободних генеричких ресурса, који називају „концептуалним вишком" (*conceptual slack*).

Концептуални вишак се односи на диверзитет аналитичких перспектива и вољу за преиспитивање процедура и поступака. Концептуални вишак унапређује могућност идентификовања претњи и сагледавања проблема из различитих перспектива и преиспитује наслеђено организационо знање (Sutcliffe & Vogus 2003, 105).

Примена хијерархијских образаца у одлучивању о комплексним, функционално различитим проблемима не води решењу проблема, напротив, мултипликује га (Кековић 2022,18). С друге стране хоризонтална устројеност може унапредити процеси осмишљавања и одлучивања укључивањем доносиоца одлуга у дневне пословне праксе и рутине (Vogus & Sutcliffe 2007; Weick et al. 1999). Ово такође означава оснаживање појединаца и тимова из организације да предузму флексибилан одговор прилагођен новој, нерутинској ситуацији. Знатан број емпиријских истраживања у овом смеру спроведен је у хитним службама. Медицински тимови за хитну помоћ морају да балансирају планиране активности са ад-хок активностима (нпр. осмишљавање и непоступање по протоколу (Faraj & Xiao 2006), док ватрогасни тимови такође у хитним случајевима примењују технике импровизације у деловању и комуникацији (Bigley & Roberts 2001). Уколико би тимови и организације погрешно интерпретирали сигнале из окружења и не би прилагодили одговор ситуацији, били би мање отпорни на нежељене и комплексне догађаје са којима се суочавају (Bigley & Roberts 2001).

Далгард-Нилсенова истиче низ карактеристичних ставова, образаца понашања, норми и вредности који омогућавају организацијама да се успешно суочавају са сложеношћу и изненађењем (Daalgard Nielsen 2017, 342). Она такође имплицитно истиче хоризонталну устројеност и флексибилност конкретизујући је као

- способност импровизације за стварање нових решења за неочекиване проблеме;

- виртуелни систем улога помоћу којег сваки члан групе разуме организацију у целини и улоге које обављају други, дозвољавајући сваком члану да подржи или преузме улоге других чланова у случају потребе;

- висок степен индивидуалне отворености и радозналости и препознавање да чак и ако је прошло искуство од помоћи, свака ситуација је потенцијално нова;

- интеракцију између чланова групе, која омогућава организацији да боље капитализује целокупно расположиво знање (Daalgard Nielsen 2017, 342).

Слично наведеном, Хамел и Валикангасова (Hamel & Valikangas 2003) и Лонгстафова (Longstaff 2005) у структурне и формалне одлике отпорних организација увршатавају скенирање хоризонта ради откривања раних знакова промене, континуирано експериментисање, спремност за брзу прерасподелу ресурса даље од постојећих активности ка новим областима и значај повратних информација прикладније од нефлексибилних стратегија и процедура.

Истраживачи су свесни разлика који у приступу слободним генеричким ресурсима и могућности пружања флексибилног одговора и хоризонталног хијерархијског устројења постоји између организација у јавном и приватном власништву, о чему ће више речи бити у поглављу о ктиичној инфраструктури. Овде је битно истаћи да унапређење отпорности организација у јавном сектору може бити отежано вредностима и ограничењима специфичним за јавни сектор (Comfort, 2005, 2012a, 2012b; Fitzgerald & Lupton, 2015; Kendra & Wachtendorf, 2003; Termeer & van den Brink, 2013).

Старк показује како кризни менаџери у Европској Унији и Уједињеном Краљевству осећају потребу да покажу компетентност кроз постојање планова и процедура без обзира на то

да ли унапред смишљени планови и процедуре помажу или штете у одговору на сложене и динамичне ризике (Stark, 2014). Међутим, процедуре се приликом манифестације нерутинских ризика често могу занемарити јер је потребно донети хитне одлуке које се најчешће доносе натуралистички. Одлучивање препознавањем прве прихватљиве одлуке (Recognition Primed Decision Making - RPDM) је у литератури препознато као основни натуралистички модел одлучивања у комплексним кризама и нежељеним догађајима (Klein 1993; Kešetović i Toth 2011; Rubens 2020). Како Рубенс наводи „у нестабилним ситуацијама, не размишљамо шта пише у уџбенику, већ користимо своје архиве личних искустава и сећања да бисмо изградили слику о томе шта се дешава“ (Rubens 2020, 227). RPDM комбинује два процеса – ситуациону анализу и менталну стимулацију: ситуационом анализом се генерише могући правац деловања, док се менталном стимулацијом тај правац евалуира (Klein 1993, 138). Другим речима, доносилац одлуке прикупља могуће правце деловања, упоређује их с ограничењима која намеће ситуација и бира први правац деловања који, с обзиром на постојећа ограничења, није одбачен (Kešetović i Toth 2011, 122). Како Кешетовић и Тот закључују, овај модел одлучивања добро функционише у условима временског притиска када се располаже делимичним информацијама, а циљеви нису јасно дефинисани (Ibid).

Такође, поједини аутори истичу да притисак ка штедњи у јавном сектору ограничава способност организација за улагање у структурне елементе отпорности као што су слободни генерички ресурси и стратешке резерве (Longstaff, 2012; Stark, 2014; Walker & Salt, 2006).

Слободни генерички ресурси, хоризонтално устројење као и флексибилност одговора од значаја су за капацитете организационе одговорности о којима ће бити речи у наставку текста.

1.2.2.3. Однос организационе отпорности и кризног менаџмента

Изучавање организационе отпорности се знатно подудара са истраживачким напорима у области кризног менаџмента, због чега сматрамо да је потребно укратко објаснити тачке пресека ова два приступа. По много чему кризни менаџмент и стратегија отпорности су два аспекта истог изазова, разумевања нежељених догађаја (Williamson et al. 2017, 750). Стога је битно да се укаже на сличности између истраживачких приступа, ови блиски појмови раздвоје и покуша изнаћи допринос који теме кризног менаџмента могу допринети успостављању јасног оквира управљања отпорношћу организација.

Наиме, услед пораста глобалних изазова, системских и нерутинских ризика који прете организацијама, препозната је потреба за јаснијим разумевањем интеракција између криза и организација, укључујући и потребу за развијањем организационе отпорности како би се изложеност и утицаји нежељеног догађаја умањили пре него што се он манифестује (Van der Vegt et al 2015; Williams & Shepherd, 2016a, Williamson et al. 2017). Како Рубенс препознаје „вредност приступа отпорности у кризном менаџменту јесте што је утицао на промену перспективе – од контроле инцидента, до менаџмента вишеструким последицама“ (Rubens 2023, 131). Према Лабаки, „Кризни менаџмент је знатно еволуирао и данас он није усмерен само на успостављање превентивних мера и развијање процедура за поступање, већ и на унапређивање процеса доношења одлука како би се доносиоци одлука могли суочити са неочекиваним и непредвиђеним ситуацијама. Према томе, унапређивање отпорности КИ представља највећи изазов за кризне менаџере“ (Labaka 2013, 1).

Научници и практичари који настоје да повежу истраживачке токове кризног менаџмента и организационе отпорности наилазе на низ проблема. Први међу њима јесте недостатак консензуса око дефиниције кризе и фрагментисана литература која се бави кризама, као и њена првенствено нормативна и прескриптивна усмереност (Williamson et al. 2017). Слично томе,

иако су истраживачи заинтересовани за разумевање како и зашто су неке организације отпорније од других на изазове, студије организационе отпорности се махом не позивају на постулате и научна достигнућа у области кризног менаџмента. Једно од објашњења за ово непреклапање јесте претпоставка да отпорне организације избегавају кризе, то јест избегавају велике поремећаје у функционисању пре, током и/или након нежељеног догађаја (Alexander 2013; Bonanno 2004; Bonanno et al. 2010; Sutcliffe & Vogus 2003).

Ипак, како Вилијамс и сар. сматрају, интегрисање истраживања у области кризног менаџмента (способност повратка система у нормални режим функционисања након ремећења) и отпорности (способности одржавања функционисања упркос ремећењу) представља природни ток за јаче утемељење теорије организационог функционисања током нежељених догађаја (Williams et al. 2017, 734). Однос између кризе и отпорности даје увид у то како организације антиципирају, прилагођавају се и одговарају на нежељене догађаје.

1.2.2.3.1. Концепт кризе

Две главне концептуализације кризе су *криза као догађај* и *криза као процес* (Кековић 2006; Кешетовић 2018, 122). И из овога можемо увидети сличност са *концептуализацијама отпорности као стања и као процес*а, о којима је било речи на ранијим страницама.

Криза као догађај је пре свега усмерена на истраживање реакција актера на ретке и изузетне, нерутинске догађаје, по чему је блиска истраживањима о отпорности другог реда. Једна од најцитиранијих дефиниција кризе у овом истраживачком оквиру гласи: „*криза је ситуација ниске вероватноће, а високог утицаја, која је перципирана од стране критичних стејкхолдера да може угрозити постојање организације*“ (Pearson & Clare 1998,66). Друга важна дефиниција јесте дефиниција Пола т'Харта који наводи да је криза „*непријатан догађај, који представља изазов за доносиоце одлука, искушава их да поступају у условима угрожавања, временске стиске и неспремности*“, те да је она „*озбиљна претња основним структурама или фундаменталним вредностима и нормама социјалног система, која, у условима временског притиска и веома несигурних околности, захтева доношење критичних одлука*“ (Rosenthal et al. 1989).

Џејмс и сар. сматрају да су три компоненте кризе - реткост догађаја, значај догађаја и ниво утицаја на заинтересоване стране – кључне за разумевање овог термина (James et al. 2011). У фокусу ових истраживања је сам догађај, а студије углавном истражују шта је био „окидач“ догађаја, те како догађај ремети и прети опстанку организације (Williams et al. 2017, 735). Дакле за разлику од приступа у студијама отпорности које не третирају догађај као такав, овде је догађај у фокусу истраживања. Кризе се у овој истраживачкој традицији посматрају као непредвиђени догађаји (насупрот рутинским догађајима), изолованим у времену и простору, који имају јасан извор или узрок и висок утицај (Pearson & Clair 1998; Shrivastava 1992; Weick 1988). Користећи ову концептуализацију, циљ кризног менаџмента је да разуме динамику кризе у њеној акутној фази и како се организације враћају у стање равнотеже (Williams et al 2017,735; Lalonde & Roux-Dufort 2010).

Концептуализација *кризе као процеса* допринела је разумевању окружења која доприносе развоју кризе, процесе организационог слабљења, еволуције кризе и како организације разликују одређене степене криза (Кековић, 2006). Перспектива сагледавања кризе као процеса наглашава да се кризе развијају током времена, а понекад и у фазама, укључујући инкубацију, догађаје окидаче и разрешење кризе (Mitroff & Pearson 1993; Roux-Dufort 2016; Turner 1976), као и да представљају прекид нормалног функционисања које захтева промене док актери тумаче и процесуирају „таласе значења“ у новом окружењу (Roux-Dufort 2007, 111). Процесна

перспектива сугерише да постоји „генеалогија криза која се може потенцијално пратити далеко пре акутне фазе, која је крајњи моменат континуираног кумулативног процеса организационих грешака“ (Roux-Dufort 2016:27). Дакле, организација може третирати претњу кризе пре, током и након догађаја окидача (Williams et al. 2017,736). Овај приступ, према томе, укључује не само ретке, нерутинске догађаје, већ истиче да су догађаји окидачи само једна од компонената криза, поред системских аномалија, организационих слабости, рањивости и свакодневних – рутинских изазова који се не примећују, игноришу или неразумевају (Rudolph & Repenning 2002; Turner 1976).

Приступ *кризама као процесима* истиче значај кризног менаџмента пре, током и након догађаја. Догађај окидач може настати услед свакодневних непримећених догађаја који се инкубирају и акумулирају у кризу услед фактора као што су:

1. погрешне претпоставке,

2. комплексност информација,

3. застој у примећивању и тумачењу сигнала и

4. одбијање замишљања најгорег могућег исхода (Turner 1976, 393-394).

Ове факторе можемо повезати са недостацима антиципативног и ресорптивног капацитета отпорности, то јест у мањкавостима током антиципације, осмишљавања и давања когнитивног одговора.

1.2.2.3.2. Кризни менаџмент – примарне теме

Кризни менаџмент се може одредити као скуп функција или процеса који имају за циљ да идентификују, изуче и предвиде могуће кризне ситуације и успоставе посебне начине које ће организацији омогућити да спречи кризу или да се са њом избори и да је превазиђе уз минимизирање њених последица и што бржи повратак у нормално стање (Кешетовић 2018, 124). Кризни менаџмент у ширем смислу обухвата и управљање ризиком, односно цео низ мера које се односе на идентификацију хазарда и анализу рањивости компаније, те напоре да се криза избегне (фаза превенције) преко припреме за кризе, с обзиром на њихову вероватноћу и озбиљност њихових потенцијалних последица и израду одговарајућих кризних планова сагласно кризној матрици (фаза припреме), те реаговање на кризу када се она догоди (фаза одговора – кризно управљање у ширем смислу) и враћање корпорације у нормално стање (фаза опоравка) уз одговарајућу имплементацију научених лекција и евентуалне измене стандардних оперативних процедура и кризних планова (Ibid, 125). Ова класификација је веома слична класификацији капацитета и фаза отпорности коју смо изнели у претходном поглављу. Ипак видимо да је кризни менаџмент, као и сваки нормативни систем менаџмента, усмерен на процену ризика, идентификацију претњи и прецизно планирање, док је концепт отпорности превасходно утемељен на потреби за флексибилношћу одговора, импровизацијом и располагањем слободним генеричким ресурсима, а не праћењем унапред одређених процедуралних корака.

Вилијамсон и сарадници су у својој прегледној студији из 2017, идентификовали три примарне теме у литератури о кризном менаџменту – кризни менаџмент као нормативна активност у циљу поновног успостављања равнотеже, улога лидера у кризном менаџменту и важност тимова за кризни менаџмент (Williams et al. 2017, 736).

Велики број емпиријских студија које тематизују кризни одговор заснован је на линеарном, формулаичком и бирократизованом моделу у којем су планирање, припрема и

митигација хазарда координисани кроз централну јединицу доношења одлука (нпр. Владу, министарство или организацију) (Canton 2007; Comfort 2007; Schneider 1992). Након ванредног догађаја настаје поремећај структура, рутина и способности. Према томе, истраживања у овој традицији настоје да унапреде политике и процедуре управљања ванредним ситуацијама (Comfort 2007; Iannela & Henricksen 2007) које указују на координацију, комуникацију и друге активности које омогућавају ефикаснији одговор, као што су јасно дефинисани циљеви, подела задужења, формална структура одговора и сет политика и процедура (Schneider 1992, 138; Quarantelli 2005). Значајан број аутора се слаже да нерутински ризици и неизвесности представљају изазов за доносиоце одлука, те закључују да, и поред њихове неоспорне важности, детаљно планирање и припрема кризног одговора не може предвидети сваку могућу кризу (Drabek & McEntire 2003; Herbane 2013; Neal & Phillips 1995; Wenger, Quarantelli & Dynes 1990). Наиме, ефикасан кризни одговор такође укључује ад-хок способности као што су импровизовање приликом одлучивања, извршавању улога, идентификацији и мобилизацији ресурса и успостављање реда кроз емергентне технике комуникације и координације (Williams et al. 2017,738).

Тематизовање лидерства у истраживањима из области кризног менаџмента и организационе отпорности доносе подударне закључке. Лидери помажу другим члановима тима у разумевању и осмишљавању обиља информација у току кризе (Christianson et al 2009) и доприносе стабилности упркос потенцијалу за хаос (Schneider 1992). Услед инхерентних ограничења приступа „војне команде“ (command and control) у кризном одговору новонастајућа лидерска понашања и развој нових норми су од кључног значаја за адресирање захтева организације у поводу кризе (Schneider 1992; Wenger 1992; Auf der Heide 1989). Активности које лидери предузимају пре настанка кризе, као што су проактивно трагање за рањивостима и њихово разумевање и третирање, могу бити значајне за успешно вођење организације кроз кризу (James & Wooten 2010, Barton et al. 2015) или њено предупређивање (Rerup 2009).

Напокон, истраживања која тематизују тимове за кризно управљање углавном покушавају да објасне како актери могу минимизирати утицај ремећења а затим се опоравити до нивоа пре-кризног функционисања (Williams et al. 2017, 739). Једно од кључних идентификованих аспеката ефикасних кризних тимова јесте њихова флексибилност, односно способност за брзо и флексибилно реорганизовање ресурса како би се с једне стране умањили стресори за системе, а с друге генерисала нова решења која би третирала измењене околности (Barton & Sutcliffe 2009; Weick & Roberts 1993). У складу са психолошким и еколошким теоријама отпорности, а одражавајући и Талебов конструкт „антифрагилности“ (Taleb 2011) истраживачи овог аспекта кризног менаџмента сматрају да организација може из кризе изаћи јача него што је била пре кризе. Наиме, високо оспособљени кризни тимови и други повезани системи у организацијама могу генерисати позитивне исходе и омогућити повратак на статус кво, или чак напредовати у односу на статус кво (James et al. 2011; Kahn et al. 2013; Maitlis & Sonenshein 2010; Maitlis & Christianson 2014).

Истраживања која кризу концептуализују као догађај, од значаја су за ову дисертацију управо зато што третирају негативне догађаје настале актуализацијом нерутинских ризика – ниске вероватноће а високог утицаја. С друге стране, концептуализација као процеса значајна је услед тога што се фазе процеса кризе готово подударају са фазама отпорности и њиховим капацитетима. Сагласно том одређењу кризе, процесно одређење отпорности уважавало би динамичку природу отпорности као интеракцију између организације и окружења. Самим тим она би укључивала предкризне/преддогађајне способности, организовање и прилагођавање током кризе и посткризни опоравак (Williams et al 2017, 742).

Следећи Тарнера (Turner 1976), можемо уочити проблеме и изазове у разним фазама актуализовања догађаја – пре свега антиципације и ресорпције – погрешне претпоставке, неадекватно осмишљавање, одбијање прихватања најгорег могућег сценарија, те преоптерећеност и комплексност информација свакако отежавају пружању правовременог когнитивног одговора и самим тим немогућности његовог превођења у бихејвиорални одговор. Такође, својство кризе да представља прекид нормалног функционисања које захтева промене док актери тумаче и процесуирају „таласе значења“ у новом окружењу одговара ономе што Тарант назива „нерутинским ризиком“.

Како Вилијамсон и сар. наводе, организације које развију когнитивне, бихејвиоралне, емоционе и релационе способности могу да се адаптирају на новонастале околности, а такође могу и да омогуће антиципацију и одговоре на догађаје окидаче. Ове способности интерагују рекурсивно са организационим напорима повезаним са поузданошћу и умањењем ризика. Истовремено са овим процесима, постоји континуирано реорганизовање и прилагођавање у складу са процесуирањем и третирањем додатних претњи. Након искушавања и превазилажења кризе, постоји повратна спрега у којој интерпретације задатака и односа актера које су они искусили током догађаја обликују организовање за будуће поремећаје (Williams 2017, 750).

Свакако, теме које доминирају у истраживањима кризног менаџмента – кризно планирање, лидерство и кризни тимови, од значаја су и за истраживања организационе отпорности. Флексибилно планирање, адаптабилност планова и одговора, приступ ресурсима, реорганизација и адаптиција, те оснаживање запослених за самосталан одговор од кључне су важности за одговор на нерутинске ризике.

Услед свих наведених сличности, поставља се питање разлика. У нашој концептуализацији, отпорност је стратегија за управљање неизвесностима и ризицима ниске вероватноће а високих последица, што по појединим ауторима одговара дефиницији кризе. Дакле, стратегија отпорности менаџмента ризиком би била подударна кризном менаџменту. Сматрамо да је разлика између кризног менаџмента (тј. способност враћања система у нормални режим функционисања након ремећења) и отпорности (тј. способности одржавања функционисања упркос неприликама) коју су предложили Вилијамс и сар. (Williams et al. 2017, 736) преуска, јер према њој би отпорност била једнака континуитету пословања. Наше мишљење је да је стратегија отпорности шири појам, који обухвата не само кризни менаџмент, већ и процесе традиционалног менаџмента ризиком, менаџмента континуитетом пословања, као и добре праксе у области планирања, људских ресурса и лидерства. Такође, фокус отпорности јесте превасходно на јачању капацитета (приступ усмерен на штићеним вредностима), узимајући у обзир да сви потенцијални ризици и кризе нису уврштени у регистар ризика и матрицу криза, а не толико на интерним и екстерним претњама. Напокон, континуирана фаза адаптације и њен одговарајући капацитет јесте дистинктивна одлика стратегије отпорности, у односу на кризни менаџмент и менаџмент континуитетом пословања.

Наша хипотеза је да ће организације, које експлицитно или имплицитно усвајају стратегију отпорности за управљање нерутинским ризицима, препознати важност функционалног и флексибилног управљања ризиком, кризама и континуитетом пословања у свим фазама антиципације, ресорпције и рестаурације.

1.2.2.4. Отпорност и менаџмент континуитетом пословања

Као тренутно водећа парадигма операционализације организационе отпорности сугерише се примена приступа менаџмента континуитетом пословања путем којег се успостављају механизми које организација користи за успешан пролазак кроз кризе и друге поремећаје

пословања. Према Бамри и сар. отпорност у контексту организација је у тесној вези са индивидуалним и организационим одговорима на поремећаје и прекиде континуитета пословања (Bhamra et al. 2014, 4).

Како наводи Британски институт за континуитет пословања, „континуитет пословања је кључна дисциплина за изградњу и унапређење организационе отпорности“ (BCI Statement on Organizational Resilience). Менаџмент континуитетом пословања усмерен је првенствено на ресорптивни (одговор на инцидент) и ресторативни капацитет организације, то јест на опоравак. У мањој мери, менаџмент континуитетом пословања усмерен је на јачање антиципативног (процена ризика и анализа утицаја на пословање су интегрални део плана континуитета пословања), као и адаптивног капацитета кроз стратегије које, на пример, укључују редундантност запослених и материјалних средстава, резервне локације, те обучавање запослених за извршавање различитих пословних задатака не само из њиховог домена,.

За Фостера и Даја отпорност се може постићи кроз спровођење система менаџмента континуитетом пословања у смислу: 1) заштите запослених; 2) заштите кључног пословања предузећа (система, објеката, инфраструктуре и процеса); 3) заштите пословних мрежа (нпр. ланца снабдевања) (Foster & Dye 2005). Хербане такође уочава да сами менаџери, тј. доносиоци одлука сматрају да се организациона отпорност може унапредити кроз адекватан менаџмент кризама и континуитетом пословања (Herbane 2013).

Осим тога, пажња коју организација поклања менаџменту ланца снабдевања, сарадњи и комуникацији са другим институцијама, организацијама и заинтересованим странама такође доприноси на бољем одговору на кризе, то јест бољој отпорности организације (Therrien, Tanguay & Beauregard-Guérin 2015).

Према томе формализоване праксе система менаџмента континуитетом пословања које су и саме засноване на пробабилистичкој процени ризика корелирају са отпорношћу првог реда, према концептуализацији Кендре и Вахтендорфа, а коју су преузели и бројни потоњи истраживачи (Hollnagel et al., 2008; Kendra & Wachtendorf, 2003; Lee et al., 2013, Daalgard Nielsen 2022). Премда поједини практичари указују на недоследност приступа усмереном на штићене вредности - менаџмента континуитета пословања применом пробабилистичке процене ризика, данас формализовани систем менаџмента (ISO 22301:2020) ову активност предвиђа као први корак. Самим тим, фокус се измешта са неизвесности и нерутинских ризика на вероватне сценарије, те је унапређивање отпорности другог реда у другом плану.

У пракси менаџмента континуитетом пословања, сценарији су углавном усмерени на штићене вредности. Међу главним штићеним вредностима су запослени, те један од основних сценарија јесте ситуација када организација остане без кључних запослених – било да је таква околност настала услед смрти, болести, отказа, епидемије, штрајка, или других ситуација које су условиле немогућност доласка на радно место кључног запосленог. Међутим, мање пажње се поклања ситуацијама када већи број „некључних“ запослених није спреман да се појави на радном месту током и након екстремних догађаја, не због физичке онемогућености (недостатка превоза, оштећења саобраћајница, повреда итд.) већ услед психичких баријера (неповерење у организацију да ће им омогућити све предвиђене мере заштите, неадекватна комуникација ризика, неразумевање своје улоге у одговору на инцидент, неразумевање важности своје организације за безбедност и добробит заједнице и државе) (Riddle 2015).

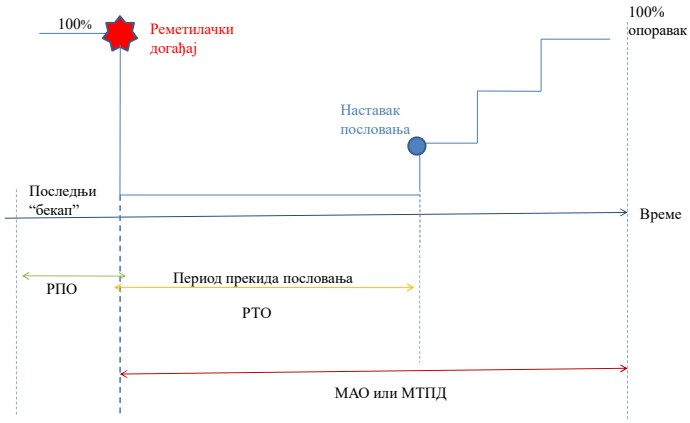
Стратегије које се у менаџменту континуитета пословања препоручују усмерене су на континуитет рада путем обука и дообука, сменског рада, географске сепарације запослених са истим вештинама и обезбеђивање подршке екстерних страна („outsourcing“). Пажња се не

поклања повећавању спремности или способности запослених да се јаве на посао. Како Ридлова закључује, потребно је јасније усмерење ка потенцијалним разлозима за одсуство током инцидента и захтевима за организације да уваже практичне и психолошке потребе запослених током екстремних догађаја узрокованих нерутинским ризицима (Riddle 2015, 17). У складу са категоризацијом ресурса Вилијамсона и сар. уочавамо да се у нормативном систему менаџмента континуитетом пословања не поклања довољно пажње когнитивним и, нарочито, емоционалним ресурсима. Према томе можемо закључити да су планирање и праксе континуитета пословања од високог значаја за ресорптивни и ресторативни капацитет отпорности, али да саме по себи нису довољне за успешно реаговање у кризним ситуацијама. Ово је нарочито приметно код манифестације хазарда са високим степеном негативних атрибута детаљно изложених у поглављу о ризицима, када се од запослених, али и доносиоца одлука, може очекивати емоционалан, а не рационалан одговор.

Менаџмент континуитетом пословања и однос овог концепта са организационом отпорношћу анализираћемо детаљније у посебном потпоглављу. Овде ћемо се укратко осврнути на план континуитета пословања чији је есенцијални део план опоравка критичних активности. Према српском стандарду SRPS ISO 22301:2014 планови континуитета пословања су документоване процедуре којима се организације усмеравају да одговоре, ***да се опораве, наставе и да се врате на претходно дефинисан ниво рада након поремећаја.*** (SRPS ISO 22301:2014:2) Дакле, видимо да Стандард не предвиђа повратак на ниво пре догађаја, већ на ниво који ће организацији омогућити да опстане.

Стандардне фазе у имплементацији система континуитета пословања јесу процена ризика, анализа утицаја на пословање, те израда плана континуитета пословања који обухвата план одговора и план опоравка. Иако у професионалној заједници не постоји консензус око потребе за проценом ризика, јер се тиме фокус усмерава искључиво на идентификоване претње, то јест на отпорност првог реда, приликом даљих корака, а пре свега анализе утицаја на пословање и планова одговора и опоравка сценарији су усмерени на штићене вредности без обзира на претње, што доприноси унапређењу отпорности другог реда.

Анализом утицаја на пословање (Business Impact Analysis - BIA), организација се упознаје са својим најважнијим, тј. критичним, производима или услугама, процесима којима се они добијају и активностима који су најважније за обављање тих процеса. За сваки производ или услугу се утврђују утицаји реметилачког догађаја, тј. какву ће негативну последицу на организацију имати неиспоручивање тих производа или услуга, у оквиру којих временских оквира итд. У наредној фази идентификују се процеси којима се стварају ти производи или услуге, а затим и активности које су саставни део тих процеса. Потом се процењује утицај на организацију који настаје необављањем ових активности током времена, слично као и у претходној фази. Осим утицаја, неопходно је одредити и приоритетне временске оквире у оквиру којих је потребно поновно покренути ове активности (RTO – Recovery Time Objective). (ISO 22317:2015) Такође, неопходно је утврдити постојеће и потребне ресурсе за подршку тим активностима – поред оних ресурса којима организација непосредно располаже, овде треба уврстити и испоручиоце, партнере и друге релевантне заинтересоване стране. (ISO 22317:2015) Колико год је могуће, требало би и идентификовати зависности и међузависности између активности, то јест колико одређена активност зависи од неке друге активности која је кључна за добијање критичних производа и услуга.



Графикон 3. Фазе периода опоравка у односу на реметилачки догађај (Нинковић 2018)

У складу са анализом утицаја на пословање план континуитета пословања усмерен је на опоравак критичних пословних функција након реметилачког догађаја и најчешће има следеће делове:

- Дефинисане улоге и одговорности за људе и тимове који имају овлашћења у току и након инцидента;
- Процес за покретање одговора (тј. када и како се доноси одлука о покретању одговора на инцидент и опоравак критичних активности);
- План одговора на инцидент;
- Детаље о начину комуницирања са интерним и екстерним заинтересованим странама;
- План опоравка критичних активности;
- Кризно комуницирање с медијима;
- Процес за повлачење узбуне након инцидента. (SRPS ISO 22301:2014)

Планови континуитета пословања треба да дају одговор на следећа питања:

- Која је моја улога у случају инцидента?
- Који су нам приоритети за опоравак?
- Које ресурсе имамо на располагању? (Нинковић 2018)

Два главна дела плана континуитета пословања су планирање одговора на инцидент и планирање опоравка пословања. У плану одговора на инцидент даје се списак и кратак опис непосредних акција које треба предузети ради одговора на инцидент, у смислу задржавања, контроле и минимизирања утицаја на пословање. Овај план често има облик чек-листе уз коју могу ићи и коментари. Примена овог плана унапређује ресорптивни капацитет организације.

План опоравка укључује мере и радње које треба предузети након инцидента у циљу минимизирања прекида пословања и времена опоравка, тако да овај план утиче на ресторативни

капацитет отпорности организације. План се активира током инцидента који организацију спречава да извршава своје редовне активности.

1.2.2.5. Интегративни аналитички модел организационе отпорности

Досадашња истраживања организационе отпорности једногласно указују на чињеницу да је реч о сложеном, композитном концепту. Међутим, око елемената овог концепта не постоји јасна сагласност. Истраживачи идентификују елементе у складу са својом концептуализацијом отпорности као исхода, процеса или стратегије, те, на пример, оно што је за једну групу аутора капацитет организације, за друге ауторе представља фазу у одговору на ризик (антиципаторни капацитет се огледа у периоду t-1 пре реметилачког догађаја, ресорпциони у периоду t током, а реституциони и адаптациони у периоду t+1 након догађаја).

Будући да у овој дисертацији отпорност концептуализујемо као стратегију менаџмента системским и нерутинским ризицима и неизвесностима, јачање елемената организационе отпорности посматрамо као кораке у припреми за одговор на нерутинске догађаје, те опоравак и константно прилагођавање система пре, током и након нерутинског догађаја.

На следећим страницама понудићемо и наш аналитички модел. Наиме, сматрамо да је за студије безбедности битно разумети да ли се доносиоци одлука, менаџери ризика и континуитета пословања, као и чланови и руководиоци кризних тимова припремају за непредвиђене догађаје или искључиво на рутинске и нерутинске ризике присутне у регистрима ризика (тзв. Отпорност првог и другог реда). Затим, да ли се отпорност унапређује на индивидуалном, тимском или системском-организационом нивоу. Анализа четири капацитета отпорности представља суштину овог приступа, и од значаја ће за истраживање бити да ли се у испитаним организацијама свим капацитетима отпорности придаје једнак значај, или су поједини капацитети доминантни, односно запостављени. Те напокон да ли се у свим тим капацитетима отпорности пажња посвећује меким или искључиво тврдим аспектима, што нужно утиче на отпорност другог реда, то јест на отпорност на непредвиђене догађаје.

1.2.2.5.1. Димензије организационе отпорности

Димензије, тј. конститутивни елементи система, разликују се у односу на скалу система - да ли се посматра организација, држава, заједница, особа или било који други систем. Када је реч о организационим системима аутори углавном идентификују четири димензије отпорности (Bruneau et al. 2003; Zobel 2010; Gibson and Tarrant 2010):

- техничку (способност физичког система организације да функционише током и након инцидента),
- организациону (способност доносиоца одлука да доносе адекватне одлуке или предузму мере које могу смањити интензитет последице или дужину трајања опоравка),
- економску (капацитет система да амортизује додатне трошкове настале услед инцидента) и
- социјеталну (способност заједнице да умањи последице кризе помажући хитним службама или волонтирањем).

Графикон 4. Димензије отпорности организације

У овом истраживању фокус је на организационој димензији отпорности оператора критичних инфраструктура. Стога, све даље референце на отпорност организације биће усмерене на организациону димензију без експлицитног помињања.

1.2.2.5.2 Извори ризика – отпорност првог и другог реда

Организациона отпорност се такође може дефинисати према врстама претњи. Према Денјеру истраживања организационе отпорности еволуирала су протеклих деценија, од превасходне усмерености на потенцијалне инциденте унутар система, до адаптације на разне екстерне изазове, од природних непогода до кључних социо-политичких трендова (Denyer 2017, 8). Затим, Бараса и сар. у закључку свог прегледа емпиријских студија о организационој отпорности у сектору јавног здравља наводи се да је „заједничка тема одабраних радова препознавање отпорности као својства комплексних адаптивних система. Отпорност је уједно функција планирања и припремања за будуће кризе (планирана отпорност), и прилагођавање хроничним стресовима и акутним шоковима (адаптивна отпорност)“ (Barasa et al. 2018).

Знатан број истраживача разликује способност организације да се носи са познатим претњама и опасностима, користећи већ постојеће и унапред планиране способности, али и способност за одговор на неочекиване проблеме учењем, мењањем и развојем нових способности у ходу. Ове способности поједини аутори називају отпорност првог и другог реда (Hollnagel et al., 2008; Kendra & Wachtendorf, 2003; Lee et al., 2013).

Отпорност првог реда подразумева ефикасно и ефективно руковање познатим претњама и опасностима путем испробаних и тестираних технологија и мера, преко централне контроле, правила и процедура који отелотворују искуство и историјско знање организације (Dalgaard Nielsen 2017, 343). Отпорност првог реда може се постићи применом интегрисаних система менаџмента ризиком, кризног менаџмента и менаџмента континуитетом пословања.

Отпорност другог реда, насупрот томе, захтева култивисање способности за опоравак од неочекиваних догађаја[9] путем делегирања, брзе повратне информације и дозволе за експериментисање и импровизацију када стандардна решења изостану (Wildavsky 1989).

Иако је корпус литературе о организационој отпорности усмеренији на отпорност на идентификоване, рутинске ризике,[10] Ленгник-Холова и сар. сматрају да организације морају развити капацитете отпорности који ће им омогућити да адекватно реагују на неочекиване догађаје који им могу угрозити опстанак, па и искористити те нежељене догађаје у своју корист (Lengnick-Hall, Beck & Lengnick-Hall 2011).

Истраживачи истичу да постизање отпорности и првог и другог реда и пребацивање између модуса праћења правила и импровизације представља велики организациони изазов (Boin & van Eeten, 2013; LaPorte & Consolini, 1991). Истраживања отпорности у јавном сектору и међу операторима критичне инфраструктуре нарочито указују да у актуелним политичким дискурсима постоје очекивања од тих система да показују отпорност и првог и другог реда. Агенције јавног сектора су позване да предвиде, спрече или ефикасно обуздају познате ризике, док се брзо прилагођавају и прилагођавају када се суоче са појавом непознате претње или опасности (Dahlberg et al., 2015; Edwards, 2009; Flynn, 2008; Homeland Security Advisory Council, 2011)2.

У наставку дисертације видећемо да је постизање отпорности другог реда пре свега еквивалентно доброј пракси у примени „„меких аспеката“ отпорности.

1.2.2.5.3. Организациони нивои отпорности

Линенлуке истиче да постоји конфузија о томе да ли је отпорност концепт који се односи на један или више организационих нивоа, од нивоа појединца, тима, организације, па до организационих мрежа (Linnenluecke 2017, Darkow 2018).

Један скуп научних радова конструише отпорност на организационом нивоу, те Ленгник-Холова и сар. наводе да се организациона отпорност „изводи из скупа специфичних организационих способности, рутина, пракси и процеса“ (Lengnick-Hall et al 2011, 246). Други аутори истичу значај отпорности на индивидуалном нивоу (то јест, запослених и доносилаца одлука) за организациону отпорност. Према овим ауторима организација може бити отпорна само колико су то појединци коју њу чине (Hillman & Guenther 2020, 3). Ленгник-Холова и сар. наводе да је разумевање индивидуалне отпорности почетна тачка за разумевање организационе отпорности, а која представља адитивни композит индивидуалних способности и деловања (Lengnick-Hall et al. 2011). Трећа група претпоставља отпорност тимова и организационих јединица као предуслов организационе отпорности, истичући да се активности и одлуке доносе и извршавају на колективном нивоу (Salanova et al. 2012).

Напокон, у корпусу литературе о организационој отпорности присутне су дискусије о томе да ли је отпорност има стратегијски или оперативни аспект (Hillman & Guenther 2020, 3). На пример, веома значајан део литературе о отпорности ланца снабдевања јасно је усмерен на оперативни ниво и у великој мери се подудара о литератури о континуитету пословања. Постоје и они аутори за које је отпорност једино могућа уколико се ускладе праксе и ресурси на свим нивоима, као што су Сатклиф и Вогусова (Hillman & Guenther 2020, 3).

[9] Индукованих нерутинским ризицима и неизвесностима, прим.аут.

[10] Под овим подразумевамо и ризике чије третирање спада у домен безбедносног менаџмента, као и оперативне ризике.

Наиме, ови аутори разликују ресурсе на индивидуалном (индивидуална знања и вештине, те обуке које воде ка индивидуалној ефикасности и компетентности у обављању задатака који превазилазе рутинска задужења), тимском (акумулирано знање, диверзитет знања и варијабилност у саставу тимова, колективна ефикасност која у складу са теоријом емергентности није једнака збиру ефикасности чланова тима) и организационом нивоу (склоност ка организационом учењу, организациона култура која стимулише слање повратних информација, флексибилне процедуре и флексибилан трансфер знања, вештина и ресурса), те сматрају да се отпорност може постићи само њиховом интеграцијом (Sutcliffe & Vogus 2003).

Ови увиди искоришћени су у теренском делу истраживања које је у једном делу покушало да да одговор на питање да ли је у операторима критичне инфраструктуре фокус спровођења организационе отпорности на организационом, тимском или индивидуалном нивоу или је присутан интегративни приступ у складу са Сатклифом и Вогусом.

1.2.2.5.4. Капацитети организационе отпорности

Према ИСО стандарду 22316-2015 Организациона отпорност – Смернице, организациона отпорност је исход организационе способности за антиципирање и одговор на поремећаје узроковане ризицима и капацитета организације за адаптацију на комплексне и променљиве околности у условима неизвесности (ISO 22316: 2015, 8). Капацитет је овим стандардом дефинисан као комбинација свих доступних снага и ресурса унутар организације, заједнице или друштва који могу умањити ниво ризика или ефекат кризе (ISO 22316: 2015, 7).

У литератури се најчешће идентификују четири капацитета (атрибута или аспекта) – предиктивни или антиципаторни, ресорптивни, адаптивни и ресторативни. (Bruneau et al., 2003; Madni, 2007; Department of Defense, 2011; Francis & Bekera, 2014; Kekovic et al. 2014) што је приступ прихваћен у овом истраживању.

Антиципаторни капацитет је степен приправности на могуће поремећаје, а који зависи од адекватне, свеобухватне и флексибилне идентификације претњи и процене ризика. Ресорптивни капацитет је степен до којег систем може аутоматски ресорбовати утицај ремећења система и минимизирати последице са што мање напора. Адаптивни капацитет је степен до којег је систем способан за самоорганизацију опоравка до жељеног нивоа функционисања и прилагођавање новом интерном и екстерном окружењу. Коначно, ресторативни капацитет је способност система за опоравак – било да је у случају повратак на почетно, пре-инцидентно стање, или у комплетно ново стање које антиципира будуће захтеве система (Keković, Dragišić & Ninković 2014).

Осим категоризације капацитета отпорности усвојеним у овом истраживању постоје и нешто различити приступи које ћемо кратко представити.

Поједине студије за капацитете користе термин „аспекти“ отпорности и говоре о: избегавању (антиципација долазећег ремећења или кризе), робусности (способности да се издржи ремећење, то јест ресорбује), способности за опоравак и (ре)конфигурацију (тј. адаптацију) (Department of Defense, 2011; Madni, 2007; Bruneau et al., 2003; Francis & Bekera, 2014). Мишљења смо да робусност и „избегавање“ нису најприкладнији термини. Уколико посматрамо организације као КАС, робусност је само један од елемената који може утицати на „амортизацију“ реметилачког догађаја, а који не укључује флексибилност и способност импровизације који су од значаја за успешан одговор на нерутински догађај. Такође, сматрамо да изједначавање антиципације са избегавањем није оправдано, будући да се неки, а нарочито егзогени системски, ризици не могу избећи већ се антиципирањем и осмишљавањем може унапредити одговор, опоравак и адаптација на новонастале околности. Такође, ми смо у овом

истраживању прихватили терминологију Гибсона и Таранта (Gibson and Tarrant 2010) који говоре о тврдом (активности, тј. оно „шта се ради“ у организацији у циљу унапређења отпорности) и меком аспекту (карактеристикама, тј. како се те активности спроводе) отпорности.

Затим, Хилманова и Гинтерова су у свом прегледном раду идентификовали двадесет и два различита атрибута, то јест капацитета, у седамдесет и једној дефиницији организационе отпорности присутних у литератури из области стратегијског менаџмента. Најчешће су то били способност за адаптацију (N=27; 38%), способност за суочавање са нежељеним догађајем (N=20; 28%), и способност за реконфигурацију (N=15; 21%) (Hillmann & Guenther 2020, 6). Наше становиште је да разликовање адаптације и реконфигурације није оправдано у контексту примене концепта отпорности као стратегије за управљање нерутинским ризицима и неизвесностима. Такође, неидентификовање капацитета за антиципацију или осмишљавање и опоравак, у одређеном је нескладу са другим категоризацијама капацитета отпорности.

За неке ауторе капацитети заправо представљају фазе процеса отпорности. Стога би предикција представљала темпоралну фазу пре догађаја, ресорпција фазу током и непосредно након догађаја, и напокон ресторација - фазу након догађаја. У зависности од аутора, фаза адаптација може настати након догађаја, али и током, па и пре избијања нежељеног догађаја. Национална академија наука САД идентификује четири фазе процеса управљања отпорношћу, а које кореспондирају са поменута четири капацитета (National Research Council 2012).

Помињана прегледна студија Дучекове такође је на трагу ових истраживања, па Дучекова говори о фазама антиципације, суочавања и адаптације (Duchek, 2020). Дучекова дефинише појам организационе отпорности као мета-способности сачињене од сета организационих способности и рутина које омогућавају успешан пролазак кроз три сукцесивне фазе отпорности (антиципација, суочавање и адаптација) (Ibid). Фаза антиципације и проактивне акције је период пре избијања нежељеног догађаја, а њој припадају когнитивна способност опсервације и идентификације ризика коју би требало превести у бихевиоралну способност приправности. У фази суочавања, током инцидента, когнитивну способност прихватања кризе утиче на осмишљавање и примену решења, док у фази адаптације способност рефлексије и учења утиче на могућност организационих промена (Ibid).

Докторска дисертација одбрањена 2021. године на Технолошком институту у Џорџији, говори о три фазе отпорности (разумевање ризика, антиципација и ресорпција) усмерене ка смањењу неизвесности повезане са изложеношћу (идентификација претњи, разумевање ризика, адаптација) или са последицама (ресорпција) (Singh 2021,27). Опоравак и адаптација инхерентно прихватају неизвесност и не фокусирају се нужно на редуковање утицаја опасности, чак и ако то подразумева промену оригиналних карактеристика система (трансформација) (Ibid). У Синговом истраживању, адаптивна отпорност је дефинисана као начин инкорпорирања отпорности у систем који поспешује флексибилност и агилност у свим елементима комплексног система. Под овом дефиницијом, сваки напор за подржавање планирања, антиципације, ресорпције и опоравка система, треба да буде „адаптабилан“, т.ј. са намерном инкорпорирањем флексибилности и агилности у различите аспекте отпорности система, који ће узети у обзир неизвесности повезане са будућим поремећајима (Ibid).

Наше је становиште да је разликовање фаза и капацитета у инфраструктури пре свега семантичко, тј. да је реч искључиво о углу посматрања, без јасне суштинске разлике. Наиме, антиципативни капацитет је значајан за фазу t-1, ресорптивни за фазу t, а ресторативни за фазу

t+1. Према нашем мишљењу, које је у сагласности са Синговим становиштем, адаптивни капацитет прожима све три фазе отпорности.

У наставку текста ћемо пружити детаљну анализу и операционализацију сва четири капацитета.

1.2.2.5.4.1. Антиципаторни капацитет

Знатан корпус литературе о организационој отпорности тематизује организационе процесе усмерене на антиципацију, превенцију или митигацију потенцијалних догађаја, као и припрему за суочавање са неочекиваним или непознатим ситуацијама. Слични истраживачки напори присутни су и у области кризног менаџмента где је антиципација од кључног значаја за умањење вероватноће да ће та нежељени догађај прерасти у „окидача" кризе (Williams et al. 2017, 746). Кризе могу потицати од „нормалних", рутинских догађаја као што су пожари, киднаповања или губитак кључних запослених, али такође и од системских нерутинских ризика као што су глобални економски потреси, појава нових технологија, пандемије или политичка нестабилност. Отпорност на потоње феномене је важна пошто такви догађаји проузрокују „колективно искуство", имају акутни почетак и временски су одређени, па је према томе брзо одлучивање у контексту које одликује висока неизвесност витална за избегавање додатног страдања (McFarlane & Norris 2006, 4).

Идентификација претњи и анализа ризика су генерално први кораци који се предузимају како би се систем учинио отпорнијим на познате претње. Ово, такође, прати процена рањивости и угрожености штићених вредности (Rodehorst et al. 2018). У складу са академским налазима, институције у САД, Уједињеном Краљевству и чланицама Европске Уније развиле су своје оквире за идентификацију критичних штићених вредности. У пракси, најчешће се као солуција подразумева унапређење ресорпције поремећаја путем стандардизованих планова и процедура, а што указује на доминантност инжењерског схватања отпорности и усмерености на отпорност првог реда. Ипак, ASIS ORM.1-2017 стандард наглашава да је проактиван менаџмент ризиком (антиципаторни капацитет) предуслов унапређења ресорптивних, али и адаптивних капацитета.

Антиципирање ризика организацији омогућава разумевање ефеката потенцијалних ризика на организационе циљеве или штићене вредности (Hamel and Välikangas 2003, Starr et al. 2003). Организационим праксама у домену предвиђања ризика, неочекиваних догађаја и могућих развоја ситуација организациони системи могу смањити своју рањивост и изградити свест запослених и доносиоца одлука (Hillmann & Guenther 2020, 6; Burnard & Bhamra 2011; Hamel and Välikangas 2003). Поједини аутори истичу да се може постићи кроз размишљање о многоструким будућностима (Välikangas & Romme 2012, Ramirez et al. 2010). На пример, планирање сценарија може унапредити способност за препознавање или предосећање будућих ситуација код доносиоца одлука и запослених (Fink et al. 2005). Вогус и Сатклиф наглашавају да су организације које настоје да предвиде будуће догађаје склоније да предузимају континуирани надзор (скрининг) окружења и/или да врше симулације могућих неочекиваних догађаја (Vogus & Sutcliffe 2007, 2). Сагласно овим становиштима, ISO 22316:2017 стандард наводи да „високо отпорне организације отпорности имају капацитет да антиципирају и одговоре на претње и прилике и да се измене у условима неизвесности како би постигле своје стратешке и операционе циљеве."

Ипак покушај предвиђања могућих будућности може довести до слепила према другим догађајима који нису очекивани (Hillmann & Guenther 2020, 6). Због тога поједини аутори наглашавају способност за стварањем смисла, то јест осмишљавањем (*sensemaking*), које је према њима важније од способности антиципације. Осмишљавање је, према Вајку, кључна

способност јер она претходи решавању проблема или деловању (Weick 1993), и од суштинског је значаја за избегавање грешака (Chan 2011). Организације морају бити способне да осете или препознају промене и потенцијална ремећења и да их правилно интерпретирају (Burnard and Bhamra 2011; Weick 1993; Weick & Sutcliffe 2007; Whiteman & Cooper 2011; Gattringer et al. 2020). То је неопходно ради предузимања адекватног деловања кроз разумевање како новонастала ситуација, неочекивани догађај или промене у окружењу могу утицати на циљеве и успех организације (Hamel and Välikangas 2003; Weick & Sutcliffe 2007; Whiteman & Cooper 2011).

Антиципативни капацитет је користан за оне ризике који се могу предвидети и о којима постоји темељно разумевање (de Bruijne, Boin & van Eeten 2010, 22). Другим речима, антиципација је важан сегмент у изградњи отпорности првог реда. Ради унапређивања отпорности другог реда, то јест отпорности на нерутинске ризике и неизвесности, неопходно је брзо осмишљавање и деловање како би се доносиоци одлука упозорили на развој ситуације и пословање задржало у оквиру прихватљивих перформанси (Schulman et al. 2004), односно активно развили кризни одговори (Weick et al. 1999). За анализирање отпорности другог реда на нерутинске ризике и неизвесности, прикладније је посматрати примере праксе осмишљавања, те ће на њима бити фокус у студији случаја у овој дисертацији.

1.2.2.5.4.2. Ресорптивни капацитет

Способност за реаговање на догађај, односно ресорпциони капацитет, укључује истрајавање и подношење утицаја реметилачког догађаја уз одржавање функционисања и минимизирање настале штете (Fleming 2012; Gilly et al. 2014, Starr et al. 2003; Stephenson 2010; Weick & Sutcliffe 2007). Ресорпциони капацитет обухвата развијање могућих опција за одговор у што краћем временском року (Acquaah et al. 2011; Mallak 1998), са посебним нагласком на способност импровизовања (Weick 1993, Ray et al. 2011).

У литератури о организационој отпорности се тематизује одговор на значајне поремећаје који су последица било организационих слабости, било изненадних екстерних догађаја (тј. манифестације нерутинских ризика). Суочени са значајним поремећајем актери, укључујући доносиоце одлука, налазе се у недоумици о активностима које је неопходно предузети, те настоје да генеришу лепезу могућих одговора (Williams et al. 2017, 747). Најефектнији одговори су они који укључују иновативно и спонтано понашање, као и способност импровизације (Stacey 1995, 478; Shepherd & Williams 2014, 977). Како Вилијамсон и сар. Истичу, способност функционисања након значајног поремећаја зависи од когнитивних и бихејвиоралних одговора организације, а које је такође контекстуално одређено (Williams et al. 2017, 747).

Когнитивни одговор на поремећај укључује способност актера да примети, тумачи и анализира промене у окружењу и да формулише одговоре (Dewald & Bowen 2010). Према томе, примећујемо да се когнитивни одговор у великој мери подудара са осмишљавањем, па се код нерутинских ризика и неизвесности антиципаторни и ресорптивни капацитети делимично преклапају. Когнитивни одговори који олакшавају прилагођавање на неповољне услове помажу доносиоцима одлука да примерено усмере пажњу, фокусирајући се на најбоље расположиве опције за умањење комплексности и генерисање алтернатива о могућим правцима даљег развоја ситуације (Lengnick-Hall & Beck 2005). У условима манифестације нерутинских ризика доносиоци одлука налазе се пред бројним изазовима. Они често не могу да процесуирају опсег и број информација потребних за доношење правовремене одлуке неопходне за адекватан одговор и координацију између бројних компоненти система. Према томе, организационе перформансе у комплексним окружењима у условима неизвесности нужно су ограничене капацитетом обраде информација (La Porte 1975). Што су доносиоци одлука у бољој позицији да разумеју садржај и

трајање поремећаја, затим начине на који промене индуковане поремећајем утичу на шире окружење, и напокон које структуралне, процедуралне или друге организационе промене треба предузети, вероватније је да ће систем одржати позитивно функционисање у новом окружењу (Lengnick-Hall & Beck 2005).

Као што је поменуто у претходном потпоглављу, за третирање поремећаја узрокованих манифестацијом нерутинских ризика, флексибилан процес одлучивања је од кључног значаја јер ригидно одлучивање може допринети повећању утицаја нежељеног догађаја (Bonanno et al. 2010; Hobfoll 2011; Rahmandad & Repenning 2016).

Бихејвиорални одговор је природни наставак когнитивног одговора који укључује деловање актера у третирању неизвесности из окружења. (Lengnick-Hall & Beck 2005, Weick 1993) Како наводе Ленгник-Хол и Бек „позитивни бихејвиорални одговор је машина која покреће актера суоченог са неизвесношћу“ (Lengnick-Hall & Beck 2005, 751). Према Сатклифу и Вогусу бихејвиорални одговори у кризним ситуацијама чине баланс између разноврсних могућности деловања и функционалних навика (рутина за управљање неизвесношћу, нпр. примена кризних и контингентних планова) (Sutcliffe & Vogus 2003, 107).

Поред уопштених стратешких поступака као што су хоризонтална хијерархијска устројеност, флексибилност планирања, склоност ка импровизацији и доступност слободних ресурса, емпиријске студије дају преглед и специфичних организационих активности којима се олакшава прилагођавање одговора на неочекиване поремећаје. (Williams et al. 2017, 748). Бечки и Окхујсен су утврдили да специјалне полицијске јединице (SWAT) и запослени у филмској индустрији развијају критичне социо-когнитивне ресурсе за управљање неизвесностима кроз технике „бриколажа“, укључујући замене улога, реорганизовање организационих рутина и рашчлањавање радних задатака (Bechky & Okhuysen 2011). Тимови хитне медицинске помоћи пружају брз, координисан и поуздан одговор у стресним ситуацијама уклањањем хијерархијских и бирократских структура кроз специфичне кризне активности (нпр. брзо делегирање, темељна обука нових чланова тима), што опет показује како отпорни тимови налазе баланс између структуре и импровизације када су суочени са динамичким и непредвиђеним догађајима (Klein et al. 2006).

Одговор такође зависи и од контекста, односно окружења организације и њених односа са системима у окружењу. Током и након нежељеног реметилачког догађаја актери могу добити нове увиде и перспективе о неопходним ресурсима, организационим променама, адаптацији, припреми и одговору на догађај (Williams et al. 2017, 749). Организације се могу разликовати по богатству социјалног капитала, а што такође може бити од значаја за њену отпорност. Мреже контаката са заједницом у којој се организација налази, као и са другим организацијама омогућава доступност разних ресурса у кризним ситуацијама, као што су информације, финансијски ресурси (зајмови и кредити), склоништа и привремени објекти, те емоционална и психолошка подршка (Aldrych & Meyer 2014; Shepherd & Williams 2014). ISO 22316:2015 стандард такође, наводи елементе социјалног капитала ка што су поверење, лојалност и посвећеност изградњи морала запослених, као веома важне за унапређење организационе отпорности (ISO 22316:2015, 4).

Различити типови социјалног капитала могу обављати комплементарне функције у подршци појединцу или организацији да ресорбују реметилачки догађај и опораве се након њега. Јаке социјалне везе преводе се у више нивое поверења и шире дељене норме унутар заједнице (Coleman 1990). Велики број студија показао је да локални контакти уобичајено служе као први пружаоци одговора (first responders) у кризним ситуацијама и несрећама, знатно пре

професионалних и формализованих спасилачких операција (Williams et al. 2017, 749; Quarantelli & Dynes 1977, Kapucu 2008). Комфортова је приметила да координација активности у условима неизвесности укључује разумевање подељеног ризика (Comfort 2002). Када се ризик дели, одлуке једне особе могу повећати или умањити укупни ниво ризика за све укључене актере и заједницу (Comfort et al. 2001, 145).

1.2.2.5.4.3. Ресторативни капацитет

Ресторативни капацитет, то јест капацитет опоравка укључује склоност ка не само пуком преживљавању већ и задржавању мање или више истих структура и функција (Freeman et al. 2004; Lampel et al. 2014;), као и брзину којом се организација враћа у стање пре догађаја или на неко друго циљано стање (Acquaah et al. 2011; DesJardine et al. 2017). Ипак, како Дарков примећује, концепт опоравка као повратка на стање пре догађаја је проблематичан из три разлога:

- Подразумева се да постоји неки лако одређени статус-кво који је потребно поново досећи;
- Ствара се утисак да постоји само један пожељан исход опоравка;
- Повратак на "старо", као мера отпорности организације би укључила "назадовање у времену" (Boin et al. 2010, 8). Колико времена треба да прође пре него што закључимо да ли је организација отпорна, односно у којој временској тачки можемо закључити да је организација неотпорна? Да ли би требало примењивати различите временске хоризонте за различите типове криза и различите врсте организација? Одговори на ова питања била би арбитрарна и без могућности теоријске концептуализације (Darkow 2018, 7).

Комплексне кризе као манифестације нерутинских ризика могу узроковати константне преласке из фаза одговора у фазу опоравка, а оне могу тећи и паралелно, па понекад дистинкција између ова два капацитета и/или фазе може бити магловита. Нерутински ризици ће услед свог високог утицаја углавном имати ефекат на шира географска подручја, али се тај ефекат не мора једнако осећати у сваком тренутку у свакој тачки. Уколико узмемо за пример пандемију COVID-19, различита географска подручја имала су тзв. „пикове", значајна повишења броја регистрованих случајева, у различитим временским периодима. Затим, вирус је мутирао, препоруке надлежних међународних и државних институција су се мењале током пандемије. У свим тим случајевима је одговор (ресорптивни капацитет) текао паралелно са опоравком (ресторативни капацитет).

Активности у фази опоравка често су стандардизоване кроз систем менаџмента континуитетом пословања, о којем је било речи у претходном поглављу. С друге стране, доносиоци одлука и запослени у организацији се током опоравка сусрећу са бројним изазовима који те активности могу отежати и понекад онемогућити. Препреке опоравку могу бити физичке (нпр. инфраструктурна оштећења у окружењу, болест већег броја запослених, итд.), али често и психичке које се огледају кроз страх и стрес запослених и доносилаца одлука, нарочито у случају актуализације ризика са високим негативним атрибутима хазарда (Riddle 2015).

Напокон, међуповезаност са другим системима (операторима критичне инфраструктуре, организацијама у ланцу снабдевања, хитним службама, експертским институцијама и мрежама) у смислу заједничког осмишљавања и промишљања одговора и активности опоравка од кључног је значаја за оснаживање ресторативног капацитета (Gibson & Tarrant 2010).

1.2.2.5.4.4. Адаптациони капацитет

Како смо претходно навели анализирајући реститутивни капацитет, повратак на старо (bouncing-back) често није могућ, а ни пожељан. Мек Фарлејн и Норис сматрају да када су кризе потенцијално трауматични догађаји који стварају колективно искуство, отпорност се може постићи само кроз колективно осећање нове нормалности, која не може бити дефинисана ex-ante (McFarlane & Norris 2006, 4). Такође, организације које искључиво планирају опоравак у смислу на стање пре догађаја могу занемарити прилике за учење и иновацију и искористити новонастале околности (D'Adderio 2014, 1325; Darkow 2018, 7).

Адаптација обухвата прилагођавање ресурса, интерперсоналних процеса и организационих рутина у циљу третирања утицаја реметилачког догађаја (Danes et al. 2009; Glover 2012). Она означава производњу динамичких способности за унапређивање и прилагођавање унутрашњих вештина и способности (Lengnick-Hall et al. 2011; Limnios et al. 2014; Wildavsky 1989).

У социо-техничким системима људско деловање модификује отпорност система, те је прилагодљивост система узрокована друштвеним фактором (Walker et al. 2006). Када постојећи систем постане неодржив, може се развити нови оквир стабилности кроз адаптивно управљање, а што захтева промене које неће утицати на структуру нити функционисање система и његове способности самоорганизације, учења и прилагођавања (Walker et al. 2002; Walker et al. 2006; Ridley 2017). У студијама социо-еколошких система адаптивни капацитет односи се на механизме за стварање нових структура и вредности и учење (Bhamra et al. 2011, 19). Према Галопину адаптивни капацитет система повезан је са капацитетом за одговор, а дефинисан је као способност система за еволуирање како би се прихватиле претње или промене из окружења, као и способност за проширивање опсега варијабилности (Gallopin 2006). Варијабилност је битан појам у кибернетици и теорији система. Такозвани „Ешбијев закон" гласи да што је већа разноликост акција доступних систему, то је већа разноликост пертурбација, које он може да прихвати (Ashby 1956). Једноставно речено, ако је опсег стратешких алтернатива које организација истражује знатно ужи од ширине промена у окружењу, пословање ће бити жртва поремећаја и промена (Hamel & Valikangas 2003, 7). Организације које су усмерене на адаптивни капацитет нису пасивне према променама у окружењу, већ континуирано развијају и примењују нова знања у односу на њихово оперативно окружење. Самим тим, адаптивни капацитет организације боље помаже приправности за поремећаје и неизвесности (Bhamra et al. 2011, 21).

Према ISO стандарду 22316 адаптивни капацитет јесте домен до кога се организација или појединац могу прилагодити низу услова који одступају од нормалних очекивања и обезбедити ефикасан и одржив одговор за суочавање са променљивим околностима (ISO 22316: 2015, 7). Адаптациони капацитет је производ широког низа способности које укључују способност за антиципирање, одговор и опоравак од реметилачких догађаја. Ове способности су често подржане утемељеним процесима као што су менаџмент ризиком и континуитетом пословања, а које су обично главни процеси за унапређивање отпорности. Предуслов ефикасног адаптивног капацитета су агилне и флексибилне пословне структуре и системи менаџмента који би им омогућили да се адаптирају на променљиве околности (ISO 22316:2015, 4).

Дакле, адаптација је капацитет који је прожима и унапређује све остале капацитете, другим речима, није везан за временску фазу t+1, како се најчешће подразумева.

Адаптација се може уградити у организациони систем применом праксе динамичког алтернативног планирања. Свако планирање се тиче неке будућности. Статички план је заснован на јединственој и неупитној будућности, која се заснива на екстраполацији трендова,

или је статички „робустан“ план развијен који ће довести до прихватљивих исхода у малом скупу вероватних будућих светова. Међутим, уколико се испостави да је реална будућност другачија од хипотетичке, план може пропасти (Walker et al. 2019, 53). Такође, временом се околности мењају а што статички планови не могу предвидети, те врло брзо могу бити застарели. Приступ планирања за услове неизвесности у литератури се назива Динамичко адаптивно планирање (ДАП). Овај приступ је прво осмишљен од стране Вокера и сар. 2001. године, да би се затим кроз примену у различитим секторима критичне инфраструктуре (саобраћај, водопривреда, енергетика) и у различите сврхе утемељио као алат стратешког планирања до краја прве деценије XXI века (Walker et al. 2001, Rahman et al. 2008, Marchau et al. 2009, Kwakkel et al. 2010). Приступ се заснива на спецификацији скупа циљева и ограничења, изради иницијалног плана који се састоји од краткорочних активности, као и успостављања оквира за будуће (контингентне) активности. Овакав план se експлицитно израђује у циљу адаптације на измењене околности (Walker et al. 2019, 53). ДАП се изводи у две фазе: прва, у којој се даје нацрт плана, програма за мониторинг и различитих активности пре и после имплементације, те друга фаза имплементације у којој се спроводе плана и програм мониторинга те преузимају корективне акције у случају нежељених догађаја (Walker et al. 2019, 53).

Овакво планирање је до сада било експлицитно имплементирано само на стратешком нивоу. Међутим уградњом његових постулата у планове одговора на ризик, кризне планове и планове континуитета пословања видимо простор за њихово унапређивање како би обухватиле неизвесности и нерутинске ризике, чиме би се позитивно утицало на отпорност другог реда.

Адаптација се у литератури често повезује са појмом организационог учења. Претходна искуства са нежељеним догађајем у вези су са потоњом отпорношћу, мада постоји значајна варијанца у природи овог односа (Brewin, Andrews & Valentine 2000; Bonanno, Westphal & Mancini 2011). Студија Бонана и сар. показала је да индивидуална отпорност на одређени догађаја зависи од сличности тог догађаја са неким догађајем доживљеним у прошлости, али не са неким различитим типом догађаја (Bonanno et al. 2010). Отпорност, дакле, може бити олакшана искуственим „наученим лекцијама“. Ипак, то учење није линеарно нити статичко (Williams et al. 2017, 749). Организације осцилирају између периода наглашавања безбедности и периода наглашавања других циљева, као што су ефикасност или иновација (Haunschild, Polidoro & Chandler 2015). Самим тим, способност учења из искуства слаби протоком времена, а што негативно утиче на рањивост организације. МекДоналд и Вестфал примећују негативне последице учења од других организација које су имале слична искуства, јер повратна информација може довести до погрешног тумачења сигнала о неповољним условима у окружењу што даље може довести до организационе кризе (McDonald & Westphal 2003).

Излагање неповољним условима такође утиче на то како доносиоци одлука тумаче будуће изазове и поремећаје, идентификују адекватне задатке и односе како би се они решили (Williams et al. 2017, 749). Поједине студије указују на то да претходна изложеност поремећајима може и негативно утицати на отпорност. На пример, континуирани прекиди рутина и задатака могу утицати на неразликовање „шума“ од „правих“ сигнала проблема (Rudolph & Repenning 2002). С друге стране, поједини нови сценарији се чине тако невероватним да актери не могу да их уклопе у постојеће виђење света (Cerulo 2008), а што резултира релативно ниским степеном учења и одговора.

Како су нерутински ризици по својој дефиницији ретки и неочекивани догађаји, те непостоји могућност примене научених лекција из сличних догађаја, уска дефиниција адаптивног капацитета као примене организационог учења није адекватна за ово истраживање.

Свакако, примена искуствених решења из сличних догађаја, било да је у питању лично или секундарно искуство, може олакшати осмишљавање, реаговање и опоравак, међутим адаптацију посматрамо шире као способност за прилагођавање услед флексибилности планова и процедура и хоризонталног хијерархијског устројства и позитивном ставу ка импровизацији приликом суочавања са неочекиваним догађајем.

Адаптацију посматрамо као капацитет који прожима и утиче на све друге капацитете отпорности: у антиципацији њен утицај је важан на процесе планирања одговора и оporавка, као и едукације и обука, у ресорпцији и ресторацији – на прилагођавање когнитивног и бихејвиоралног одговора.

1.2.2.5.5. Аспекти организационе отпорности

Широко коришћен модел за организациону отпорност је Гибсонов и Тарантов модел рибље кости (Gibson and Tarrant 2010). Овај модел препознаје да организација поседује значајан опсег способности и предузима низ активности (колективно оно што организација „ради“) које доприносе отпорности. У нашем истраживању ћемо „способности“ и „активности“ назвати тврдим аспектом отпорности. С друге стране, организација такође показује бројне карактеристике („како“ организација функционише), које утичу на ефикасност способности и активности и самим тим утичу на унапређење отпорности организације. У нашем истраживању „карактеристике“ називамо меким аспектом отпорности.

Док је већина тврдих и меких аспеката критична за функционисање у рутинском окружењу, начин на који се могу прилагодити нерутинском окружењу ће створити отпорност. Неколико тврдих аспеката је специфично за функционисање у нерутинском окружењу, као што су континуитет пословања, управљање кризама и ванредним ситуацијама. Међутим, постоје неке карактеристике које заиста долазе до изражаја у помагању у стварању отпорног стања помажући свим аспектима организације да боље функционишу у нерутинском окружењу. Неки од ових критично важних фактора укључују:

- Изоштреност – способност препознавања онога што се догодило у прошлости и повезивање са новонасталом ситуацијом или надолазећим ризиком; свест о ситуацији – шта се дешава сада и предвиђање – разумевање шта би се могло догодити у будућности. Изоштреност пружа могућност преузимања информација и идентификовања индикатора раног упозорења о драматичним променама и пружа разумевање могућих опција за решавање тога.

- Толеранција двосмислености – способност да се настави са доношењем одлука и предузимањем акција у временима велике неизвесности.

- Креативност и агилност – изналажење нових начина за решавање проблема брзином која одговара променљивости.

- Суочавање са стресом – да људи, процеси и инфраструктура настављају да функционишу под растућим захтевима и неизвесношћу.

- Способност учења – способност организације да користи лекције из свог и туђег искуства како би боље управљала преовлађујућим околностима, укључујући коришћење лекција у реалном времену како се појаве (Gibson and Tarrant 2010).

Релативни допринос и важност отпорности сваке од способности, активности и карактеристика зависиће од природе променљивих околности са којима се организација суочава. (Ibid)

Активности и способности укључују: управљање, процесе доношења одлука, усклађеност, управљање ризиком, комуникацију, обученост запослених, БЦМ и управљање кризама, инфраструктуру и технолошку способност, управљање ванредним ситуацијама, управљање односима, способност ресурса, финансијско управљање (Ibid).

Карактеристике укључују: лидерство, стратешку сигурност, културу, суочавање са стресом, вредности, оштрину, понашање, способност учења, поверење, агилност, креативност, међусобне везе, толеранцију на двосмисленост (Ibid).

1.2.2.5.5.1. Аспекти и способности – тврди аспект организационе отпорности

Активности и способности у моделу отпорности представљају, у извесној мери, мерљиве елементе и стога се може тврдити да се овај спектар модела може сматрати опипљивијом или „тврдом“ страном отпорности. Ове активности и способности ће највероватније бити присутне у многим врстама организација (van Maaren 2022, 202).

Отпорна организација може ефикасно ускладити своју стратегију, системе управљања, операције, структуре управљања и способности доношења одлука на такав начин да се организација може прилагодити променљивим ризицима и околностима и може преживети поремећаје и користити их за стварање предности (Starr et al. 2003, Parsons 2010). Активности као што су управљање континуитетом пословања и управљање кризним ситуацијама – изузетно су важне за организације које раде у нерутинским окружењима као што су кризе и генерално се сматрају важним факторима који доприносе отпорности организације (Cerullo and Cerullo 2004; Herbane et al. 2004; Elliot et al. 2010; Speight 2011, Tracei et al. 2017).

Неколико других активности и могућности је укључено у модел, као што су инфраструктурна и технолошка способност, управљање односима, усклађеност и финансијско управљање. Према Парсонсу, од виталног је значаја да организација има довољно знања о међузависности са стејкхолдерима и регулаторима и како да се придржава правила и прописа који их се тичу (Parsons 2010). Штавише, поседовање сигурног финансијског управљања – на пример финансијске или континуалне резерве – сматра се важним фактором који доприноси отпорности (Gibson and Tarrant 2010).

Укратко, на организациону отпорност могу утицати многи мерљиви фактори које Гибсон и Тарант (2010) описују као активности и способности. Организација треба да буде у стању да обавља ове активности и да користи ове способности иу рутинским и у нерутинским окружењима и околностима како би постала отпорнија.

1.2.2.5.5.2. Карактеристике – меки аспект отпорности

Друга страна модела отпорности рибље кости може посматрати као „мекше“, „нематеријално“ понашање организације. Меки аспект утиче на начин на који организација функционише и у рутинским и у нерутинским ситуацијама. Севил и др. (Seville et al. 2006) наглашавају важност карактеристика и тврде да проблеми са отпорношћу утицаји су често повезани са меком и мање опипљивом страном отпорности организација, укључујући културу организације, лидерство и визију. Добра комуникација и развијени односи поверења са кључним, интерним и екстерним, заинтересованим странама су од суштинског значаја за организациону отпорност (Ibid). Ово подржава претпоставку да карактеристике својствене

организацији могу у великој мери утицати на перформансе активности и способности (тврдом аспекту отпорности), што све доприноси отпорности организације.

Нарочито нерутинске околности одликоване високим степеном неизвесности захтевају од организација да има јаку и уједињену сврху, стратегијску сигурност и висок ниво суочавања са стресом (Gibson and Tarrant 2010; Parsons 2010). Такође, многи аутори верују да организација треба да пружа довољно простора за креативност и окретност и на управљачком и на оперативном нивоу како би се омогућило организација да ради на нове, иновативне начине, а што је неопходно у нерутинским условима. Поред тога, тврди се да организација треба да поседује одређени степен способности за учење како би се применила сопствена искуства и научене лекције, као и искуства других организација (Gibson and Tarrant 2010).

1.2.2.6. Закључак

У овом поглављу покушали смо да комплексни концепт отпорности сагледамо кроз призме различитих приступа и научних дисциплина, са фокусом на истраживања која су тематизовала отпорност организационих система.

Затим, разматрањем проблема отпорности из углова жељеног стања, процеса и стратегије управљања ризиком, дошли смо до закључка да би из перспективе студија безбедности овај последњи приступ потенцијално могао бити најплоднији за даља истраживања и концептуализацију у овој научној дисциплини.

За операционализацију појма отпорности закључили смо да би било корисно рашчланити овај сложени концепт на димензије, нивое, капацитете и аспекте, чиме смо дошли до варијабли које смо пилотирали у истраживачком делу дисертације.

Напокон, сматрали смо корисним да у оквиру овог поглавља анализирамо додирне и дивергентне тачке појмова организационе отпорности, кризног менаџмента и менаџмента континуитетом пословања будући да се ови концепти преплићу и понекад изједначавају. У овој дисертацији организациону отпорност посматрамо као појам вишег реда у односу на кризни менаџмент и менаџмент континуитетом пословања, будући да њих посматрамо као тврде аспекте ресорпционог и ресторативног капацитета.

1.3. Критична инфраструктура

Појава концепта критичне инфраструктуре у политичком лексикону Запада може се објаснити променама које су најпре настале у перцепцији претњи и све већом међуповезаношћу разних инфраструктурних елемената, што заједно чини друштво изузетно рањивим на разне врсте напада и отказивања критичних инфраструктурних система (Ракић 2015, 58).

Појам „критична инфраструктура“ односи се на имовину која укључује физичке и рачунарске системе од есенцијалног значаја за обезбеђивање економске и политичке стабилности земље (Radvanovsky & Mc Dougall 2010, 3). Ови системи, заправо, представљају оквир међузависних мрежа и система одређених индустрија, институција (укључујући људе и процедуре) и капацитета за дистрибуцију који пружају поуздан проток производа и услуга неопходних за одбрамбену и економску сигурност земље, неометано функционисање власти на свим нивоима, као и друштва у целини (Кековић и Нинковић 2020, 11). Критична инфраструктура обухвата, али није ограничена на, енергетске системе, телекомуникације, саобраћај, воду, храну, банкарске системе и финансије, цивилну администрацију, укључујући владин и приватни сектор (Radvanovsky & McDougall 2010, 3). Ниједна подела критичне

инфраструктуре није апсолутна, већ је углавном заснована на проценама стручњака и/или доносиоца политичких одлука (Кековић и Нинковић 2020, 11).

Упркос великом броју дефиниција критичне инфраструктуре, универзална дефиниција овог појма још увек не постоји. Ипак, све дефиниције усмерене су на чињеницу да критичност одређене инфраструктуре представља њен кључни значај за обезбеђивање виталних функција друштва и државе. Према Закону о критичној инфраструктури Републике Србије, критична инфраструктура подразумева „системе, мреже, објекте или њихове делове, чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије“ (Закон о критичној инфраструктури РС 87/2018, Члан 4). Министарство за отаџбинску безбедност Сједињених Америчких Држава дефинише критичну инфраструктуру као „вредности, системе и мреже, физичке и виртуалне, који су од толико виталног значаја за Сједињене Државе да би њихово уништење или онеспособљавање ослабило безбедност, државну економску безбедност, јавно здравље или сигурност, или било коју њихову комбинацију“ (Department of Homeland Security 2012).

Националне дефиниције се разликују по критеријумима које користе за одређивање критичности инфраструктуре. Највећи број држава и институција користи унакрсне критеријуме који дају прелиминарну идентификацију инфраструктуре у свим секторима. Након тога, секторски критеријуми се користе за прецизније одређивање дефиниција у оквиру сваког појединачног сектора. У појединим државама ти критеријуми наглашавају циљ или сврху инфраструктуре (тј. инфраструктура је критична зато што има виталну функцију за друштво), док је у осталима акценат на тежини последица или ефектима дисрупције или уништења поједине инфраструктуре на друштво (тј. инфраструктура је критична зато што би њен губитак био катастрофалан за друштво) (Кековић и Нинковић 2020, 13).

Када говоримо о критичним инфраструктурама, увек морамо да имамо на уму да су оне комплексни системи који захтевају холистички приступ приликом промишљања њиховог деловања, интерних и екстерних извора угрожавања, важност за сектор којем припадају, као и зависности и међузависности са другим секторима и инфраструктурним објектима. Пошто би губитак постројења и мрежа које називамо критичном инфраструктуром, а надасве њихових производа и услуга, представљао велики проблем за функционисање друштва, једне или више држава, њихова заштита представља важан аспект националне, па чак и међународне безбедности. Услед свега тога заштита критичне инфраструктуре одвија се и на институционалном нивоу држава, али и на нивоу наднационалних ентитета, попут ЕУ и НАТО.

Основне варијабле које карактеришу критичну инфраструктуру су небезбедност, тј. изложеност различитим ризицима, комплексност, међуповезаност и међузависност. Како је реч о социо-технолошким, „комплексним адаптивним“ системима, оне су у сталној промени и флуксу како би се прилагодили, тј. адаптирали на промене у окружењу (Rinaldi Peerenboom & Kelly 2001).

Међузависност критичних инфраструктура је двосмерна зависност између две или више критичне инфраструктуре, при чему стање једне утиче или је у корелацији са стањем друге критичне инфраструктуре или обратно. (Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura, NN 47/2016). Критичне друштвене функције данас се значајно преплићу и концепт међузависности треба бити разматран за интероперабилност система заштите критичне инфраструктуре, јер поремећај у редовном функционирању или чак потпуна дисфункција

система, може се догодити унутар једног сектора, али и између више сектора који су погођени значајним утицајем (Mikac, Cesarec i Larkin 2018, 217). Дакле, осим тога што је међузависност значајан појам за заштиту критичне инфраструктуре, она је значајна и за отпорност критичне инфраструктуре. Риналди, Перенбом и Кели сматрају да се врсте међузависности разликују и да свака има своје особине и различит утицај на елементе инфраструктуре, као и да постоје четири главне врсте међузависности критичних инфраструктура: физичка, кибернетичка, географска и логичка (Rinaldi, Peerenboom & Kelly 2001).

Стога се у у сврхе заштите и отпорности критичне инфраструктуре на националном нивоу улажу напори у израду стратешких и законских аката који би требало да дефинишу појам критичне инфраструктуре, идентификују секторе критичне инфраструктуре, као и критеријуме за даљу секторску идентификацију конкретних постројења и мрежа, затим надлежности институција и државних тела, начине сарадње јавног и приватног сектора, као и националну контактну тачку за сарадњу са међународним институцијама и спровођење међународних стандарда и директива у овој области.

Крајем 2018. године Република Србија је донела Закон о критичној инфраструктури (*Закон о критичној инфраструктури*, Сл. гласник РС бр. 87/2018), ради нормативног регулисања ове области и као одраз потребе усклађивања са европским законодавством. Посебно је значајно да је законодавац дефинисао и поступак којим се системи, мреже објекти или њихови делови у одређеном сектору према критеријумима одређују као критична инфраструктура.

За спровођење поступка идентификације критичне инфраструктуре у одређеном сектору задужена су министарства надлежна за одређене области, при чему критеријуме за идентификацију критичне инфраструктуре и начин извештавања прописује Влада. С тим у вези, идентификација и одређивање критичне инфраструктуре у Србији врши се у секторима енергетике, саобраћаја, снабдевања водом и храном, здравства, финансија, телекомуникационих и информационих технологија, заштите животне средине и функционисања државних органа (Закон о критичној инфраструктури, члан 6). У јуну 2022. године донета је Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије којом се прописују критеријуми у сваком од наведених сектора.[11]

Поред осам наведених сектора, критична инфраструктура може се одредити и у другим секторима, на предлог министарства надлежног за одређену област, а у складу са овим законом. Коначну листу критичне инфраструктуре у Србији утврђује Влада, на предлог Министарства унутрашњих послова (Закон о критичној инфраструктури, члан 6). Изузетак представља критична инфраструктура у надлежности Министарства одбране и Војске Србије, чије се

[11] Треба напоменути да је знатан број оператора критичне инфраструктуре (или њихови поједини елементи) идентификован као велики технички системи од значаја за одбрану или да су у поседу или управљају објектима од значаја за одбрану према законском оквиру Републике Србије (Закон о одбрани „Сл. Гласник РС, бр. 116/2007, 88/2009, 88/2009 – др. закон, 104/2009 – др. закон, 10/2015 и 36/2018“, Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије „Сл. Гласник РС, бр. 18/92“, Одлука о објектима од посебног значаја за одбрану „Сл. Гласник РС, бр. 112/2008“, Одлука о великим техничким системима од значаја за одбрану „Сл. Гласник РС, бр. 41/2014, 35/2015, 86/2016 и 53/2017“). У Републици Србији под појмом објекти од посебног значаја за одбрану сматрају се објекти за које се проценом утврди да би њиховим оштећењем или уништењем, односно откривањем врсте, намене и локације, код којих се то чува у тајности, могле наступити теже последице за одбрану и безбедност. (Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије „Сл. Гласник РС, бр. 18/92“) Дакле, критична инфраструктура је као појам општији од појма објеката од значаја за одбрану земље (Николић, Ковач и Митић 2018, 180). Самим тим, они су делимично у надлежности Министарства одбране Републике Србије које може имати своје процедуре о заштити и управљању безбедносним ризицима.

коришћење, чување, заштита, контрола и надзор врше према одредбама Закона о одбрани и Закона о Војсци Србије (Ibid, члан 7). Закон дефинише заштиту критичне инфраструктуре као „скуп активности и мера које имају за циљ осигурање функционисања критичне инфраструктуре у случају ометања или уништења, односно заштиту у случају претњи и спречавање настанка последице ометања или уништења" (Ibid, члан 2). За разлику од заштите, концепт отпорности није присутан у нашем закону. Ово истраживање следи секторски приступ дефинисан Законом о критичној инфраструктури Републике Србије. Наиме, све организације које су укључене у истраживање припадају секторима идентификованим законом.

У складу са европским стандардима, Закон о критичној инфраструктури уводи појам оператора критичне инфраструктуре који је повезан са „државним органима, органима аутономне покрајине, органима јединице локалне самоуправе, јавним предузећима, привредним друштвима или другим правним субјектима који управљају системима, мрежама, објектима или њиховим деловима као критичном инфраструктуром" (Ibid). Оператори критичне инфраструктуре дужни су да израде Безбедносни план оператора за управљање ризиком, којим се дефинишу безбедносни циљеви и мере оператора на основу анализе ризика, и за њега прибаве сагласност Министарства унутрашњих послова најкасније шест месеци по одређивању система, мрежа, објеката или њихових делова за критичну инфраструктуру (Ibid, члан 8).

Поред тога, оператори критичне инфраструктуре морају имати официра за везу, као лице које служи за контакт између оператора и МУП-а, које обезбеђује сталну контролу ризика и претњи, обавештава о променама у односу на критичну инфраструктуру и о евалуацији ризика, претњи и рањивости, координира Безбедносним планом оператора за управљање ризиком, врши тестирања кроз вежбе и друге активности предвиђене планом и обавља све друге послове везане за критичну инфраструктуру. Официра за везу именује МУП, на основу предлога оператора критичне инфраструктуре из редова запослених, при чему то лице мора имати одговарајућу лиценцу. (Ibid, члан 9) Треба напоменути да институција официра за везу до завршетка овог истраживања није успостављена у оператерима критичне инфраструктуре у Републици Србији.

1.3.1. Отпорност критичне инфраструктуре

Међузависност инфраструктура на националном, регионалном и глобалном нивоу представља део проблема. Сложеност међусобно повезаних глобалних инфраструктура резултира непредвиђеним међузависностима и потенцијалом за домино ефекте који нису ни предвидљиви нити их је могуће избећи (Jin et al. 2021). Системски стресори као што су климатске промене, велике природне катастрофе, емергентне технологије и пандемије угрожавају оперативни капацитет инфраструктуре – посебно с обзиром на њихову повећану учесталост, непредвидљивост и интензитет (Horton et al. 2022, 220).

Као што смо истакли у поглављу о ризику, традиционални, пробабилистички приступ управљању ризиком заснива се на идентификовању претњи, повезаних вероватноћа и последица, анализу нивоа ризика, предлагање мера за његово смањење и предвиђање могућих сценарија. Овим приступом, то јест стратегијом, практично је немогуће у потпуности заштитити критичне инфраструктуре, будући да су оне комплексни и рањиви системи суочени са широким спектром комплексних природних хазарда и антропогених претњи које су такође еволутивне (Boin & McConnell 2007; Fritzon et al 2007; Cools & Pashley 2013; Curt & Tacnet 2018). Ова ситуација је погоршана убрзаним глобалним природним геополитичким и технолошким променама. Самим тим, корпус радова који тематизују отпорност критичне инфраструктуре нарочито се увећао након катастрофа које су погодиле америчку (Ураган Катрина) и јапанску (Фукушима) инфраструктуру, као и пандемију COVID-19.

Упркос неоспорном развоју и сазревању приступа традиционалног менаџмента ризиком, оне су и даље подложне озбиљним недостацима нарочито у контексту комбинованих природних катастрофа и технолошких акцидената (Curt & Tacnet 2018, 2). Ограничења пробабилистичких процедура менаџмента ризиком у критичним инфраструктурама могу бити приписана:

– Недостатку знања (непознате претње – „црни лабудови“) и квантитативним неизвесностима (неочекивана магнитуда природних феномена, манифестација догађаја занемарљиве вероватноће – тј. нерутинских ризика). Како истичу Бојн и МекКонел, кризно планирање је само по себи контрадикторно – како се може планирати одговор на догађај који по својој природи не одговара хипотезама које планери користе као основу за његову предикцију (Boin & McConnell, 2007)?

– Растућом комплексношћу великих социо-техничких система и комбинацијом организационих и техничких грешака што доводи до неочекиваних ситуација и/или домино ефекта услед јаких веза међузависности између инфраструктура (Curt & Tacnet 2018, 2). Критичне инфраструктуре реципрочно интерреагују услед све доминантнијег ослањања на информационо-комуникационе технологије (Vinchon et al., 2011). Унапређивање система менаџмента ризиком у контексту међуповезаних мрежа постаје прохибитивно финансијски али и у смислу потребног времена за њихову имплементацију (Linkov et al., 2014).

– Недовољно или лоше постављеним или одржаваним заштитним мерама (Kadri, Chatelet, & Chen, 2014; Landucci, Argenti, Tugnoli, & Cozzani, 2015).

– Грешкама у процедурама (грешке у примени или лоше постављене процедуре), неефикасне безбедносне обуке или предуго време одговора (Khakzad, Khan, Amyotte, & Cozzani, 2014; Landucci et al., 2015).

Према томе, критичне инфраструктуре су рањиве на претње и, услед међузависности, потенцијални трансмитери нежељених догађаја. Током догађаја мере управљања ризиком могу бити неутралисане, системи, организације и становништво суочено са непредвидивим развојем ситуације, а на која морају одговорити (Curt & Tacnet 2018, 2). Виталне друштвене функције морају бити поновно успостављене или се прилагодити новонасталим околностима што је брже могуће. Ови капацитети и планирање односе се на отпорност критичне инфраструктуре.

Као што је већ наведено у сегменту о организационој отпорности, отпорност критичне инфраструктуре производ је отпорности различитих димензија посматраног социо-техничког система: техничке (капацитета да испуни функцију, на потребном нивоу током и након нежељеног догађаја), организационе (капацитета организација да управљају инсталацијама, одржавају кључне функције, и доносе одлуке за одржавање/побољшање ситуације током догађаја), социјеталне (мере посебно осмишљене да смање ниво до којег заједнице и државне јурисдикције могу бити подложне утицајима узрокованим губитком критичних услуга услед догађаја, људско понашање током катастрофалних догађаја), и економске (способност смањења директних и индиректних економских губитака, алокација ресурса, одржавање активности).

Иако димензије отпорности нису независне, ова дисертација је искључиво усмерена на анализу организационе димензије, тако да ће остале димензије остати ван оквира истраживања.

У литератури, отпорност критичне инфраструктуре проблематизована је на два различита нивоа – макро – као система, односно мреже, критичне инфраструктуре на одређеном географском или административном подручју (националном, наднационалном и регионалном) и на микро-социотехничком, тј. организационом нивоу. Узевши у обзир значај које критичне инфраструктуре имају за државу и заједницу, у свим овим истраживањима се преплићу концепти безбедности, заштите и отпорности државе, заједнице и организације.

Макро ниво тематизује факторе који систем критичне инфраструктуре једне територије чине отпорним на екстерне, системске ризике, као што су, да поменемо само неке, климатске промене, енергетска зависност, власничка структура. Системски ризици превазилазе способност било ког система или дела система да их ефикасно контролише, што је иманентно модерном друштву, његовој комплексности и међузависности (Кековић, 2022). Дакле, овде се критична инфраструктура посматра збирно, као систем система, мрежа, објеката или њихових делова који могу узроковати поремећаје у функционисању друштва и становништва на одређеној територији. Другим речима, отпорност критичне инфраструктуре посматра се директно кроз призму националне безбедности. Такође, знатан број развијених држава развио је легислативне и стратегијске оквире који усклађују рад критичних инфраструктура и настоје да спрече појаву домино (каскадних) ефеката услед међуповезаности и међузависности критичних инфраструктура.

На другом, социо-техничком нивоу, студије посвећене отпорности критичне инфраструктуре, представљају подгрупу истраживања организационе отпорности. Значајан део тих истраживања посвећен је информационој инфраструктури, узевши у обзир међузависност информационе инфраструктуре и свих осталих сектора, значај за привреду и становништво, а такође и експоненцијално увећавање претњи у сајбер окружењу. О овим оквирима биће детаљније говора на наредним страницама овог поглавља.

1.3.1.1. Територијални (системски) ниво

Концепт отпорности критичне инфраструктуре на тлу одређене географске или административне површине предмет је бројних академских и стручних студија, али и легислативних и стратегијских докумената на регионалним, националним и наднационалним нивоима.

Академске студије које припадају овом приступу углавном се заснивају на инжењерском приступу моделовања система критичних инфраструктура на одређеној територији, идентификовању њихових зависности и међузависности, те техничким решењима и захтевима који могу утицати на умањење ризика од природних и антропогених ризика кроз јачање антиципативних ресорптивних, адаптивних и ресторативних капацитета отпорности (Biringer, Vugrin & Warren 2013; Lewis & Petit 2019; Macaulay 2008). С друге стране, ове студије приметно мало простора поклањају организационој и социјеталној димензији отпорности. Тако, веома цитирана монографија Биринgерове, Вугрина и Ворена из института Сандија, као главни резултат истиче развој Методологије процене отпорности инфраструктуре (IRAM – Infrastructure Resilience Assessment Methodology). IRAM се састоји од четири примарне компоненте – дефиниција отпорности усмерена на мерљивост, квантитативна методологија за мерење отпорности, структурни квалитативни приступ анализи отпорности, процес процене отпорности (Biringer, Vugrin & Warren 2013, 104).

Иста студија унутар капацитета отпорности идентификује елементе приказане у табели 3.

Табела 3 Капацитети отпорности (према Biringer, Vugrin & Warren 2013, 117-123)

Ресорптивни капацитет	**Адаптивни капацитет**	**Ресторативни капацитет**
Вишак инвентара крајњих производа или сирових материјала.	Супституција – способност замене компоненти система или кључних материјала.	Системи осматрања и раног упозоравања
Робусност – физичка заштита, техничка решења за ојачавање инсталација.	Измена маршрута (*rerouting*) – код транспортне, енергетске и ИКТ инфраструктуре.	Препозиционирање ресурса за хитни одговор у ванредним ситуацијама

Редундантност – бек-ап системи, алтернативне руте, добављачи.	Проналажење нових добављача.	Уговори о реципрочној помоћи и мреже подршке
Сегрегација – физичко раздвајање постројења, логичко раздвајање дигиталних мрежа, географска дисперзија добављача.	Конзервација или рационирање – умањена потрошња постојећих ресурса.	
	Реорганизација	
	Оригиналност, креативност (ingenuity)	

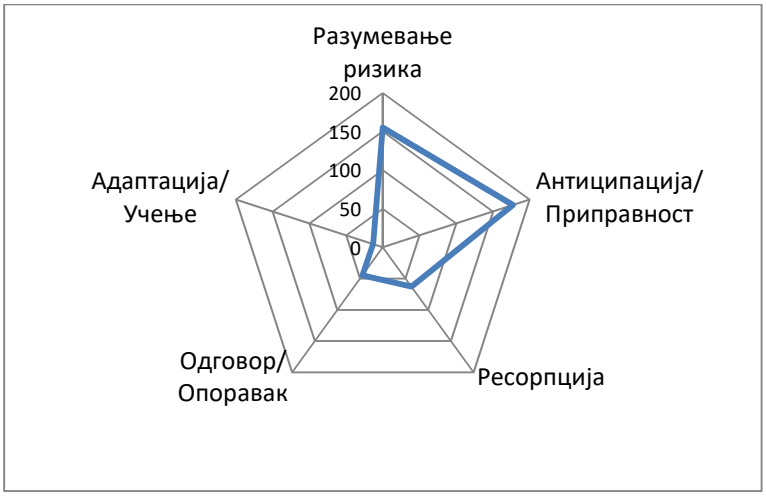
Видимо да је у овој студији веома мало пажње посвећено меким аспектима отпорности (капацитетима, према моделу „рибље кости“ Гибсона и Таранта), што имплицира да је фокус истраживања Бирингерове, Вугрина и Ворена отпорност првог реда критичне инфраструктуре, то јест отпорност на познате претње.

1.3.1.2. Организациони ниво

Истраживања отпорности критичне инфраструктуре на микро нивоу, тј. на нивоу организације, као елемента система критичне инфраструктуре једне територије, полазе од имплицитне премисе да је систем критичне инфраструктуре отпоран онолико колико су отпорни његови елементи – сектори и организације, услед јаких веза међузависности између елемената. Ове студије могу бити фокусиране на један или више сектора критичне инфраструктуре, и такође на једну или више димензија (организациону, економску, техничку или социјеталну) отпорности.

Детаљном анализом литературе спроведеном током писања ове дисертације, закључили смо да су емпиријска истраживања о организационој димензији отпорности најприсутнија у секторима здравства, енергетике (нарочито подсектора нафте и гаса и дистрибуције електричне енергије) и саобраћаја, док су, на пример, истраживања у секторима финансија и телекомуникационих и информационих технологија превасходно усмерена на техничку (отпорност логичких мрежа на сајбер нападе, или на физичка или техничка оштећења настала услед различитих фактора), односно економску (доступност финансијких средстава услед поремећаја на тржишту) димензију.

Готово све новије емпиријске студије спроведене у организацијама критичне инфраструктуре усвајају теоријски приступ о четири капацитета отпорности: антиципацију, ресорпцију, опоравак и адаптацију (Bhamra et al. 2011; Hosseini et al. 2015; Martin-Breen and Anderies 2011; Wan et al. 2018, Singh 2021). Према свеобухватној прегледној студији Јовановића и сар. (2016) поред ова четири капацитета (то јест управљачке фазе), као засебна фаза идентификована је и разумевање ризика, то јест „осмишљавање“ (sensemaking). У периоду до писања те прегледне студије највећи број истраживачких напора усмерен је на фазе антиципације коју аутори изједначавају са приправношћу (n=170) и разумевања ризика (n=150), мањи број на фазе ресорпције (n=50) и рестраурације (n=60), док је капацитет, тј.фаза, адаптације била присутна у свега 10 анализираних јединица (графикон 5)



Графикон 5 – Дистрибуција литературе пронађене за сваку фазу циклуса отпорности инфраструктурних система. (Jovanović et al. 2016, према Singh, 2021.)

У докторској дисертацији Синга (Singh 2021, 4), адаптацији је посвећено релативно мало простора, упркос литератури из других области која истиче њену важност за сваки систем који настоји да буде отпоран, нарочито у околностима брзих и значајних промена окружења. Према Сингу, чија је дисертација усмерена на критичне транспортне инфраструктуре, у пракси приступања отпорности идентификација ризика, ресорпција шока (поремећаја) и брзи опоравак (повратка у нормално стање пре ремећења) узимају за критичне елементе отпорног система (Bruneau et al. 2003; Wan et al. 2018).

Синг даље истиче да је кључни разлог занемаривања адаптационог капацитета у транспортним системима недостатак квантитативне метрике перформансе за адаптацију (Singh 2021, 5). Адаптација не може бити лако квантификована, а одлучивање о јавним улагањима традиционално фаворизује објективне и мерљиве процесе при евалуирању и финансирању пројеката. Ово постаје значајан проблем услед растуће неизвесности повезане са будућим климатским сценаријима и учесталим екстремним догађајима, што интензивира потребу за развојем адаптивне отпорности у инфраструктурним системима (Ibid, 5).

Изузетно је значајна прегледна студија из 2021. године Бента и сар. о примени концепта организационе отпорности у нафтном и гасном сектору (Bento et al. 2021). Аутори су анализирали двадесет академских радова и утврдили да највећи број (n=16) експлицитно повезује безбедност и отпорност, а такође већина радова (n=13) почива на претпоставци да отпорност доприноси безбедности (Ibid, 5). У истој прегледној студији даље се наводи да, док поједини радови (Azadeh et al.2016) изједначавају отпорност са редундантношћу људства и опреме, други шире појам отпорности на способност самоорганизовања, тимског рада и свести о ризицима (Rabbani et al., 2019), те формализовање процеса одлучивања и управљања променама, адекватних обука запослених и развијање вештина за суочавање са неочекиваним догађајима (Thorogood 2013; Thorogood & Crichton 2014).

Албрехтсен указује на важност приступа заснованог на отпорности као допуне високо формализованој пракси менаџмента, утемељеној на поштовању и усаглашености са процедурама, а што у случајевима неочекиваних догађаја отежава адаптацију на новонастале околности (Albrechtsen, 2015). Мултиметодска студија Андерсена и Мостуеа препоручује приступ заснован на отпорности за унапређење безбедности система (Andersen & Mostue 2012).

Њихова студија случаја описује како се радници ослањају на различите праксе попут познавања рафинерије, претходног радног искуства и здравог разума приликом надгледања процеса, адаптације и антиципирања могућих исхода (Ibid, 2014-2015). Налази добијени у студији Андерсена и Мостуеа у великој мери одражавају четири капацитета отпорности на које је усмерена и ова дисертација.

Бенто и сар. истичу да је ипак у скоро свим (n = 19) анализираним студијама отпорност представљена као апстрактни конструкт, пре него као стратегија имплементирана у организационом окружењу која утиче на пословну праксу, а што је идентификовано као главни изазов за будућа истраживања (Bento et al. 2021, 8).

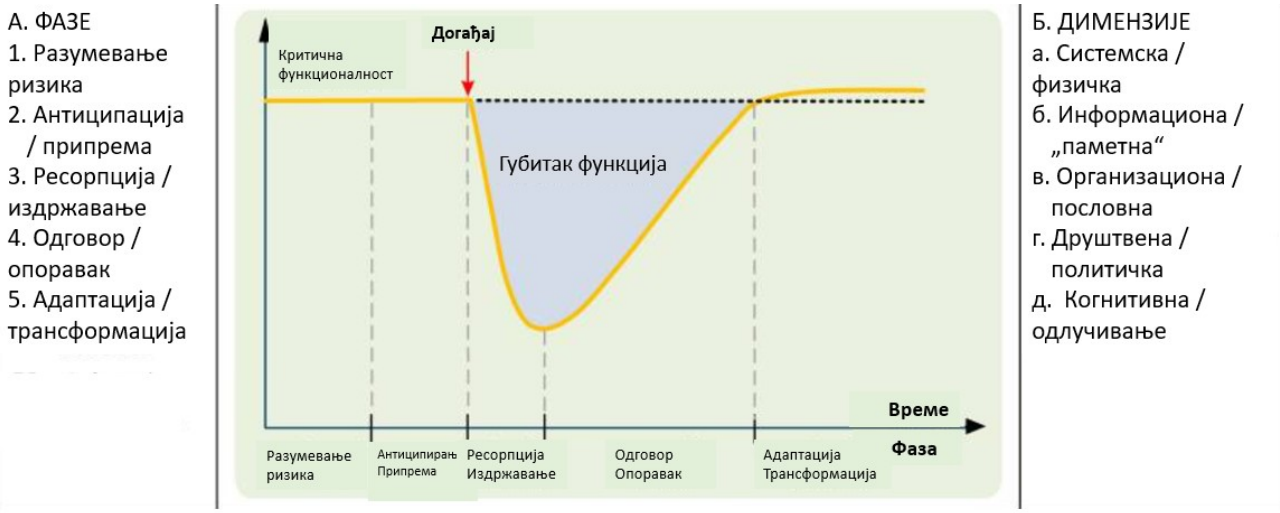
Пошто су организације комплексни системи, аналитички фокус би требало да буде на интеракцијама између елемената система, као почетног корака ка развијању иновативних пракси за промовисање отпорности на нивоу система. Ово практично значи да постоји потреба за разумевањем свакодневних неформалних процеса интеракције, који не могу бити у потпуности схваћени посматрањем формалних организационих структура. (Ibid, 9) У овом смислу, анализа друштвених мрежа (Borgatti et al. 2009; Borgatti, et al. 2018) омогућила је важне алате за идентификовање баријера за комуникацију, као и за анализу настајућих промена у структури неформалних интеракција у организацијама.

Аутори ове студије истичу да адаптациони процеси у вези са поремећајима у окружењу, као што је криза узрокована пандемијом коронавируса генеришу питања о учењу и променама у интеракцијама у организацијама критичне инфраструктуре (Bento et al., 9). Постоји потреба за разумевањем како ново знање настаје из кризних ситуација и како управљачке праксе могу поспешити адаптивне процесе (Ibid). У комплексним системима, ово обично укључује логику фацилитације пре него контроле (Sandaker, 2009).

Интегративна и свеобухватна анализа отпорности критичне инфраструктуре, предложена од стране Јовановића и сар. у оквиру пројекта *SmartResilience* помиње пет фаза:

1. Разумевање и антиципирање ризика, укључујући нове/емергентне ризике, који представљају претњу функционалности инфраструктуре, и покушава да да одговор на питање „шта може представљати нежељени догађај?“
2. Припрема за антиципиране или неочекиване реметилачке догађаје. Фаза укључује планирање и проактивне стратегије адаптације.
3. Ресорпцију њихових утицаја, која, према Јовановићу, укључује анализу рањивости и анализу могућег „домино ефекта“, тј. Стрмину и дубину кривуље ресорпције.
4. Одговор и опоравак односи се на стављање нежељеног догађаја под контролу што је брже могуће, утичући на трајање догађаја, као и стрмину позитивне кривуље опоравка, која показује брзину и степен нормализације функционалности.
5. Адаптацију/трансформацију инфраструктуре или њеног пословања засновану на наученим лекцијама. Ова фаза укључује разноврсне мере унапређења инфраструктуре и њеног окружења, које утичу на то колико је инфраструктура успешно прилагођена након догађаја и да ли је отпорнија и одрживија. Активности у овој фази воде ка припреми на будуће догађаје (Jovanović et al. 2018).

Јовановић и сар. у аналитички апарат укључују пет димензија – системску (физичку), информациону (паметну), организациону (пословну), друштвену (политичку) и когнитивну (одлучивање). Отпорност сваке димензије се, према овом моделу, динамички посматра кроз фазе. (Ibid)



Графикон 6 Фазе и димензије отпорности критичне инфраструктуре (Jovanović et al. 2018)

Јовановић и сар. применили су свој интегрални, свеобухватни концептуални модел на случају отпорности здравственог система Аустрије током пандемије COVID-19. У табели бр. 4 представљени су кључни индикатори према фазама и димензијама.

Табела 4 – Индикатори отпорности према фазама и димензијама (према Jovanović et al. 2018)

Фазе→ Димензије ↓	**Разумевање ризика**	**Антиципација/ припрема**	**Ресорпција/ издржавање**	**Одговор/ опоравак**	**Адаптација/ трансформација**
Системска/ физичка	Путање лечења пацијената. Токови транспорта пацијената између различитих типова институција здравствене заштите (лекари, болнице, апотеке)	Прилагођавање густине одређеног типа пружаоца услуга у одређеној регији како би се осигурала покривеност потреба становништва у случају догађаја.	Тријажа пацијената у циљу одређивања различитих нивоа хитности.	Нега и транспорт пацијената у складу са дефинисаним нивоом хитности.	Ревизија система менаџмента и прилагођавање планова деловања.
Информациона/ Подаци	Увођење система електронских здравстених досијеа на националном нивоу	Квантификација здравља популације у реалном времену, као функције демографских варијабли и места становања.	Константни мониторинг токова пацијената на нивоу здравствених институција	Константни мониторинг токова пацијената на нивоу здравствених институција	Континуирано ажурирање релевантних индикатора кључних перформанси – „паметна критична инфраструктура “
Организациона/ Пословна	Квантитативна и квалитативна анализа ризика	Додела улога, надлежности и хијерархијских схема укљученим организацијама и њиховом кључном особљу.	Спровођење акционог плана на нивоу индивидуалне здравствене установе (интерни догађаји) и на нивоу регије (екстерни догађаји).	Праћење чек-листа	Редовно вежбање сценарија и обуке за кључно особље

Друштвена/ Политичка	Улагање у инфраструктуру, политичке дискусије и преговарање између заинтересованих страна.	Формулисање заједничких планова деловања и обезбеђивање неопходних ресурса за њихово спровођење.	Дистрибуирање релевантних информација медијима, запосленима и другим заинтересованим странама.	Дистрибуирање релевантних информација медијима, запосленима и другим заинтересованим странама.	Редистрибуција фондова и улагања.
Когнитивна/ Одлучивање	Разумевање разлика између хитних процедура и рутинског пословања.	Антиципација догађаја који имају потенцијал за довођење до масовних жртава или драстичног смањења броја оперативних здравствених институција.	Идентификација релевантних претњи.	Праћење чеклиста и договорених процедура.	Унапређење координације између различитих здравствених установа и других релевантних организација.

Јовановићев модел је значајан за ово истраживање будући да истиче когнитивну димензију која је у начелу битна за постизање отпорности другог нивоа. Међутим, меки аспекти – карактеристике, не налазе се међу његовим индикаторима, већ су индикатори искључиво активности, што нам се чини као недостатак овог модела.

Адаптација у организационом окружењу обично подразумева учење и нове обрасце понашања, као и промене у структури мреже социјалних интеракција. Неколико анализираних радова (Bento and Garotti 2019; Carlson 2018; Grabowski and Roberts 2016; Johnsen 2012; Skjerve et al. 2012; Tveiten et al. 2012) у области отпорности сектора нафте и гаса помиње адаптивне процесе, али нема артикулације нити испитивања еволутивних процеса који доприносе отпорности. Ове студије претпостављају нормативну перспективу, фокусирајући се на индикаторе отпорности попут посвећености, свести и приправности (Bento et al 2021, 9). Поредећи ову студију са Синговом дисертацијом о транспортној инфраструктури видимо да долазе до истих закључака.

Будући да је услед деценија неолибералних политика знатан проценат критичне инфраструктуре у земљама „Запада“ у приватном власништву[12] (85% критичне инфраструктуре и кључних ресурса у САД, 80% у Европској Унији), контекст налаза студија о заштити и отпорности КИ се не може увек јасно пресликати на ситуацију у Републици Србији и региону. Стога је студија Далгард-Нилсенове (Dalgaard-Nielsen 2017) о реалним могућностима постизања организационе отпорности јавног сектора у Данској од изузетног значаја за ову дисертацију, услед чињенице да знатну већину критичне инфраструктуре у овој земљи, као и у Србији, представљају организације у државном власништву, те заслужује да се на њу да шири осврт.

Студија Далгард-Нилсенове показује како руководиоци настоје да уведу елементе организационе отпорности путем „виртуелних резерви“ и општих, флексибилних планова за ванредне ситуације (Dalgaard-Nielsen 2017, 339). Међутим, фискална штедња и страх од окривљавања (*blame game*) ограничавају руководиоце да делегирају овлашћења, инвестирају у

[12] Подаци објављени на званичним сајтовима наводе да је 85% КИ у САД (US Government Accountability Office 2009 https://www.gao.gov/assets/gao-09-654r.pdf) и 80-90% КИ у Европској Унији (Umbach 2023 https://www.gisreportsonline.com/r/europe-critical-infrastructure/, Limnell 2018 https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-6-Limnell.pdf Deutche Welle 25.10.2022. https://www.dw.com/en/germanys-critical-infrastructure-is-poorly-protected/a-63505983) у приватном власништву.

слободне ресурсе и отворе простор за експериментисање и иновације у циљу прилагођавања емергентним ризицима. Уочена потреба да се демонстрира политичка одговорност путем хијерархијске контроле, заједно са личним преференцијама руководилаца за линеарно и рационално вођство усмерено ка планирању додатно ограничава простор у којем се могу одвијати отпорне организационе праксе (Ibid 340).

Налази указују на потребу преиспитивања услова организацијске отпорности када су у питању организације јавног сектора. Према Далгард-Нилсеновој, широко распрострањено присуство отпорности као циља и решења у дискурсима о националној безбедности могло би да послужи да инспирише релевантна организациона прилагођавања, али организациона отпорност није „сребрни метак“ за руковање све сложенијим пејзажом претњи и опасности у контексту фиксних или умањених буџета јавног сектора (Dalgaard-Nielsen 2017,342).

Да би се истражило како свакодневна прагматика данске Владе обликује граничне услове отпорности у организацијама јавног сектора, Далгард Нилсенова је обавила полуструктуриране експертске интервјуе са дванаест извршних директора у бирократији националне безбедности Данске (Ibid). Како је студија била експлораторна и користила је експертске испитанике, одлучено је да се ослони на полуструктурисане интервјуе (Aberbach and Rockman 2002). Извршна перспектива је одабрана не зато што се од руководилаца очекивало да буду лично ангажовани у активностима отпорности на првој линији, већ зато што је требало да буду на челу преговарања о потенцијално супротстављеним притисцима и очекивањима усмереним на њихове организације. Очекивање аутора студије било је да њихово деловање игра значајну улогу у одређивању величине и природе простора унутар њихових организација у којој би се организационе праксе усмерене ка унапређењу отпорности могле одвијати (Dalgaard-Nielsen 2017,342).

Интервјуи нису директно приступили питању изводљивости политички наведених циљева отпорности, већ су истраживали потенцијалне компликације и дилеме кроз групе питања о приступима за суочавање са тренутним пејзажом претњи и опасности, спољним актерима и њиховим очекивањима, организационим приоритетима и променама циљева, менаџмента и специфичних активности управљања (Ibid).

Накнадна анализа је мапирала податке интервјуа са увидима о отпорним организационим дизајном и навикама извученим из анализе литературе. Конкретно, анализа је имала за циљ да утврди:

1. да ли су циљеви и приоритети организационог развоја испитаника компатибилни са дизајном и навикама отпорних организација,
2. који аспекти организационе отпорности су компатибилни/некомпатибилни са искуственом реалношћу руководилаца,
3. да ли тип и начин лидерства испитаника погодује примени организационе праксе усмерених на унапређивање отпорности (Ibid, 343).

Ова дисертација покреће слична питања у Републици Србији и земљама у окружењу у којима је удео критичне инфраструктуре у државном власништву већи, иако не постоје прецизни подаци о процентима. Како наводи Мићовић: „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.“ (Мићовић 2020, 27) Теренско истраживање спроведено током писања ове докторске дисертације се, дакле, у значајној мери ослањало на питања која је Далгард-Нилсенова покренула у Данској.

1.3.1.3. Приступ отпорности критичне инфраструктуре Европске Уније

На наднационалном нивоу Европске Уније почетке уређивања области критичне инфраструктуре можемо датирати у 2004. годину, када је Европски Савет (European Council) затражио од Европске комисије (European Commission, у даљем тексту ЕК) да припреми свеобухватну стратегију заштите критичне инфраструктуре. У Комуникеу који је Комисија упутила Европском савету и Европском парламенту, критична инфраструктура дефинисана је као „физичка и информационо-технолошка постројења, мреже, услуге и друге штићене вредности који, у случају онеспособљавања или уништења, могу имати озбиљан негативни утицај на здравље, безбедност, сигурност или економску добробит грађана или ефикасно функционисање влада држава Европске уније“ (COM/2004/0702 final). На сличну дефиницију наилазимо и у предлогу директиве ЕК о идентификацији европске критичне инфраструктуре (ЕКИ) из децембра 2006. године (CNS 2006/0276*). У финалној директиви из децембра 2008. године наводи се да „критична инфраструктура подразумева постројење, систем или њихов део смештен на територији држава чланица који је од суштинског значаја за одржавање виталних друштвених функција, здравља, сигурности, безбедности, економског и друштвеног благостања људи, а чије би онеспособљавање или уништење имало значајан утицај на државу чланицу као исход неодржавања тих функција“ (Directive 2008/114/EC). Ипак, ова директива третира искључиво два сектора европске инфраструктуре – енергетски и саобраћајни.

Овом директивом примењује се системски приступ у анализирању ризика и претњи, као и приликом креирања превентивних механизама и стратегија заштите критичне инфраструктуре (Кековић & Нинковић 2020). Осим приступа заснованог на отпорности и међузависности, Европска унија користи и следеће критеријуме критичности инфраструктурних система: економске ефекте, ефекте на животну средину и ефекте на јавност. Директива 2008/114/ЕК наглашава да критеријуми који се користе за утврђивање значаја инфраструктурних сектора за друштво треба да рефлектују озбиљност утицаја који има уништавање или узурпирање рада неке инфраструктуре и да их треба одредити посебно за сваки случај (Directive 2008/114/EC). Европска унија је на основу овог приступа дефинисала и мере заштите критичне инфраструктуре: превентивне мере, информационе системе за узбуњивање у оквиру критичне инфраструктуре, процесе заштите и дељења информација између држава, подршку земљама чланицама у вези за националном критичном инфраструктуром, планирање непредвидивих ситуација и финансијске мере заштите (Directive 2008/114/EC). Дефинисане мере заштите требало би да усвоје све државе чланице и потенцијални кандидати како би се: успоставили интероперабилност и сарадња и ускладили законски и стратегијски оквир са Унијом; предвидели степен пропадања критичне инфраструктуре и могућност нарастајућег отказа критичне инфраструктуре; предвидео модел понашања критичне инфраструктуре и побољшање исте; оценили ефективност и ефикасност функционисања критичне инфраструктуре; унапредила методологија за анализу животног циклуса критичне инфраструктуре и планирали дугорочни и краткорочни програми унапређења и изградње заштите критичне инфраструктуре (Directive 2008/114/EC).

Године 2022. Директиву 2008/114/ЕК замењује Директива 2022/2057 Европског парламента и савета о отпорности критичних ентитета. Како се наводи у тачки два уводног дела Директиве 2022/2057: „Директива Савета 2008/114/ЕК предвиђа процедуру за одређивање европске критичне инфраструктуре у енергетским и транспортним секторима чије би нарушавање или уништење имало значајан прекогранични утицај на најмање две државе чланице. Та Директива се фокусира искључиво на заштиту такве инфраструктуре. Међутим, евалуација Директиве 2008/114/ЕК спроведена 2019. године показала је да, због све више међусобно повезаних и

прекограничне природе операција које користе критичну инфраструктуру, саме заштитне мере које се односе на појединачна средства нису довољне да спрече све поремећаје. Због тога је неопходно померити приступ ка томе да се осигура боље третирање ризика, да улога и дужности критичних субјеката као пружалаца услуга од суштинског значаја за функционисање унутрашњег тржишта буду боље дефинисани и кохерентни, као и да се усвоје правила Уније како би се побољшала отпорност критичних ентитета. ***Критични субјекти треба да буду у позицији да ојачају своју способност да спрече, заштите, реагују, одупру, ублаже, ресорбују, прилагоде и опораве се од инцидената који имају потенцијал да поремете пружање основних услуга***."

Промене у окружењу које су утицале на потребу за доношењем и усвајањем нове Директиве дате су у тачки 3 коју такође дословно цитирамо: „Док бројне мере на нивоу Уније, као што је Европски програм за заштиту критичне инфраструктуре, и на националном нивоу имају за циљ да пруже подршку заштити критичне инфраструктуре у Унији, требало би учинити више да се субјекти који управљају таквом инфраструктуром боље оспособе да третирају ризике за њихово пословање који би могли да доведу до ометања пружања основних услуга. Такође би требало учинити више на бољој припреми таквих субјеката јер постоји динамичан пејзаж претњи, који укључује еволуирајуће хибридне и терористичке претње, и растућу међузависност између инфраструктуре и сектора. Штавише, постоји повећан физички ризик услед елементарних непогода и климатских промена, што интензивира учесталост и размере екстремних временских појава и доноси дугорочне промене просечних климатских услова које могу смањити капацитет, ефикасност и животни век одређених типова инфраструктуре уколико мере адаптације на климу нису успостављене. Поред тога, унутрашње тржиште карактерише фрагментација у погледу идентификације критичних субјеката јер релевантни сектори и категорије субјеката нису доследно препознати као критични у свим државама чланицама. Ова Директива стога треба да постигне солидан ниво хармонизације у погледу сектора и категорија субјеката који спадају у њен делокруг."

Ова Директива не третира отпорност на сајбер претње и сектор „дигиталне инфраструктуре", пошто је та област већ уређена Директивом 2022/2555 о мерама за постизање високог заједничког нивоа сајбер безбедности у Европској Унији. Директива (ЕУ) 2022/2555 захтева од субјеката који припадају сектору дигиталне инфраструктуре, а који се могу идентификовати као критичним, да предузму одговарајуће техничке, оперативне и организационе мере за управљање ризицима који представљају безбедност мрежних и информационих система, као и за обавештавање о значајним инцидентима и сајбер претњама (Directive 2022/2555/EC). И Директива 2022/2555 примењује приступ заснован на свим опасностима који укључује отпорност мрежних и информационих система, као и физичке компоненте и окружење тих система.

Такође, услед осетљивости сектора Директива 2022/2057 не третира критичне субјекте у секторима одбране, националне безбедности, јавне безбедности и судства, те је стога уређивање њихове отпорности препуштено државама чланицама, али се препоручује примена смерница Директиве.

Директива налаже да се у свим државама чланицама успоставе стратегијски оквири за унапређење отпорности критичне инфраструктуре. Даље, „активности држава чланица у циљу идентификације и унапређења отпорности критичних субјеката треба да прате ***приступ заснован на ризику*** који се фокусира на најрелевантније субјекте за одржавање виталних друштвених функција или економских активности. Како би се осигурао такав циљани приступ, свака држава чланица треба да изврши, у оквиру усклађеног оквира, ***процену релевантних***

природних и антропогених ризика, укључујући оне међусекторске или прекограничне природе, који би могли утицати на пружање есенцијалних услуга, укључујући техничко-технолошке несреће, природне катастрофе, ванредне ситуације у области јавног здравља као што су пандемије и хибридне претње или друге антагонистичке претње, укључујући терористичке акте, криминалну инфилтрацију и саботажу („процена ризика државе чланице“). Када врше процене ризика, државе чланице треба да узму у обзир друге опште или секторске процене ризика које се спроводе у складу са другим правним актима Уније ***и треба да размотре у којој мери сектори зависе један од другог***, укључујући и секторе у другим државама чланицама. и треће земље.“ (Директива 2022/2557, тачка 17).

Даље, према Директиви, Државе чланице треба да одреде или успоставе установе за надзор примене мера наложених Директивом, те да одреде контактну тачку за међудржавну комуникацију и сарадњу (Директива 2022/2557/ЕК, тачке 22 и 23).

За ово истраживање значајне су тачке које ближе говоре о процени ризика и отпорности – тачке 28 и 29: „Критични субјекти треба да имају свеобухватно разумевање релевантних ризика којима су изложени и дужност да анализирају те ризике. У том циљу, они треба да врше процене ризика кад год је то потребно с обзиром на њихове посебне околности и развој тих ризика, најмање на сваке четири године, како би проценили све релевантне ризике који би могли да поремете пружање њихових основних услуга („процена ризика критичног ентитета“).“ (Директива 2022/2557/ЕК, тачка 28).

„Критични субјекти треба да предузму техничке, безбедносне и организационе мере које су прикладне и пропорционалне ризицима са којима се суочавају како би ***спречили, заштитили, одговорили, одупрли се, ублажили, ресорбовали, прилагодили и опоравили*** се од инцидента. (...) детаљи и обим таквих мера треба да одражавају различите ризике које је сваки критични субјект идентификовао као део своје процене ризика (...).“(Директива 2022/2557/ЕК, тачка 28).

Ипак, као једини ризик који се експлицитно помиње у Директиви је ризик од злоупотребе приступа запослених у критичних субјектима, те се као мера умањења ризика предлажу безбедносне провере и спецификација услова приступа критичним субјектима (Ibid, тачка 32).

Налаже се оснивање Групе за отпорност критичних субјеката при Европској комисији, коју ће сачињавати експерти из држава чланица (Ibid, тачка 37). Ова Група ће блиско сарађивати са Групом за сарадњу предвиђеном Директивом 2022/2555/ЕУ о сајбербезбедности, у циљу заједничког оквира за сајбер и не-сајбер отпорности критичних субјеката (Ibid, тачка 38).

Директива наводи следећу дефиницију отпорности „***способност критичног ентитета да спречи, заштити, реагује, одупре се, ублажи, ресорбује, прилагоди и опорави се од инцидента***“ (Ibid, члан 2, деф.2).

Члан 4 Директиве говори о националним стратегијама отпорности критичне инфраструктуре. Између осталог, Стратегија мора да садржи опис мера неопходних за побољшање укупне отпорности критичних субјеката, укључујући опис процене ризика.

Члан 13 Директиве говори о мерама за унапређење отпорности критичних субјеката. Мере је потребно осмислити и применити у циљу:

(а) спречавања настанка инцидената, узимајући у обзир смањење ризика од катастрофа и мере прилагођавања клими;

(б) обезбеђивања адекватне физичке заштите објеката и критичне инфраструктуре, узимајући у обзир, на пример, ограде, баријере, алате и процедуре за надзор периметра, опрему за детекцију и контролу приступа;

(ц) реаговање на инциденте и ублажавање последица инцидената, узимајући у обзир примену процедура и протокола за управљање ризицима и кризним ситуацијама и процедуре узбуњивања;

(д) опоравак од инцидената, узимајући у обзир мере континуитета пословања и идентификацију алтернативних ланаца снабдевања, како би се наставило са пружањем основне услуге;

(е) адекватно управљање безбедношћу запослених, узимајући у обзир мере као што је одређивање категорија особља које обавља критичне функције, успостављање права приступа просторијама, критичној инфраструктури и осетљивим информацијама, успостављање процедура за проверу прошлости и одређивање категорија лица од којих се тражи да се подвргну таквим проверама и утврђују одговарајуће услове за обуку и квалификације;

(ф) подизање свести о мерама наведеним у тачкама (а) до (е) међу релевантним особљем, узимајући у обзир курсеве обуке, информативне материјале и вежбе.

Директива 2022/2557/ЕК представља знатан искорак у односу на Директиву 2008/114/ЕК, из два очигледна разлога – успоставља оквир за идентификацију критичне инфраструктуре у једанаест уместо два сектора предвиђена Директивом 2008/114, а такође покушава да операционализује концепт отпорности критичне инфраструктуре на нивоу Европске Уније и земаља чланица.

Ипак, конкретне мере које се налажу овом Директивом, у одређеном су нескладу са дефиницијом датом у члану 2, која, између осталог, наводи и потребу за адаптацијом. Мере за унапређење отпорности састоје се од систематског увезивања процеса физичко-техничке заштите, пробабилистичког менаџмента ризиком, инцидентима, кризама и континуитетом пословања, безбедносним проверама запослених и подизању свести путем обука.

Фокус је, дакле, искључиво на предвидивим ризицима (отпорност првог реда), а Директива, осим у дефиницији отпорности, не помиње мере које би утицале на адаптацију. Ослањање на усклађене планове и процедуре имплицира да је флексибилност и иновативност одговора занемарена. Такође, Директива не помиње слободне/флуктуирајуће ресурсе који би се могли ангажовати у случају манифестације нерутинског ризика или непредвиђеног догађаја, као ни оснаживање појединачних запослених и тимова за аутономан одговор у случају хитности или непостојања процедура. Чини се да и поред знатне временске дистанце у односу на стратегијска и легислативна документа исте или сличне тематике, оквир за унапређење отпорности критичне инфраструктуре у Европској Унији и даље заостаје за приступима у САД, Уједињеном Краљевству и Аустралији које ћемо укратко представити у наставку.

1.3.1.4. Национални приступи отпорности критичне инфраструктуре

Како је питање заштите и отпорности критичне инфраструктуре као система система од кључног значаја за безбедност и добробит државе и њених грађана, приметно је интересовање законодаваца и доносиоца одлука у области државне безбедности и одбране да законским и стратегијским документима уреди ову област. Отпорност критичне инфраструктуре се конкретизује и операционализује у званичним актима, а повезаност њеног континуитета

пословања и одржавања виталних функција државе све је јасније исказана. За сада, у овој области предњаче Сједињене Америчке Државе, Уједињено Краљевство и, нарочито, Аустралија, чија ћемо званична документа на националном и регионалном нивоу укратко представити на следећим страницама.

1.3.1.4.1. Сједињене Америчке Државе

Почетак примене концепта отпорности у контексту заштите критичне инфраструктуре у САД започиње 2006. године, када је Радна група за критичну инфраструктуру, Савета за унутрашњу безбедност САД иницирала дебату поводом превелике усмерености државних политика о критичној инфраструктури на заштиту од терористичких напада, уз занемаривање отпорности на друге претње (Homeland Security Advisory Council 2006). Радна група је истакла да су политике Владе САД потенцирале улагања у мере заштите као што су опрема за видео-надзор, радници обезбеђења итд., али нису подстицале напоре који би омогућили штићеним вредностима да наставе да функционишу на одређеном нивоу, или да се поврате на пуну оперативност након напада. Такви напори, према Радној групи, могли би укључити повећану редундантност (нпр. вишеструки резервни извори напајања) или пројектовање робуснијих система (Moteff 2012). Прва препорука Радне групе јесте да се промовише концепт отпорности критичне инфраструктуре као примарни стратешки циљ којим ће се водити планирање националних политика (Homeland Security Advisory Council 2006, iii).

Већ наредне, 2007. године, Национална стратегија отаџбинске безбедности САД повезује структурну отпорност „критичне инфраструктуре“ са „оперативном отпорношћу“ хитних служби, државних институција и приватних предузећа у случају кризе. Ова стратегија истиче да ниједна од претњи са којом се ови системи сусрећу није у потпуности предвидива, те претпоставља концепт отпорности старијем концепту превенције (National Strategy of Homeland Security 2007). Према овој стратегији, отпорност се, између осталог, може постићи кроз дисперзију кључних функција на вишеструке пружаоце услуга, флексибилан ланац снабдевања и повезаних система (Ibid, 28).

Према Извештају о заштити критичне инфраструктуре Савета за националну инфраструктуру (National Infrastructure Advisory Council - NIAC) САД из 2009. године, отпорност критичне инфраструктуре дефинисана је као „способност за редуковање магнитуде, утицаја или трајања ремећења” (NIAC 2009, 2). Овај извештај наводи следеће карактеристике отпорне критичне инфраструктуре поседује следеће карактеристике:

- Робусност –способност одржавања критичних функција и ресорпције утицаја насталог услед кризе или ремећења;
- прилагодљивост - способност за припрему, одговор и управљање кризом или поремећајем пословања кроз успостављање и одржавање адаптивних капацитета за преусмеравање ресурса и вредности;
- капацитет за брз опоравак – способност за што брже и ефикасније враћање у нормалан режим функционисања. (NIAC 2009, 24)

Председничка директива 21 – „Безбедност и отпорност критичне инфраструктуре” из 2013. године, истиче потребу за постојањем безбедне, оперативне и отпорне критичне инфраструктуре, а у циљу одржавања континуитета есенцијалних функција државе (PPD/21 2013). За разлику од докумената донетих непосредно после напада на Куле близнакиње који су превасходно мотивисани претњом терористичких напада, у овој директиви присутан је приступ усмерености на свеобухватне хазарде, као и на феномене међузависности и „домино ефеката”.

Ова директива посебно истиче критичност енергетских и комуникационих система, услед њиховог утицаја на све друге секторе критичне инфраструктуре (Ibid).

План заштите националне инфраструктуре *(National Infrastructure Protection Plan - NIPP)* из 2013. године није план у ужем смислу, тј. не даје конкретне процедуре за активирање у случају ванредног догађаја, већ, пре свега, детаљно износи механизме сарадње и координације јавног и приватног сектора у менаџменту ризиком и унапређењу отпорности критичне инфраструктуре. НИПП 2013 наслања се на Председничку директиву 21 и представља ажуриране верзије Планова из 2006. и 2009. године. Фокус плана је на интегрисаном и колаборативном приступу јавног и приватног сектора у циљу постизања визије „нације у којој је физичка и сајбер критична инфраструктура безбедна и отпорна, рањивости умањене, последице минимизиране, претње идентификоване и осујећене, а одговор и опоравак убрзан.“ У складу са Директивом 21 и Националном стратешком проценом ризика (*The Strategic National Risk Assessment (SNRA)*), присутан је приступ свеобухватне листе претњи. Наиме, SNRA дефинише претње и хазарде у широко постављеним категоријама непријатељских/људских, природних и техничко-технолошких фактора. Критични системи, постројења и мреже суочавају се са свим овим категоријама претњи, од терористичких (физичких или сајбер) напада, временских непогода, пандемија, па до акцидената узрокованих дотрајалошћу инфраструктуре. Потенцијал за међуповезане догађаје са непознатим последицама додаје фактор неизвесности уз идентификоване и анализиране ризике.

План, такође, истиче значај фактора све веће међузависности између система критичне инфраструктуре, а нарочито ослањања на информационо-комуникационе технологије, што доводи до повећане рањивости на физичке и сајбер претње, као и потенцијалних последица. „У све више међуповезаном свету, у којем критичне инфраструктуре прелазе националне границе и у којем постоји глобални ланац снабдевања, потенцијалне последице расту са тим међузависностима, као и способност различитих претњи да те рањивости искористе.“ (NIPP, 2013: 8). У план су укључена још два сектора– комуникације и поштанске и шпедитерске услуге – што даје укупан број од осамнаест сектора критичне инфраструктуре.

Федерална агенција за сајбер безбедност и критичну инфраструктуру (CISA) је 2020. године Плану заштите националне инфраструктуре додала четири практична пратећа документа, међу којима је и документ под називом „Укључивање отпорности у пројекте критичне инфраструктуре“ Овај документ, намењен првенствено федералним и локалним властима које започињу или планирају инвестирање у нове инфраструктурне пројект, садржи кораке у процесима планирања и инвестирања који могу бити примењени у циљу приоритизације оних пројеката који промовишу отпорну инфраструктуру. Кораци су:

- Укључивање пројектованих утицаја климатских промена у процес доношења одлука о изградњи или инвестирању;
- Мерење директних и индиректних трошкова и бенефита пројекта (нпр. Цена губљења функција и услуга инфраструктуре, друштвени утицај пројекта, утицај на животну средину итд.);
- Испитивање демографских трендова и антиципирање будуће демографске слике у циљу предикције потреба за инфраструктуром;
- Консултовање са ФЕМА-ом око ризика од поплава на планираним локацијама;
- Примена доступних научних и предиктивних алата о будућим трендовима и ризицима приликом избора локације (нпр. трендови подизања нивоа мора);
- Примена адекватних стандарда и најбољих пракси за укључивање резилијентности од почетне фазе, тј. од пројектовања система;

- Процена рањивости инфраструктуре на познате, али и на будуће ризике;
- Примена алата за процену ризика и планирање сценарија у циљу доношења одлука заснованих на ризику;
- Идентификовање кључних зависности и међузависности унутар и између сектора;
- Мапирање потенцијалних каскадних ефеката након потенцијалних поремећаја функционисања инфраструктуре;
- Сарадња са партнерима у циљу постизања јасне слике како ће се пројекат уклопити у регионални систем критичне инфраструктуре;
- Развој свеобухватног плана одговора на инциденте, који укључује планирање сценарија на ризике са највећом вероватноћом и јасно артикулисане улоге и обавезе свих партнера;
- Уграђивање редундантности у инфраструктурни систем у циљу заустављања локализованих поремећаја;
- Буџетирање за митигацију ризика (тј. за мере управљања ризиком);
- Израда плана континуитета пословања;
- Планирање периодичних ажурирања мера умањења ризика у циљу примене нових технолошких решења;
- Процена да ли природни бафери (мочваре, пешчаре) могу бити инкорпорирани у пројектовање система у циљу умањења ризика од природних непогода;
- Обавезно уграђивање резервних мануалних и физичких контрола у све аутоматизоване системе. (Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects 2020)

1.3.1.4.2. Уједињено Краљевство

Постепено напуштање искључиве усмерености на претњу тероризма и померање фокуса на свеобухватне претње и отпорност јавља се и у другим државама које су биле укључене у „Рат против терора". Извештај сер Мајкла Пита о катастрофалним поплавама које су погодиле Уједињено Краљевство (УК) 2007. године, истакао је по први пут недостатке политика заштите критичне инфраструктуре од природних хазарда. Пит је закључио да „Влада треба да успостави систематичну, координисану, мултисекторску кампању како би умањила поремећаје настале услед деловања природних догађаја на критичну инфраструктуру и виталне услуге" (Pitt 2007).

„Стратешки оквир са изјавом о политици" који се позива на Питов Извештај публикован 2010. године даје прецизније смернице за операционализацију концепта отпорности, са фокусом на природне катастрофе, пре свега поплаве. Према Стратешком оквиру, главни циљ је „идентификација и процена ризика од природних хазарда, а затим развој разноврсних опција за избегавање, трансфер, прихватање, редукцију или поделу тих ризика. Опције могу варирати од физичке заштите, преко релокације штићених вредности, обезбеђивање алтернативних ланаца снабдевања, па до унапређених аранжмана са хитним службама" (UK Cabinet Office 2010, 5). Даље, Стратешки оквир наглашава да је „важно успостављање правог баланса између инвестирања у критичну инфраструктуру и инвестирања у одговоре на ванредне догађаје, капацитете и планове опоравка. Програм за унапређење отпорности критичне инфраструктуре УК треба да обухвати превенцију, заштиту, одговор и опоравак. Услед све умреженијег окружења, Програм мора да узме у обзир зависности и међузависности унутар и између сектора критичне инфраструктуре" (Ibid, 7).

Истовремено, у Стратегији националне безбедности УК из 2010. године прихвата се приступ отпорности за непредвидиве ризике (HM Government 2010a, 25). Иста стратегија наглашава важност отпорности мрежа великих британских привредних друштава на сајбер-нападе и поремећаја и прекида телекомуникационих система (Ibid 29). Напокон, међу „задатке националне безбедности" уврштено је „унапређење отпорности УК подизањем спремности на све врсте ванредних догађаја, способности за опоравак након ремећења и одржавање виталних услуга" (Ibid, 33).

Стратешки преглед о одбрани и безбедности из исте године наводи услове потребне за испуњавање тог задатка, између којих су: безбедност и отпорност инфраструктуре од кључне важности за функционисање државе (укључујући нуклеарна постројења) на нападе, оштећења или уништења; капацитете за кризни менаџмент који могу да предвиде и одговоре на разне ванредне догађаје и одрже функционисање Владе; отпорне системе снабдевања и дистрибуције критичних услуга; ефикасне, добро организоване локалне одговоре на ванредне догађаје, засноване на способностима хитних служби, привредних друштава и заједница на локалном нивоу (HM Government 2010b, 14). Преглед такође предвиђа оснивање Савета за безбедност и отпорност инфраструктуре, са задатком унапређења сарадње јавног и приватног сектора и унапређења отпорности инфраструктура у приватном власништву на све типове хазарда и претњи, укључујући и сајбер нападе (Ibid, 49).

И наредни стратешки документи из области одбране и безбедности без изузетка говоре о отпорности критичне инфраструктуре као једном од стубова националне безбедности. У Стратегији безбедности и одбране из 2015. одељак Г, под називом „Отпорност и одговор на кризу"укључује одредбе које се директно тичу отпорности критичне инфраструктуре. Поглавље започиње реченицом „Отпорност УК зависи од свих нас – од хитних служби, локалне и централних власти, пословних субјеката, заједница и појединачних особа" (HM Government 2015, 43). Затим се наводи да је највећи део критичне инфраструктуре у приватном власништву, те да су потребни заједнички напори Владе и власника и оператора критичних инфраструктура у циљу умањења ризика од људских претњи и природних хазарда, као и од сајбер претњи (Ibid, 44). Напокон, истиче се да је неопходно обезбедити испоруку кључних добара у случају прекида снабдевања електричном енергијом на ширим географским подручјима, те да је потребно увести нове мере које би унапредили отпорност на овај ризик (Ibid, 44). Учесталост термина „resilience" се такође повећала, па је од 11 понављања у Стратегији одбране и безбедности из 2010, у Стратегији из 2015. године овај термин употребљен чак 53 пута.

Годишњи прегледи који прате спровођење стратегије националне безбедности и одбране конкретизују ове захтеве. Тако у извештају за 2018. годину, параграф 2.100 наглашава напоре које улаже Влада у формирању адекватног и измене постојећег регулаторног оквира за постизање отпорности Националне критичне инфраструктуре на будуће претње, те да се врши непрестана ревизија регистра ризика како би се идентификовали утицаји на безбедност и отпорност критичне инфраструктуре (HM Government 2018, 24).

У Извештају о сајбер безбедности националне критичне инфраструктуре за период 2017-2019, заштита критичне инфраструктуре од сајбер претњи представља нерешив проблем (*wicked problem*), за који се препоручује приступ отпорности, а не антиципације (Joint Committee on the National Security Strategy 2018, 8).[13] Отпорност, према Извештају, претпоставља јачање регулаторног оквира, подизање прага минимума усаглашености и унапређења „културе"

[13] О теоријским постулатима нерешивих проблема види Rittel & Webber 1973. О односу концепта отпорности и нерешивих проблема види Craig 2020.

власника и оператора КИ у смислу јачања тзв. „сајбер хигијене" (политике минималног приступа, лозинки итд) и процене ризика у ланцу снабдевања (Ibid, 11-12).

Напокон, Студија о отпорности Комисије за националну инфраструктуру УК из 2019. године добар је показатељ тенденције ка свеобухватном приступу и усмерености на системске ризике. У уводној речи каже се да „Садашња и будућа инфраструктура УК мора бити отпорна на растуће изазове климатских промена, демографског раста и повишене зависности и интегрисаности дигиталних технологија. Ови хазарди су укључени поврх свакодневних безбедносних претњи, природних катастрофа и економских поремећаја. (...) Тешко је пронаћи примере холистичког и мултисекторског приступа отпорности, а још увек не постоји ни опште разумевање отпорности и рањивости инфраструктуре УК" (National Infrastructure Commission 2019, 4).

Нарочито је значајан став Комисије да ће у наредном периоду њени напори бити усмерени на следећа питања:

1. Који системски проблеми инфраструктуру чине рањивом на садашње поремећаје и будуће промене и како се они могу решити?
2. Шта јавност очекује од организационих система оператора критичне инфраструктуре и како њихова мишљења могу бити уважена у одлукама о отпорности?
3. Које би промене у управљању и одлучивању могле унапредити тренутне нивое отпорности и обезбедити одговор на будуће изазове? (Ibid)

1.3.1.4.3. Аустралија

Аустралија, услед свог специфичног географског положаја и геополитичке улоге у свету, рано одбацује доминантан наратив да је тероризам „претња свих претњи" по критичну инфраструктуру и националну безбедност. Како теоретичари, тако и доносиоци одлука и законодавци, увидели су да на широким и пустим пространствима Аустралије климатски феномени, као и зависност од страних ресурса представљају изузетно висок реметилачки фактор. Већ крајем прве деценије овог века приступ отпорности почиње да преузима примат над приступом заштите.

Како се у Уводу Стратегије отпорности критичне инфраструктуре из 2015. године наводи: „Извештај о заштити критичне инфраструктуре из 2009. године установио је да, док је за неке инциденте могуће планирати заштитне мере, узевши у обзир бројност потенцијалних претњи и хазарда, укључујући природне непогоде, пандемије, немар, технолошке акциденте, криминал или нападе на рачунарске мреже, није могуће предвидети, умањити или спречити све те догађаје. Нарочито, безбедносне мере заштите не могу умањити ризик од поремећаја ланца снабдевања, нити обезбедити брз опоравак услуга. Власници и оператори критичне инфраструктуре често имају ограничене капацитете да наставе пословање на неодређено време уколико им је снабдевање кључним ресурсима и услугама онемогућено. Због тога, приступ отпорности је прикладнији за одговор на све хазарде" (Critical Infrastructure Resilience Strategy – Policy Statement 2015, 2).

У званичној аустралијској терминологији јасно су разграничени појмови безбедности, у смислу заштите, и отпорности критичне инфраструктуре, припадајућих извора ризика, као и институционалних надлежности.

Закон о безбедности критичне инфраструктуре из 2018. године усмерен је на управљање комплексним ризицима по националну безбедност као што су саботаже, шпијунаже и принуде, а који потичу од страног присуства (власништва или управљања) у аустралијској критичној инфраструктури (The Security of Critical Infrastructure Act, 2018). Закон се примењује на око две стотине организационих система у секторима електричне енергије, гасне инфраструктуре, водопривреде и морских лука. Безбедност критичне инфраструктуре потпада под надлежност Министарства унутрашњих послова Аустралије, који одржавају регистар критичне инфраструктуре и могу захтевати детаљне информације од власника и оператора критичне инфраструктуре (Ibid, 3). Закон овлашћује Министарство да наметне мере умањења ризика власницима и операторима критичне инфраструктуре, уколико оне нису претходно, или су неадекватно предузете (Ibid).

Системски оквир за унапређење отпорности критичне инфраструктуре оформљен је још 2003. године у виду Мреже за размену поузданих информација (Trusted Information Sharing Network – TISN). Ова платформа служи за размену информација између Владиних институција и приватног сектора путем координисања одговора на безбедносне изазове и потенцијална ремећења континуитета пословања, а у циљу унапређења отпорности критичне инфраструктуре (TISN 2021). Сектори обухваћени Мрежом укључују: банкарство и финансије, комуникације, енергетику, здравство, пољопривреду, производњу и дистрибуцију хране, саобраћај и водопривреду. Такође, у оквиру Мреже успостављени су специјалистички форуми и експертска група за отпорност. Активности Мреже укључују развој заједничких оквира деловања, смерница и планова, те организовање вежби и радионица усмерених на одговор на специфичне претње са којима се сектори суочавају.

Прва Стратегија отпорности критичне инфраструктуре донета је још 2010. године (Critical Infrastructure Resilience Strategy, 2010). Стратегија предвиђа широк спектар активности у циљу унапређивања отпорности КИ: од изградње капацитета, промовисања концепта отпорности и ширења корпуса практичног знања, до успостављања Програма за моделовање и анализу (*Critical Infrastructure Program for Modelling and Analysis*), који моделује и симулира понашање система критичне инфраструктуре и „домино ефекат" поремећаја у једном сектору на друге секторе (Ibid).

Нова Стратегија објављена је 2015. године, и подељена је на стратешку изјаву *(policy statement*) и практични део. На националном нивоу, термин „заштита критичне инфраструктуре" користи се за описивање предузетих активности или мера за умањење ризика од специфичне претње тероризма, док термин „отпорност критичне инфраструктуре" обухвата приступ Владе заснован на свим претњама, што укључује и тероризам" (Critical Infrastructure Resilience Strategy – Policy Statement 2015, 2). Циљ Стратегије дефинисан је као континуирано функционисање критичне инфраструктуре упркос свим претњама (Ibid 3).

Стратегија предвиђа два приступа за остваривање наведеног циља. Први је менаџмент предвидивим ризицима кроз приступ заснован на процени и управљању ризиком. Други представља менаџмент непредвидивим ризицима, тј. неизвесностима, који се може остварити применом приступа организационе отпорности (Ibid, 7-8). „Организације морају изградити унутарњу способност за одговор на непредвиђене или неочекиване ризике и догађаје. Упркос неповољном догађају, организације са јаком културом и капацитетом отпорности дуже ће одржати континуитет функционисања и брже се вратити у нормалан режим пословања. (...) Организација са **развијеном културом отпорности** ће размењивати информације са другима, учити из криза, имати флексибилан приступ решавању проблема и успостављене режиме сарадње са Владом и различитим секторима привреде. Приступ организационе отпорности не

искључује примену традиционалног менаџмента ризиком. Високо отпорне организације умеју да прилагоде и примене методе и алате за менаџмент ризиком у најразличитијим околностима. Поврх планирања за предвидиве ризике, отпорне организације се припремају за неизвесност успостављањем прилагодљивих и скалабилних аранжмана на ремећења свих врста" (Ibid, 8).

Дакле, према наведеним изводима из регулаторних и стратегијских докумената, можемо закључити да је у развијеним земљама стратегија отпорности преузела примат у промишљању проблематике заштите критичне инфраструктуре, у складу са теоријским постулатима приказаним у претходним поглављима.

1.3.2. Закључак

Ово поглавље покушало је да укаже на различита промишљања отпорности у контексту критичне инфраструктуре. Разликовали смо два основна приступа – системски и организациони.

Према првом приступу, критична инфраструктура се посматра као систем система на одређеној територији (државе, суб-националне, или супра-националне регије). Ово је приступ који примењују законодавци и институције, као и научно-истраживачке организације попут националних лабораторија Sandia и Argonne, повезаних са државним војним и цивилним властима. Ова истраживања су углавном концептуална и заснована на моделовању. Преглед истраживања, легислативних и стратешких аката пружа значајан хронолошки увид у померање фокуса са конкретних, најчешће антропогених, ризика на приступ усмерен на „све претње" и штићене вредности. Према аустралијској стратегији отпорности критичне инфраструктуре из 2015. године отпорне организације ће „размењивати информације са другима, учити из криза, имати флексибилан приступ решавању проблема и успостављене режиме сарадње са Владом и различитим секторима привреде".

За ову докторску дисертацију важнија су истраживања која тематизују факторе организационе отпорности у операторима критичне инфраструктуре. Приступ у овим истраживањима одсликава концепте које смо помињали у претходном поглављу (капацитети, димензије и нивои отпорности, слободни ресурси).

Од нарочитог значаја за ову дисертацију су:

1. преглед емпиријских истраживања организационе отпорности по секторима критичне инфраструктуре идентификованим у складу са Законом о критичној инфраструктури Републике Србије, по којем видимо да су истраживања најчешће спровођена у секторима енергетике, саобраћаја и здравства, док су у осталим секторима малобројна;
2. анализа прегледних студија која третирају различите четири капацитета отпорности (антиципативни, ресорптивни, ресторативни и адаптивни), из којих закључујемо да је фокус емпиријских истраживања био на капацитету антиципације и ресорпције, док је мање пажње усмерено на капацитете за опоравак (ресторативни) и прилагођавање новонасталим околностима (адаптивни капацитет).
3. Емпиријска студија о могућностима и границама примене постулата организационе отпорности у критичној инфраструктури у јавном власништву, на примеру Данске.

2. Истраживачки део

2.1. Предмет, циљеви и хипотеза истраживања

Безбедност и отпорност критичне инфраструктуре је у сваком друштву предуслов националне безбедности. Ипак, када говоримо о безбедности и отпорности критичне инфраструктуре, пре свега имамо на уму не физичке објекте у којима се она налази или дигиталне мреже, а који су неоспорно веома важни, већ њихово пословање, то јест испоруку њихових производа и услуга који су од виталног значаја за безбедност државе и добробит њених грађана. Те кључне услуге и производи настају делатношћу организационих система оператора критичне инфраструктуре. Будући да систем критичне инфраструктуре посматрамо као мрежу међуповезаних и међузависних организационих, социо-техничких система, фокус овог истраживања јесте организациона отпорност појединих елемената те мреже на ретке догађаје који могу имати високи негативни утицај на њихово пословање, те последично и на националну безбедност и добробит становништва.

У овој дисертацији полазимо од претпоставке да је за управљање нерутинским ризицима (ризицима ниске вероватноће, а веома високих последица) стратегија отпорности адекватнија од стратегије антиципације. Ипак, ми и **стратегију антиципације у овој дисертацији посматрамо као један сегмент свеобухватне стратегије отпорности у управљању ризицима**, било да је та стратегија експлицитно формулисана или имплицирана организационом праксом традиционалног менаџмента ризиком. Конкретно, стратегију отпорности посматрамо као интегративне напоре управљања ризицима, кризама и континуитетом пословања, уз додатне, али неопходне „меке аспекте“ лидерства и организационе културе, као и оснаживање капацитета за прилагођавање.

Аналитички модел коришћен у овом емпиријском истраживању представља иновативни покушај **комбинације модела капацитета отпорности организације, са тзв. моделом „рибље кости“ Гибсона и Таранта који прави дистинкцију између тврдог аспекта (одговор на питање: Шта се ради?) и меког аспекта (Како се то ради?).** Мишљења смо да је њихово комбиновање од високог аналитичког и практичног значаја, те ће ово истраживање покушати да направи први корак у том смеру. Стога је емпиријски део ове дисертације усмерен је на анализу капацитета и аспеката организационе отпорности на нерутинске ризике организација критичне инфраструктуре у Републици Србији и окружењу, те разматрања могућности њиховог унапређивања.

У складу са анализираним теоријским оквиром, отпорност посматрамо као композитни концепт четири капацитета – антиципаторног, ресорптивног, ресторативног и адаптивног. Иако поједини аутори ове аспекте називају „фазама“, у складу са истраживањима из области кризног менаџмента, у овом истраживању предност је дата термину „капацитети“, будући да не могу бити сви јасно темпорално одређени, нарочито адаптивни капацитет који може бити од значаја пре, током и након нежељеног догађаја. У сваком капацитету су даље, а у складу са моделом „рибље кости“, идентификовани индикатори тврдог (активности) и меког (карактеристике) аспекта. Подсетимо да „тврду страну“ отпорности чине активности и способности (постојање формализованих система менаџмента – ризицима, континуитетом пословања, ванредним ситуацијама, ланцем снабдевања, те јасне процедуре доношења одлука, делегирања, комуницирања итд.), док „меку страну“ чине фактори који се односе на организациону културу, лидерство, способност организационог учења и други бихејвиорални, релациони и когнитивни аспекти организационог понашања. Посебна пажња поклоњена је „мекој страни“ отпорности, која је од нарочите важности приликом суочавања са нерутинским ризицима.

Наш приступ је био да идентификујемо најчешће спомињане индикаторе у литератури, а пре свега оне који су Гибсон и Тарант укључили у спектар „активности и способности“, односно

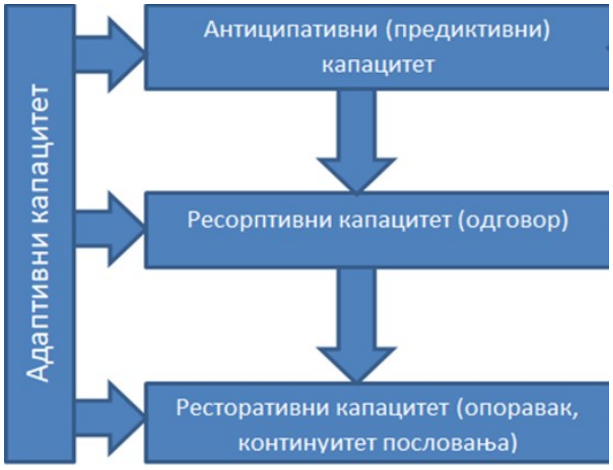
„карактеристика“, те смо их анализирали у смислу подобности за истраживање у научном и проблемском потпољу безбедности. Како се истраживање ограничава на организациону димензију отпорности, из њега смо изоставили индикаторе везане за финансијску, социјеталну и инфраструктурно-техничку димензију који су махом присутни у другим истраживањима која тематизују отпорност критичне инфраструктуре.

Дакле, Гибсонов и Тарантов аналитички модел „рибље кости“ допушта нам да у сваком од четири капацитета анализирамо „тврде“ и „меке“ аспекте, а који у овом истраживању представљају индикаторе нивоа усмерености на стратегију отпорности у управљању нерутинским ризицима. Као што су друга истраживања анализирана у теоријском делу дисертације показала, меки аспект је често кључан и „карика која недостаје“ у унапређивању организационе отпорности. Другим речима, сâмо постојање формалних процеса управљања ризиком, кризама и континуитетом пословања, премда несумњиво од изузетног значаја, није довољно за анализу отпорности, уколико се не узме у обзир начин на који се те активности извршавају, а што нарочито долази у фокус приликом одговора на нерутинске ризике.

Премда знатан број истраживања организационе отпорности тематизује отпорност организација на познате и рутинске претње (отпорност првог реда), у овом истраживању смо пажњу усмерили и на отпорност другог реда, на нерутинске ризике, који нису били или нису могли бити антиципирани.

Отпорност првог реда подразумева ефикасно и ефективно руковање познатим претњама и опасностима путем испробаних и тестираних технологија и мера, преко централне контроле, правила и процедура који отелотворују искуство и историјско знање организације (Daalgard Nielsen 2017, 343). Отпорност првог реда може се постићи применом интегрисаних система менаџмента ризиком, кризног менаџмента и менаџмента континуитетом пословања, а чије присуство у организацијама смо у истраживање као индикаторе за тврде аспекте отпорности. Следствено томе, присуство индикатора који припадају тврдом аспекту резилијентности указивало би на организациону отпорност првог реда (отпорност на познате претње, или рутинске ризике)

Следећи Вилдавског, према коме отпорност другог реда, захтева култивисање способности за опоравак од неочекиваних догађаја путем делегирања, брзе повратне информације и дозволе за експериментисање и импровизацију када стандардна решења изостану (Wildavsky 1989), закључујемо да „карактеристике”, то јест „меки аспект” отпорности директно утичу на отпорност другог реда организација. Питање отпорности првог и другог реда, то јест отпорности на познате ризике и на неизвесности анализирано је коришћењем истог скупа података.



Графикон 7 - Капацитети отпорности

Графикон 8 - Модел „рибље кости“ (Gibson & Tarrant 2010)

Модел „рибље кости“ адаптиран је у складу са ужом темом којом се ово истраживање бави и њеним усмерењем на организациону димензију отпорности критичне инфраструктуре. Самим тим, један број активности, способности и карактеристика је одбачен будући да се односе на друге димензије отпорности (социјеталну, финансијску или физичку димензију). С друге стране, додати су индикатори идентификовани у процесу анализе литературе, као што су дистинкција између усмерених и слободних-генеричких ресурса, разликовање између праксе комуницирања ризика и кризног комуницирања и динамичко активно планирање. Такође, секвенцијалном анализом теренских података добијених из интервјуа дошли смо до потребе да изоставимо одређене индикаторе који се односе на стратегијски ниво пословања организације. Наиме, будући да су велику већину (n=12) од укупног броја испитаника (n=15) представљали руководиоци сектора корпоративне безбедности који нису нужно укључени у стратегијске одлуке својих организационих система, нисмо добили задовољавајуће одговоре на питања која су се тицала тих индикатора. Те индикаторе би било свакако било пожељно укључити у будућа истраживања.

Антиципативни капацитет анализиран је кроз анализу постојања праксе процене и управљања ризицима у организацијама критичне инфраструктуре, планирања одговора на ризик кроз припрему сценарија усмерених на претње и/или штићене вредности, обуке кључних и некључних запослених са препорученим мерама одговора на ризик, као и постојања слободних генеричких ресурса који се могу активирати приликом одговора на нерутински ризик и за потребе опоравка. Партиципативни приступ планирању и комуникација ризика су идентификовани као меки аспекти или карактеристике, тј. на који начин се активности („тврди аспект“) извршавају. Треба напоменути да под комуникацијом ризика овде не подразумевамо формалне праксе присутне у плановима и интерним процедурама, већ комуникациони сегмент партиципативног приступа управљању ризицима који смо издвојили због његове важности за развој приправности на неочекиване и нерутинске догађаје.

Тврди аспект ресорптивног капацитета анализиран је кроз присуство формализоване пословне праксе кризног управљања и комуницирања. Као карактеристике (меки аспект) одговора на реметилачки догађај идентификоване су осмишљавање и изоштреност, односно креативност и флексибилност, који су у литератури препознати као од значаја за одговор на

реметилачке догађаје индуковане нерутинским ризиком, нарочито оне за које не постоји организационо и лично искуство.

Ресторативни капацитет посматран је кроз планирање и праксу опоравка, тј. континуитета пословања током и након реметилачког догађаја. Карактеристике овог капацитета су међуповезаност, односно сарадња са хитним службама и експертском заједницом, као и суочавање са стресом. Индикатор за суочавања са стресом, који се према Гибсону и Таранту односи на наставак функционисања људи, процеси и инфраструктура под растућим захтевима и неизвесношћу анализирали смо путем присуства кључних и некључних запослених на радном месту, то јест расположивост људских ресурса. Овај индикатор је већ испитиван у академским истраживањима (Riddle 2015), а имплицитно је препознат и у међународном стандард ISO 22317:2015 истиче идентификацију минимума прихватљивог броја запослених за извршавање одређене активности, потребна знања, вештине и квалификације, као и захтеве радног места (нпр. да ли запослени те активности могу да обављају од куће или са неке удаљене локације). Уколико се кључни или већи број не-кључних запослених у организацијама критичне инфраструктуре не би појавио на радном месту током одговора на и након екстремних догађаја, то би отежало опоравак не само тих организација, већ и друштвене заједнице која од њихових услуга и производа зависи.

Адаптивни капацитет се у овој дисертацији посматра као капацитет који прожима и унапређује све остале фазе и капацитете отпорности. Дакле, не посматрамо га као посебну фазу у односу на реметилачки догађај у временском тренутку „t“. Овде, свакако нисмо могли да анализирамо формални систем менаџмента који би представљао „тврди аспект“ капацитета, већ једино елементе организационе културе и лидерства као што су примена принципа динамичког адаптивног планирања (тврди аспект), као и способности организационог учења (меки аспект).

Табела 5: Интегративни модел анализе капацитета и аспеката отпорности

Капацитет	Аспект	Индикатори
Антиципативни	Тврди	1. Менаџмент ризиком 2. Постојање слободних ресурса 3. Способност запослених (обуке за кључно и некључно особље)
	Меки	1. Партиципативни приступ (управљање односима) 2. Комуницирање ризика
Ресорптивни	Тврди	1. Систем управљања кризама, инцидентима и ванредним догађајима 2. Кризно комуницирање
	Меки	1. Осмишљавање и изоштреност (Accuity) 2. Толеранција двосмислености 3. Креативност и флексибилност
Ресторативни	Тврди	1. Систем менаџмента континуитетом пословања
	Меки	1. Суочавање са стресом 2. Међуповезаност
Адаптивни	Тврди	1. Динамичко адаптивно планирање
	Меки	1. Способност учења

Што се тиче питања о нивоу организационе отпорности предузет је интегративни приступ, усвајајући становиште да организација може бити отпорна само онолико колико су њени запослени (како на индивидуалном, тако и на тимском нивоу) отпорни.

Природа и обим инцидента може имати важну улогу у способности организација да се опораве од резултирајућих дисрупција (Riddle 2015, 13). Избор студије случаја није случајан, већ је утемељен у теоријском оквиру перцепције ризика (Royal Society Study Group 1992; Pidgeon 1992). У студији Бернса и Словика, ризици од пандемије су високо котирани на листи од деведесет и шест сценарија које су испитаници оцењивали у складу са субјективном перцепцијом ризика (Burns & Slovic 2009). Ови догађаји могу имати велике негативне акутне ефекте по јавно здравље, као и значајан потенцијал за широке психолошке и бихејвиоралне последице, које могу имати дисруптивне ефекте на ниво продуктивности запослених и самим тим негативан утицај на пословање (Riddle 2015, 15). Епидемије и пандемије имају широк просторни и временски оквир, као и велике и дуготрајне последице, што може утицати на организације, територијалне јединице и државе да се врате у нормално стање. Наиме, одсуствовање запослених може у великој мери погодити пословање и приходе. Као илустрацију можемо узети податак да су локална предузећа недељу дана након нуклеарног акцидента на Острву Три Миље у Пенсилванији, 1979, имале губитак од 7.67 милиона долара (Houts et al. 1988). Овај губитак је генерисан бројним факторима, укључујући прекиде у ланцу набавке као и забринутости јавности о контаминираним прехрамбеним производима, међутим за главни разлог тих губитака узима се нерасположивост запослених услед евакуације која је обухватила широку територију (Ibid).

Водећи се овим налазима из литературе, истраживање је анализирало капацитете и аспекте отпорности оператора критичне инфраструктуре у Републици Србији и земљама у окружењу (Република Хрватска и Босна и Херцеговина) у рутинским условима, као и нерутинским условима индукованим пандемијом коронавируса (COVID-19, узрокована вирусом SARS-COV-12). Наиме, полуструктурисани интервју и анкета садржали су питања усмерена на адекватност и правовременост првог одговора (ресорптивни капацитет), опоравка (ресторативни капацитет) те прилагођавања на новонастале околности (адаптивни капацитет). Ово је оригинални допринос истраживања, јер је овакав приступ анализи отпорности још увек није примењиван на организације, већ искључиво на ниво отпорности заједница на катастрофе (community and disaster resilience). Такође, оригинални допринос рада произилази и из покушаја синтетичког приступа модела анализе капацитета и модела „рибље кости“ Гибсона и Таранта. Пошто су истраживања организационе отпорности коришћењем истих или сличних индикатора, предмета и циљева истраживања већ покретана у истраживачкој пракси, ово истраживање је послужило и као валидација раније добијених налаза из других просторних и временских оквира.

Сматрамо да ова дисертација може имати практични значај како за унапређење квалитета безбедносних планова оператора за управљање ризиком, тако и за подизање свести официра за везу критичних инфраструктура, менаџера ризика, корпоративне безбедности и континуитета пословања, као и највишег руководства организација критичне инфраструктуре о нерутинским ризицима и начинима унапређења организационе отпорности инфраструктура за које су задужени.

Налази овог истраживања могу бити искоришћени за креирање стратегија и планова комуницирања ризика и кризног комуницирања. Такође, критична инфраструктура је од стране Међународне организације за стандардизацију (ISO) препозната као нова област стандардизације у области безбедности и отпорности, али која је још увек недовољно

артикулисана, те налази могу бити примењени у изради нових и унапређењу постојећих међународних стандарда.

2.1.1. Циљеви истраживања

Циљеви овог истраживања су научна дескрипција фактора који утичу на организациону отпорност критичне инфраструктуре у случају манифестације нерутинских ризика. Организациона отпорност посматрана је као композитни концепт састављен од четири капацитета (антиципаторни, ресорптивни, ресторативни и адаптивни), од којих сваки поседује „тврди“ и меки аспект.

Користећи квалитативни приступ, ова теза има за циљ да:

- Идентификује претпоставке које доносиоци одлука имају о неизвесностима и нерутинским ризицима.
- Анализира праксе управљања ризиком у смислу фокуса на отпорност првог или другог реда.
- Анализира потенцијалне разлике у пажњи коју доносиоци одлука поклањају тврдим меким аспектима отпорности.
- Анализира нивое организационе отпорности у операторима критичне инфраструктуре – усмерености на индивидуални, тимски или организациони-системски ниво.
- Анализира антиципаторне, ресорптивне, ресторативне и адаптивне капацитете отпорности критичне инфраструктуре током пандемије COVID-19.
- Идентификује примере добре праксе у организацијама критичне инфраструктуре које буду учествовале у истраживању.
- Упореди резултате добијеним овим истраживањем са налазима истраживања спроведених у другим просторним и временским оквирима.

Коначно, истраживање као практични циљ има унапређивање праксе комуницирања ризика, планирања и управљања континуитетом пословања и израде безбедносних планова оператора организација критичне инфраструктуре.

2.1.2. Хипотетички оквир истраживања

Основна хипотеза овог истраживања јесте да је стратегија отпорности имплицитно препозната као стратегија избора за управљање нерутинским ризицима у организацијама критичне инфраструктуре. Посебне хипотезе су:

Х1 – *Формални процеси и усмереност доносилаца одлука у операторима критичне инфраструктуре је на рутинским ризицима на које се примењује стратегија антиципације*.

Х2 – *За нерутинске ризике и неизвесности имплицитно се примењује стратегија отпорности кроз примену неформалних пословних пракси усмерених на карактеристике или меки аспект отпорности*.

Х3 - *Напори доносилаца одлука и надлежних организационих јединица су равномерно усмерени на јачање сва четири капацитета отпорности.*

У складу са дефинисаним предметом, циљевима и хипотезама истраживања, дисертација ће покушати да одговори на следећа истраживачка питања:

1. Која су уверења менаџера безбедности и менаџера континуитета пословања оператора критичне инфраструктуре за планирање одговора на нерутинске ризике и неизвесности?
2. Која су уверења менаџера безбедности и доносиоца одлука о могућности управљања неизвесностима?

3. На које капацитете отпорности оператори критичне инфраструктуре поклањају највише пажње?
4. Колико пажње се у операторима критичне инфраструктуре поклања меким аспектима отпорности у циљу постизања отпорности другог реда?
5. У којим капацитетима су присутнија усмерења на меке аспекте отпорности?
6. На које организационе нивое су усмерени напори у јачању отпорности организације (индивидуални, тимски или системски)?
7. На који начин се руководи кризним ситуацијама индукованим нерутинским ризицима?
8. Које претпоставке менаџери безбедности и менаџери континуитета пословања организација идентификованих као критичне инфраструктуре имају о понашању запослених током и након екстремних догађаја?
9. На који начин се може допринети унапређењу отпорности критичне инфраструктуре да функционише и унапреди опоравак након екстремних догађаја?
10. На који начин се могу комуницирати нерутински ризици према запосленима у критичним инфраструктурама?
11. Које су националне специфичности одговора запослених на екстремни догађај? То јест, колико налази овог истраживања одступају од налаза истраживања спроведених у другим просторним оквирима?

2.1.3. Тип и метод истраживања

Планирано истраживање је квалитативног типа са доминантно дескриптивним циљевима. Примарни циљ истраживања јесте опис пословне праксе оператора критичне инфраструктуре и уверења њихових доносиоца одлука о начинима и могућностима примене стратегије отпорности на догађаје индуковане нерутинским ризицима и неизвесностима. Код дескриптивних истраживања у основи пројектовања су хипотезе изведене из теорије и резултата претходних истраживања на ову тему.

У свом говору на додели Нобелове награде, Хајек је истакао да су предмети проучавања у друштвеним наукама феномени „организоване комплексности“. У организованој комплексности карактер структуре не зависи искључиво од својстава елемената који је чине и релативне учесталости са којом се јављају, већ и од начина на који су они међусобно повезани. Услед тога конкретну информацију није могуће заменити статистичком, уколико желимо да из теорије изведемо специфичне предикције о индивидуалним догађајима (Hayek, 1974). Аспекти комплексних система за које можемо добити квантитативне податке нужно су ограничени, а не морају укључивати оне елементе који се касније могу показати значајнима (Ibid). Овакав став имплицира нужност квалитативног приступа у постизању дубинских увида о структури и о функционисању комплексних система.

Будући да су циљеви истраживања усмерени на разумевање искустава људи, то јест доносиоца одлука у области безбедности и континуитета пословања оператора критичних инфраструктура, њихових ставова, мишљења, осећања и перцепције, примењен је квалитативни тип истраживања и метод студије случаја.

Формулисање нацрта квалитативног истраживања јесте континуирани процес који захтева стално преиспитивање одлука и никако се, као у случају квантитативних истраживања, не може ограничити као засебна рана истраживачка фаза (Lewis, 2003, p.47). На тврдњи о отвореној природи квалитативних истраживања утемељен је и концепт секвенцијалне анализе која управо иде у сусрет потреби за континуираним балансирањем почетних идеја и откривених знања и као процес који траје током целог истраживања (Ђурић, 2013, p. 40-41). Одлуке донесене у прелиминарном нацрту истраживања и предвиђени истраживачки захтеви морају се

током трајања истраживања усклађивати с идејама које се секвенцијално генеришу из прикупљених података (Ђурић, 2013, p.41). У овом истраживању, иницијално прикупљени и анализирани подаци током фаза секундарне анализе података, као и иницијални одговори испитаника, у касније спроведеним интервјуима довели су до редефинисања и модификовања водича за полуструктурисане интервјуе са доносиоцима одлука и менаџерима корпоративне безбедности и континуитета пословања.

Јединица анализе или случај је догађај настао актуализацијом нерутинских ризика – пандемија COVID-19. Студија случаја одабрана је у складу са налазима претходних истраживања која су тематизовала перцепцију ризика, идентификујући пандемију као ризик који поседује висок број „негативних атрибута хазарда“, те се самим тим налази на самом врху неприхватљивих ризика код испитаника (Burns & Slovic, 2009). Чињеница да је пандемија изазвана вирусом COVID-19 догађај који још увек у великој мери погађа организације широм света, доприноси утиску да ће подаци добијени анализом овог случаја бити емпиријски богати и корисни за даљу анализу организационе отпорности на пандемијски ризик. Такође, интервјуисаним особама постављана су питања у вези са другим догађајима ниске вероватноће, а високог утицаја – нерутинским ризицима, са којима се њихова организација сусретала.

Компарација налаза добијених анализом емпиријских података са налазима сличних истраживања спроведених у другим просторним и временским оквирима представљена је у резултатима истраживања, као потпоглавље „дискусија“.

2.1.4. Узорак истраживања

Истраживање је спроведено у системима идентификованим као критичне инфраструктуре у секторима енергетике, саобраћаја, банкарства, здравства, дигиталне инфраструктуре, водопривреде, отпадних вода и финансија, као и великих привредних субјеката у приватном власништву, у складу са Директивом Европске Уније 2022/207 и Уредбом о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије. У интервјуима је коришћен намерни узорак, будући да је било потребно одабрати оне учеснике који се налазе на руководећим позицијама у организацијама критичне инфраструктуре, то јест стручним лицима који планирају и спроводе мере управљања ризиком и континуитета пословања, било да је реч о стратегијама антиципације или отпорности.

2.1.5. Технике за прикупљање података

Узимајући у обзир комплексност предмета истраживања и анализе истраживачке праксе у овој области, те типа података које је потребно прикупити и анализирати, за извођење истраживања примењен је доминантно квалитативни приступ. Како је за постизање истраживачких циљева потребно стећи увид у ставове, идеје и мишљења менаџера безбедности, менаџера континуитета пословања и запослених у критичним инфраструктурама, те остваривање увида у налазе претходних истраживања која су се бавила истом или сличном тематиком, технике које ће се применити биће секундарна анализа података и полуструктурисани интервју.

Интервјуи су организовани углавном уживо у просторијама организација оператора критичне инфраструктуре. Услед ограничености финансијских и организационих ресурса један део полуструктурисаних интервјуа спроведен је онлајн путем рачунарских апликација за конференцијске позиве – Skype, Zoom, а поједини испитаници одговарали су писменим путем на питања послата електронском поштом. Коришћење онлајн платформи за прикупљање

квалитативних података позитивно је оцењено у студијама које су се бавиле овом тематиком, уз истицање повољности као што је уштеда на времену, лак приступ и осећај приватности (Archibald et. al 2019; Gray et. al, 2020; Zoia & Bode, 2015).

2.1.5.1. Секундарна анализа података

Секундарна анализа подразумева коришћење постојећих скупова података, њихово ново тумачење, извођење налаза или примену било каквих аналитичких процедура које претходно нису коришћене (Ђурић, 2013, стр.111). Секундарно су анализирани институционални подаци и претходне студије које су тематизовале ову област. Такође, у истраживању су коришћени и институционални подаци. Институционални подаци које поједине установе стварају независно од научних интереса јесу значајан извор постојећих подтака у квалитативном проучавању безбедности (Ђурић, 2013).

Секундарна анализа података је коришћена за прикупљање података о екстерном и интерном контексту организација идентификованих као критичне инфраструктуре. Ово укључује: политике безбедности, безбедносне планове оператора, планове континуитета пословања и друге планске и организационе документе којима ће се стећи увид у праксу организација критичне инфраструктуре у планирању одговора или приправности на нерутинске ризике. Такође, законодавни и стратешки оквири Републике Србије, али и других држава (Републике Хрватске, Босне и Херцеговине, Републике Црне Горе, Републике Македоније, Сједињених Америчких Држава, Уједињеног Краљевства, Аустралије), као и званични документи Европске Уније припадају корпусу институционалних података.

Интерни документи оператора критичне инфраструктуре били су махом недоступни, те се увид у праксу тих организација могао остварити тек применом технике полуструктурисаног интервјуа.

Секундарна анализа искуствене грађе из постојећих квалитативних и квантитативних академских и стручних истраживања примениће се у циљу остваривања ширине искуствене евиденције, али и компарације налаза добијених у току ових истраживања са налазима истих или сличних истраживања остварених у другим државама и на другим узорцима.

Синтетизовани налази добијени свеобухватним прегледом литературе коришћени су и за припрему водича за полуструктурисани интервју.

2.1.5.2. Полуструктурисани интервју

Полуструктурисани интервјуи су најчешћа техника у квалитативним истраживањима, јер се управо у таквом типу научног разговора могу остварити отвореност и флексибилност, а у исто време може се постићи оптималан ниво систематичности и структурисаности процеса прикупљања података (Ђурић, 2014).

Како је студија била дескриптивна и користила је експертске испитанике, одлучено је да се ослони на полуструктурисане интервјуе (Aberbach and Rockman 2002). Аутор ове дисертације сагласан је са ставом Далгард-Нилсенове приликом спровођења њене студије о отпорности јавних институција Краљевине Данске, то јест да доносиоци одлука играју значајну улогу у одређивању величине и природе простора унутар њихових организација у којој би се организационе праксе усмерене ка унапређењу отпорности могле одвијати (Dalgaard-Nielsen 2017, 342). Наше истраживање, према томе, обухватило је интервјуе са представницима највишег руководства у операторима критичне инфраструктуре, укључујући менаџере корпоративне безбедности и еквивалентне позиције, руководиоце организација или високо

позиционирана техничка лица укључена у планирање кризног одговора и континуитета пословања.

Досадашња истраживања су показала да менаџери безбедности и континуитета пословања имају бројне и контрадикторне претпоставке о томе како запослени и општа јавност реагују на ванредне ситуације, на пример, да ће паничити и неће пратити упутства (Pearce et al., 2011; Carter et al., 2014). Ове претпоставке имају импликације по планирање одговора на инцидент и могу резултирати неоптималним одговором запослених (Rogers & Pearce, 2013). Овим истраживањем утврђено је да сличне претпоставке поседују и професионалци задужени за безбедност и континуитет пословања у организацијама националне критичне инфраструктуре. Према томе, ова студија је користила низ полуструктурисаних интервјуа ради стицања дубинских увида у ставове и претпоставке менаџера безбедности и континуитета пословања о приправности, одговору и адаптацији на нерутинске ризике, понашању људи у екстремним догађајима, као и о одговорима на пандемију COVID-19. Такође, стећи ће се увиди и о пракси управљања нерутинским ризицима и управљањем континуитета пословања у организацијама који простим увидом у припадајуће планове и осталу документациону грађу не би били видљиви.

У првој фази истраживања идентификоване су организације критичне инфраструктуре и помоћу информаната су успостављени контакти са релевантним особама из организација. Укупно је организовано петнаест интервјуа, (додати број и врсте организација, позиције интервјуисаних), трајања од 30-120 минута.

Интервјуи су организован уживо када је то било могуће, али је углавном примењивана техника телефонских и он-лајн интервјуа (синхроних - путем Скајпа и Zoom-а и асинхроних – путем електронске поште). Примена он-лајн апликација за синхроно и асинхроно интервјуисање научно је утемељена у новијој методолошкој литератури. Четири интервјуа организована су уживо, док су осталих једанаест организовани он-лајн (два синхрона - путем Zoom апликације и осам асинхроних – путем електронске поште).

Интервјуисани учесници припадају високом менаџменту оператора критичних инфраструктура. Дванаест учесника је директно одговорно за послове корпоративне безбедности, један учесник је начелник (највиша позиција у организацији), док су два испитаника техничка лица (инжењерске струке) на челу кључних сектора својих организација. Сви испитаници су директно укључени у послове кризног планирања. Дванаест учесника је укључено или руководи пословима менаџмента континуитета пословања, док у три организације ови послови по систематизацији припадају другим секторима или нису присутни. Десет испитаника је из Републике Србије, три из Републике Хрватске и два из Босне и Херцеговине.

Према водичу за полуструктурисани интервју, који је дат у анексу ове дисертације, интервју је обухватио одговоре на седамнаест питања, од којих су три уводна и закључна, а четрнаест усмерених на само истраживање.

Интервју је структурисан је тако да питања покривају сва четири капацитета, то јест фазе, отпорности организација критичних инфраструктура, као и „тврдих“ и „меких“ аспеката отпорности. Аутор се водио тезама Бруноа и сар., Кековића и сар., Мадниja, Франсиса и Бекере (Bruneau et al., 2003; Madni, 2007; Department of Defense, 2011; Francis & Bekera, 2014; Kekovic et al. 2014) о идентификацији четири капацитета отпорности – антиципаторног, ресорптивног, адаптивног и ресторативног, као и аналитичког модела „рибље кости“ Гибсона и Таранта (Gibson & Tarrant 2010).

Три питања интервјуа директно су повезана са антиципаторним капацитетом (питања 2, 3 и 4), од шестог до седмог питања – ресорптивним и ресторативним (одређени делови одговора односили су се на ресорптивни, а одређени на ресторативни), док је пето питање намењено

анализи адаптивног капацитета организација. На питања од осам до једанаест добијени су одговори за чије је сегменте кодирањем установљено да одговарају сваком од четири капацитета отпорности. Дванаесто питање је везано за конкретну анализу свих капацитета у припреми, одговору, опоравку и адаптацији на пандемију вируса COVID-19.

Питања, такође, анализирају отпорност организација критичне инфраструктуре у складу са Холнагеловим тезом да отпорни системи морају бити способни да надзиру (да „знају шта посматрају“), антиципирају (знају шта да очекују), одговоре (знају шта даураде) и уче (знају шта се десило) (Hollnagel 2012; 2014a; 2014b). Затим, питања су усклађена и са одликама отпорности у складу са ASIS стандардом - Безбедност и отпорност организација и њиховог ланца снабдевања – Захтеви и смернице (ASIS ORM.1-2017), конкретно са захтевима о потреби за проактивним планирањем, као и оснаживањем запослених да одговоре на промене и нежељене догађаје на информисан начин.

Тврдња Вилдавског да „да бисмо одабрали антиципацију као најбољу могућу стратегију за одређену ситуацију, морамо прво доказати да су највећи ризици са којима се сусрећемо они које можемо предвидети уз високу вероватноћу“ пружила је теоријску основу за формулисање питања везаних за идентификацију претњи, анализу ризика и креирање и увежбавање сценарија за одговор. Претпоставка је да се за нерутинске ризике креирају кризни планови и планови континуитета пословања усмерени на штићене вредности, а што у литератури потврђује и Тарантов став да кризни планови и планови континуитета пословања служе као припрема за ефикасно функционисање организације у нерутинском моду. Питања везана за меке аспекте формулисана су у складу са идентификованим карактеристикама отпорности организација, према Гибсону и Таранту. Меки аспекти отпорности важни су за унапређевање отпорности другог реда, односно за отпорности на неизвесности и нерутинске ризике (Gibson and Tarrant 2010; Parsons 2010, Seville et al. 2006).

Потврђена хипотеза из докторске дисертације Ридлове (Riddle 2015) да искрено и прецизно извештавање запослених о озбиљном инциденту, нарочито о оном који је окарактерисан негативним атрибутима хазарда, као што су непостојање личног искуства с ризиком и тешкоће у поимању изложености и будућих ефеката ризика повољно утиче на спремност запослених да дођу на посао и тиме у знатној мери унапреде континуитет пословања, а у случају критичних инфраструктура и позитивно утичу на националну безбедност и отпорност, послужила је за формулисање питања четири, шест, седам и осам, као и за питање о организационом одговору на пандемију COVID-19. Шесто и седмо питање формулисани су у складу са теоријом ПМПП која је детаљно изложена у делу о перцепцији ризика. Напокон, Тарантова тврдња да је кризно планирање и комуницирање од значаја за одговор и отпорност на нерутинске ризике, утицала је на постављање седам од 11 конкретних питања.

Пето питање формулисано је у складу са теоријским постулатима и добром праксом динамичког адаптивног планирања, које је препознато као важан фактор адаптационог и антиципаторног капацитета организационе отпорности. Наиме, наведен је став који деле Бараса и сар. и Пајк, Доли, и Томани (Barasa et al. 2018; Pike, Dawley & Tomaney 2010) да је флексибилност политика, планова и процедура од највишег значаја за функционисање организације упркос изазовима.

2.1.5.3. План обраде података

Квалитативни облици анализе и обраде података укључују уочавање, испитивање, упоређивање и супротстављање и тиме откривање смислених образаца и правилности (Ђурић, 2013, стр.260). Квалитативни подаци добијени су секундарном анализом података и полуструктурисаним интервјуима. Интервјуи су снимани уз пристанак учесника, а затим су транскрибовани и анализирани применом тематске анализе, флексибилне истраживачке технике

којом је могуће идентификовати обрасце у подацима, такозване „теме“. Први корак у анализи представљао је читање транскрипата. Након тога, транскрипти су кодирани, уочавањем и категоризовањем важних образаца усклађених са истраживачким питањима, темама и индикаторима. Последњи корак представљало је поређење кодова и њихово комбиновање у теме и подтеме (Braun & Clarke, 2006). Теме у нашем истраживању представљају капацитети и аспекти отпорности, а индикатори – подтеме.

2.2. РЕЗУЛТАТИ

2.2.1. Антиципаторни капацитет

Капацитет	**Аспект**	**Индикатори**
Антиципаторни	Тврди	1. Планови (управљања ризиком, кризни планови и планови континуитета пословања) 2. Вежбање сценарија и обуке за кључно и некључно особље 3. Постојање слободних генеричких ресурса
	Меки	1. Партиципативни приступ планирању 2. Комуницирање ризика

Под антиципаторним капацитетом подразумевамо степен приправности на могуће поремећаје. Овај капацитет зависи од конкретних активности (тврди аспект) у смислу адекватне и свеобухватне идентификације претњи и процене ризика, израда сценарија и увежбавање одговора, обука и едукација запослених, те постојања слободних људских, финансијских, материјалних и других ресурса (знања, вештина) који се могу активирати у случају нежељеног догађаја. Антиципаторни капацитет је користан за оне ризике који се могу предвидети и о којима постоји темељно разумевање (de Bruijne, Boin & van Eeten 2010, 22). Другим речима, антиципација је важан сегмент у изградњи отпорности првог реда. Међутим, антиципација је такође битна за отпорност другог реда у смислу „очекивања неочекиваног“ кроз обезбеђивање слободних ресурса и планирања усмереног на штићене вредности и рањивости.

Меки аспект антиципаторног капацитета, то јест, оно што у свом моделу „рибље кости“ Гибсон и Тарант називају „карактеристикама“, обухвата партиципативни приступ који уважава богатство перспектива, искустава и знања запослених приликом планирања одговора на ризик и кризу, јер је у фази планирања, односно приправности или антиципације од виталног значаја да особе укључене у одговор имају довољно прилике у фази планирања да успоставе ефикасне односе са оним особама са којима ће их ванредно стање довести у додир, како унутар, тако и изван организације“ (Crichton, Ramsay & Kelly 2009, 33). Друга анализирана карактеристика јесте пракса комуницирања ризика којом се могу ублажити негативни атрибути хазарда, путем смањења конфликата кроз процес међусобног размишљања и уважавања мишљења.

2.2.1.1. Тврди аспект - активности

Идентификација претњи и анализа ризика су генерално први кораци који се предузимају како би се систем учинио отпорнијим на познате претње. Ово, такође, прати процена рањивости

и угрожености штићених вредности (Rodehorst et al. 2018). Према ASIS ORM.1-2017 стандарду проактиван менаџмент ризиком (антиципаторни капацитет) предуслов је унапређења ресорптивног, али и адаптивног капацитета. Антиципирање ризика организацији омогућава разумевање ефеката потенцијалних ризика на организационе циљеве или штићене вредности (Hamel and Välikangas 2003, Starr et al. 2003). Организационим праксама у домену предвиђања ризика, неочекиваних догађаја и могућих развоја ситуација организациони системи могу смањити своју рањивост и изградити свест запослених и доносиоца одлука (Hillmann & Guenther 2020, 6; Burnard & Bhamra 2011; Hamel and Välikangas 2003). Активности које лидери предузимају пре настанка кризе, као што су проактивно трагање за рањивостима и њихово разумевање и третирање, могу бити значајне за успешно вођење организације кроз кризу (James & Wooten 2010, Barton et al. 2015) или њено предупређивање (Rerup 2009).

Сви испитаници су потврдно одговорили да се процес процене ризика приоритизује у организацијама, те да постоје регистар ризика и припадајући планови управљања ризицима. Ажурирање регистара ризика и планова континуитета пословања истакнуто је у разговорима са представницима оператора телекомуникационе инфраструктуре:

- „Сваке године апдејтујемо регистре ризика јер се ствари мењају. Једном годишње имамо ресертификацију, спољне куће нам долазе и проверавају стандарде. С времена на време вршимо анализу, купимо повратне информације из читаве команије, из свих делова пословања, па их онда апдејтујемо и користимо у пословању.“ (Испитаник Г)
- “ Постоје формални процеси процене и управљања ризиком, кризама и континуитетом пословања. Процеси се обављају у складу са домаћим прописима, међународним стандардима, те техничким правилима везаним за специфичну делатност и важност критичне инфраструктуре. Наша организација има процене ризика из различитих области, физичко техничке претње, претње од природних и техничко-технолошких несрећа, те читав низ претњи из области одржавања поузданости и континуитета пословања и пружања услуга.“ (Испитаник Д)
- „Свакако постоје формални процеси процене ризика, криза и континуитета пословања. Преко осамдесет процената је у складу са међународним стандардима, а делимично по интерним процедурама поштујући принцип супсидијарности по дислокацијама. То се ради да би процедуре, упутства, процеси, активности и кораци били локално спроводиви, али не у колизији са међународним стандардима. (Испитаник Е)
- „Успостављен је троделни систем, са три подсистема изградње отпорности компаније, сваки са својим задацима и улогама, али врло уско повезани, увезани и надограђујући чине јединствен систем са својом сврхом, елементима, подсистемима и комуникацијом. Управљање ризицима и хитним ситуацијама спроводи се кроз целу организацију. У планирању се води рачуна и о специфичностима одређене локације, делатности, технолошким процесима, изворима опасности итд.“ (Испитаник Ж)
- „Да, постоје формални процеси процене и управљања ризиком. Такође, постоје интерне процедуре за управљање кризом, укључујући и кризни тим организације, а имплементиран је и стандард за управљање континуитетом пословања. Наравно, постоје и процедуре за одговоре на инциденте и ванредне ситуације.“ (Испитаник И)
- „Имамо све то, доста тога је предвиђено законом и стандардима. Планови и процедуре се редовно ажурирају, не само због законских обавеза и ресертификације, већ и због реалних потреба фирме.“ (Испитаник К)
- „Да, врло смо ажурни у том смислу. Редовно апдејтујемо регистар ризика, планове, правилнике, процедуре. Имамо их на и на кровном и на секторском нивоу. “ (Испитаник Л)

Планови континуитета пословања у складу са ISO стандардом 22310 нису присутни у свим организацијама у јавном сектору, али постоје слични планови који се тичу пословања у ванредним ситуацијама:

- „Ми сарађујемо са Министарством одбране, они нам долазе у инспекцијски надзор, шаљемо им документацију и ми имамо обавезу и у ратним и ванредним околностима да наставимо и одржавамо производњу. Ми то зовемо план континуитета, али је термин сличан и намера иста.“ (испитаник Б).
- „Имамо план производње вршења услуга у ванредним ситуацијама, од тога да вам 50 посто производње искочи из погона, у неким ратним ситуацијама како се сналазимо“ (Испитаник В).
- „Како су наши објекти критичне инфраструктуре ЕУ у мањкавости подзаконских прописа, ослањали смо се на властите процене претњи и штићења објеката кроз планирана улагања у системе безбедности.“ (Испитаник Ђ)

Поједини аутори истичу да се може постићи кроз размишљање о многоструким будућностима (Välikangas & Romme 2012, Ramirez et al. 2010). На пример, планирање сценарија може унапредити способност за препознавање или предосећање будућих ситуација код доносиоца одлука и запослених (Fink et al. 2005). Вогус и Сатклиф наглашавају да су организације које настоје да предвиде будуће догађаје склоније да предузимају континуирани надзор (скрининг) окружења и/или да врше симулације могућих неочекиваних догађаја (Vogus & Sutcliffe 2007, 2). Сагласно овим становиштима, ISO 22316:2017 стандард наводи да „високо отпорне организације отпорности имају капацитет да антиципирају и одговоре на претње и прилике и да се измене у условима неизвесности како би постигле своје стратешке и операционе циљеве.“

Израда сценарија је стандардни приступ у функцији антиципаторног капацитета отпорности и у пракси интервјуисаних представника оператора критичне инфраструктуре. Њихова примена је најчешће:

- „за оне догађаје који се понављају фокус је усмерен на стечена искуства и у складу са тим одговори се планирају у виду сценарија“ (Испитаник А)
- „Управо су примарно третирани највероватнији сценарији, а затим најгори могући сценарији.“ (Испитаник Ђ)
- „С обзиром на делатност, најизаженији су ризици који произлазе из техничко-технолошких процеса, пожари, експлозије, загађења животне средине, страдања људи, те се у том случају приступа у складу с процењеним нивоима могућих последица и штетних утицаја, па се одговор и планови израђују за претходно дефинисан ниво – значајан инцидент.“ (Испитаник Ж)
- „Сценарији се бирају на основу процене ризика, а њихова примена је за подизање свести запослених и руководилаца о ризицима и увежбавању одговора.“(Испитаник И)
- „Израђујемо и увежбавамо сценарије који се тичу како најфреквентнијих ризика, тако и оних са највећим последицама. Увежбавањем одговора доводи до преиспитивања и ажурирања планова и процедура, као и стицања знања, али и самопоуздања особа задужених за одговор.“ (Испитаник Љ)

Како Хилманова и Гинтерова истичу, покушај предвиђања могућих будућности путем сценарија и планирања одговора на ризике и кризе може довести до слепила према другим догађајима који нису очекивани (Hillmann & Guenther 2020, 6). Имплицитно прихватајући ову

премису, испитаници су махом истакли да се осим сценарија претњи, анализирају и сценарији последица:

- „Нама је то неодвојиво. Што се мене тиче, када радимо те планове и када их ажурирамо, увек морамо да предвидимо неке сценарије у смислу вектора напада, али увек имамо у виду и вредност коју штитимо (...) С једне стране нам је важно да анализирао потенцијални напад, колико је он чест, да ли наш систем може то да издржи, на пример да ли DDOS напад може нешто да обрише, уништи од података. То нам је изузетно важно да знамо шта све тим нападом може да буде угрожено.“ (Испитаник Г)
- „Фокус је на претњама, а мере и активности су евалуиране финансијски, те према учинковитости и делотворности у односу на утицаје – штићене вредности“. (Испитаник Е)
- „Када радимо управљање ризицима, онда израђујемо сценарија која су везана за претње. Ту се увежбавају процедуре одговора, коришћење заштитних средстава и тако даље. Што се тиче сценарија која су везана за последице, то је пре свега везано за континуитет пословања - шта ако нам ово постројење не ради? шта ако немамо струје? шта ако нам неки кључни запослени није на располагању? Ту онда, на пример, разматрамо алтернативне локације, набавку додатне опреме, алтернативних извора електричне енергије, обуке и дообуке за запослене.“ (Испитаник К)

Већина испитаника је истакла да се сценарија развијају за ризике и са највећом вероватноћом и са највећим последицама:

- „Сценарио је заснован са највећом вероватноћом, а последице могу бити различите у зависности од тога колико дуго траје недоступност.“ (Испитаник А)
- „Да, све узимамо у обзир, зато што ако испустимо неке од тих сценарија, после је касно, ви немате неку бекап варијанту, не можете да је покријете и онда се ту праве планови за посебне врсте.“ (Испитаник Б)
- „Обраћа се пажња и на једно и друго. Постоје ризици који су учестали, интензивни, али који не изазивају тешке последице. Ми као компанија ако не водимо рачуна о последицама, него сам о ризицима, мислим да бисмо правили грешку. Ми водимо рачуна и о једном и о другом. Не могу да искључим ниједан сценарио. (...) Постоје делови система који су боље штићени од других, рецимо наша веб страница и напад на њу неће допринети неком великом проблему, али ако доживимо неко цурење података или нам буде блокиран део базе података, то може да буде веома опасно за компанију.“ (Испитаник Г)
- „Сваки ризик је прошао идентификацију, анализу, мерење ризика и мере за спречавање или сузбијање ризика. У тренутној констелацији неки од сценарија који су идентификовани, обрађени и увежбани су: поплаве, пожари и експлозије, терористички напад, субверзија и диверзија, те сајбер напади.“ (Испитаник Ђ)
- „Развијамо и увежбавамо различите сценарије, како оне са високом вероватноћом а релативно малим последицама, као што су крађе, тако и оне ређе али са високим последицама. Ипак то су углавном неки рутински ризици за које постоје процедуре, као на пример пожар - нисмо га имали годинама, али увежбавамо одговор. То је једноставан пример, има наравно и сложенијих, али не бих ишао у детаље.“ (Испитаник И)
- „И једно и друго, пошто први могу имати кумулативно велики утицај на пословање, а друге због катастрофалних последица, ако и кад се догоде.“ (Испитаник Л)

Коначно, обуке за одговор на идентификоване ризике и уопште активности подизања свести о ризицима присутне су у свим операторима критичне инфраструктуре обухваћеним

истраживањем. Ипак, испитаници су на различите начине оценили степен обучености својих кључних и некључних запослених:

- „Никада није довољно. Потребно је чешће то чинити пре свега кроз обуке и тренинге. Наравно и нормативно дограђивати постојеће процедуре и упутства“ (Испитаник А)
- „Ми имамо сталне обуке, тренинге, радионице сталног карактера и из свих области. Ја на почетку године правим план шта би нам то било важно. Један део тренинга држи и сектор безбедности и ако на нивоу фирме постоји довољан број запослених, онда организујемо то. Зовемо и спољне фирме, државне органе, све који могу да допринесу (...) Имамо стални план провера свих запослених, од генералног директора па надаље. Правимо фишинг и антифишинг кампање, најављене или ненајављене, пуштамо лажне мејлове по фирми да видимо како ће људи реаговати. Провежбавамо разне сценарије. Имали смо на срећу, прошле године такву ситуацију. Прошле године су биле, на пример, оне честе дојаве о постављеним бомбама. То је и нас закачило. То је било први пут да и ми исконтролишемо како тај план и процена заштите ризика и анекс о евакуацији зграде како то функционише.“ (Испитаник Г)
- „Нико не воли ту обавезу (обуке). Неки јесу, неки нису обучени. Не могу да генерализујем, колико год да их обучавате, неки ће бити овако или онако. Не можете правити генерализацију јер имате запослене који су савесни, одговорни, свесни протокола, процедура, а има и оних других. Разних људи има у нашем систему.“ (Испитаник Б)
- Никад није довољна освешћеност и спреност на одговоре код људи, независно да ли говоримо о конкретној критичној инфраструктури и њеном сектору безбедности, или уопштено. Периодичне обуке су кључне да се људи држе у стању правовремее и прописане реакције, међутим јасно нам је да постоје хазарди који могу направити изненађења на које људски фактор не може утицати: јаки разорни земљотреси као у Турској 2023, затим терористички напади који се изводе брзо и ненадано. Код осталих запослених изражена је континуирана потреба за едукацијом, нарочито јер они нису примарно безбедносно оријентисана лица, те је потребно вршити фреквентније обуке и чешће их подсећати ради развијања безбедносне културе. (Испитаник Ђ)
- „Свака криза је специфична, са својим захтевима и изазовима, тако да се супротстављање покреће од стратешког нивоа, а спровођење одлука и активности је на тактичком и оперативном нивоу. Спровођење одлука, имплементација и учинковитост зависе од квалитетне, правовремене и свеобухватне интерне комуникације којом ће на одговарајући начин поруке допрети до свих запослених. Тако да можемо рећи да нису сви радници директно упознати са системом, осим кроз основне постулате у интерној регулативи, која је свима доступна путем Интранета. Непосредни судионици, чланови тима, оперативна подршка, упознају се кроз редовне радионице, вежбе за столом (једноставне, комплексне, симулацијске) где употпуњују своја знања, стичу додатно самопоуздање, развијају тимски рад, процес доношења одлука, без обзира какав је сценарио постављен за вежбу.“ (Испитаник Ж)
- „Тешко је генерализовати, има запослених који желе да науче нешто ново, да се усавршавају, а има и оних других којима то представља само додатну обавезу. Постоје системски покушаји, дакле на нивоу организације, да се константно ради на подизању свести о безбедносним ризицима, на јачању безбедносне културе. Мислим да смо имали солидне помаке.“ (Испитаник Ј)
- „Обуке су веома важне за запослене у циљу подизања свести о могућим ризицима и претњама. Такође, вежбање сценарија је битно за чланове кризног тима. У теорији је то тако. У пракси би требало, али се често испрече неке друге, хитније обавезе, посебно

када вежбе и обуке укључују руководећи кадар. Није то због недостатка свести, то би био прелободан закључак, јасно је свима да је безбедност основа свега, ипак притисак текућих обавеза често преовлада. Што се тиче обичних запослених, дакле оних који немају директну улогу у кризном планирању и у континуитету пословања за њих организујемо обуке, трудимо се да им објаснимо које су њихове улоге. Они присуствују, али са колико ентузијазма и колико тога "покупе" са едукација то је већ друго питање." (Испитаник Љ)

Према Вилдавском, (Wildavsky 1989) располагање слободним, генеричким ресурсима је од кључног значаја за одговор на неизвесности и нерутинске ризике. Студије о организацијама високе поузданости (High Reliability Organizations – HRO) показују да оне улажу ресурсе у превенцију и третман одређених ризика, али и успостављају организационе праксе за импровизацију и употребу слободних ресурса када и како су им потребни, иако претходно нису имали сазнања да ће им бити потребни (Wildavsky 1989, 433). У складу са становиштем Вилдавског, Вилијамс и сарадници такође истичу да отпорност укључује импровизовање и коришћење генеричких ресурса (Williams et al. 2017, 746).

Међу испитаницима постоји сагласност да је потребно постојање додатних ресурса, али се они углавном разумеју као наменске материјалне или финансијске залихе:

- „Ми немамо такве врсте резерве, имамо планове који су везани за функционисање плана шта нам треба. Ми смо обавезни да Министарству достављамо уговоре да имамо те сировине у случају проглашења ванредног стања, предочимо им ту врсту уговора, ту врсту средстава за функционисање. (...) Води се рачуна колико се може о тој некој едукацији запослених, конкретно ви не можете заменити неког инжињера који ради у производном погону, али он надгледа притиске, протоке, али ми немамо једног таквог инжињера. Имамо их четири или пет људи који се ротирају с њим и раде. Те процесне линије су сличне и сви они су у разним фазама каријере били на сличном производном процесу. То вам је та комоција коју имамо као запослени, да може ту свако да утрчи кад треба." (Испитаник Б)
- „Слободни материјални ресурси увек постоје јер морате да имате капацитете и додатне количине лекова. У сваком тренутку морате да знате где вам шта стоји и са чиме располажете." (Испитаник В)
- „Нас је пандемијска криза освестила да морамо да правимо залихе. Схватили смо да смо препуштени сами себи, од набављања маски до разних других средстава" (Испитаник Б)
- „Ми неколико година унапред планирамо те трошкове, шта треба да се купи од опреме, кад истичу лиценце, међународна путовања. Гледамо планове, рецимо, ове године треба да заменимо камере, па онда треба да се замени овај сервер, па да се обнови нека лиценца... Део нам одлази за хитне трошкове, али и на то да се новац планира за неке капиталне трошкове на нивоу године." (Испитаник Г).
- „Постоје наменски људски и материјални ресурси који су предвиђени за случај кризних ситуација" (Испитаник Ђ)
- „По плану континуитета пословања и из њега деривираним Плановима опоравка организацијских јединициа одређена је динамика ангажмана потребних ресурса у складу са БИА анализом утврђеним RTO и MTPOD. У случају ескалације кризе изван тих оквира, у процесу управљања кризном ситуацијом треба ангажовати додатне ресурсе, интерне или спољашње." (Испитаник Е)
- „У подручју управљања хитним ситуацијама планирају се потребни ресурси и капацитети за одговор (...), за шта је наравно потребно планирати и осигурати

финансијска средства. (...) У случају кризног менаџмента, а с обзиром на врло непредвидив развој и захтеве ситуације, како се показало и за време епидемије, није могуће оставити финансијска средства „да седе на рачуну“, јер компаније живе и раде на тржишту. Задатак је тима кризног менаџмента да се прилагоди захтевима и да управља свим аспектима пословања компаније у кризним условима“. (Испитаник Ж)

- „Немамо такве врсте слободних ресурса, ако не говоримо о финансијским резервама које се морају предвидети контингентним плановима. “(Испитаник Ј)
- „У сектору безбедности немамо додатна средства која бисмо активирали у случају неког већег ванредног догађаја. Постоје материјални ресурси у виду додатне опреме, извора електричне енергије, као и финансија.“ (Испитаник К)

Што се тиче расположивости слободних људских ресурса, приметна је разлика у одговорима између јавног и приватног сектора.

- „Постоје запослени који долазе од куће (у случају повећане потребе за запосленима), а ако то није довољно, узимамо људе из других установа.“ (Испитаник В – јавни сектор)
- „Води се рачуна колико се може о тој некој едукацији запослених, конкретно ви не можете заменити неког инжињера који ради у производном погону, али он надгледа притиске, протоке, али ми немамо једног таквог инжињера. Имамо их четири или пет људи који се ротирају с њим и раде. Те процесне линије су сличне и сви они су у разним фазама каријере били на сличном производном процесу. То вам је та комоција коју имамо као запослени у јавном сектору, да може ту свако да утрчи кад треба.“ (Испитаник Б – јавни сектор)
- „Ја у секјуритију немам огроман број људи, некад је више, некад мање, људи иду на боловања, одморе. Добра ствар је та што људи могу да раде и од куће. Водимо рачуна и о томе, нарочито ако дође до кризе у ИТ сектору, као прошле године кад је постојала бојазан да ће нас један део људи напустити у потрази за бољим послом и већим платама.“ (Испитаник Г – приватни сектор)
- „Немамо тај луксуз да можемо да запошљавамо вишак људи које бисмо могли активирати у случаје неке кризе или одсуства већег броја запослених. За запослене организујемо различите врсте едукације и обука, тако да могу привремено покрити пословне задатке и обавезе колега.“ (Испитаник Л - приватни сектор)

2.2.1.2. Меки аспекти – карактеристике

Поред присуства организационих пракси процене ризика, планирања управљања ризиком, континуитета пословањем и одговора на кризу, обука, израде и увежбавања сценарија и постојања слободних генеричких ресурса потребно је анализирати и начин на који се они спроводе, а на то нам указују „меки“ аспекти антиципаторног капацитета организационе отпорности.

Анализирајући литературу и, пре свега, Гибсонов и Тарантов модел „рибље кости“, дошли смо до закључка да би међу карактеристике антиципаторног капацитета превасходно требало уврстити партиципативни приступ планирању и комуницирање ризика.

Већина испитаника дало је потврдне одговоре на учествовање различитих интерних сектора и лица, у процесима процене и планирања:

- „Како је текао нацрт документа људи из различитих сектора, свако је био дужан да изради референце безбедности, да ли су поштовани стандарди, сценарији, слабе тачке, старост објеката.“ (испитаник Б)

- „Најчешће нису укључени сви, али остављена је могућност да се укључе сви они сектори или њихови делови који могу бити од користи. Различити сектори дају представнике тимова за континуитет пословања и кризних тимова, а укључују се и запослени који сами нису чланови, онда када се сматра да за тим има потребе. (...) Пажња се поклања и сарадњи са екстерним институцијама где и кад год је потребно.“ (Испитаник А)
- „Овиси о ком делу и сегменту пословања се ради. Увек су укључени одређени делови пословања, на пример финансијског пословања, маркетинга, продаје, па се онда иде на уже делатности, не морају сви да се укључују у то. (...) Сектор безбедности је власник тог процеса, али то не значи да се односи само на нас, него ми координишемо, укључујемо разне секторе и ово далеко превазилази посао делатности сектора безбедности. Рецимо за сертификације и ресертификације за ИСО 27001, апсолутно сви сектори су били укључени јер сви имају интерес да буду максимално заштићени у протоку информација, од маркетинга, информација, продаје, технике... Безбедност мора да буде зачин у свакој чорби.“ (Испитаник Г)
- „У процесу планирања одговора не учествују само неки топ менаџери, руководиоци на нижим функцијама, већ нам често долазе стручни и школовани људи на нижим позицијама. (...) Дакле, обичај је да иду руководиоци, али могу и људи на нижим нивоима. На пример, менаџери имају бољи увид, на извору су информација и могу одмах сутрадан да пренесу шта треба, док људи на нижим позицијама можда понекад нису најсналажљивији, али ми понекад делегирамо и те људе.“ (Испитаник В)
- „Све кључне особе су укључене у одржавање континуитета пословања у складу са својим вештинама и компетенцијама. Такође, именоване су и њихове замене, тако да се осигура континуитет контакт тачки и континуирана доступност оперативаца унутар компаније по принципу „24/7““ (Испитаник Ђ)
- „Сектор сигурности и заштите био је носилац свих иницијатива подизања и изградње свести о потреби улагања у системе безбедности. У деловање кризног тима организације укључени су сви сектори, кроз именоване чланове тима. Остали запослени су били укључени једино кроз редовне пословне активности.“ (Испитаник Д)
- „У подручју управљања хитним ситуацијама сви на локацији су укључени кроз упознавање с опасностима, начинима одговора, кроз оспособљавања и увежбавања и упознавања са својим обавезама. Кризни тим је састављен од највишег менаџмента компаније и представника подржавајућих функција (БЗР, корпоративне комуникације, безбедност, информационе технологије, финансије, људски ресурси, правни послови). У подручју континуитета пословања укључени су сви нивои одређеног бизниса, они су ти који најбоље знају шта раде, како раде, који су ресурси потребни, какви профили радника, одређених знања, компетенција, какве су зависности и међузависности, како интерне тако и екстерне. Дакле, просечни запослени су запослени јер они који непосредно испуњавају свакодневне радне задатке најбоље знају шта и како. Немерљив је њихов допринос у прикупљању информација и анализи стања, што је квалитетна подлога за израду анализе утицаја на пословање, анализе и управљања ризицима и плана континуитета пословања.“ (Испитаник Ж)
- „И у кризни тим и у тим за континуитет пословања укључују се представници разних функција и сектора, како добра пословна пракса налаже.“ (Испитаник З)
- „Да, укључени су припадници различитих сектора. Потребна су различита знања, профили, познавање пословних процеса и запослених. Нема само највише руководство улогу, оно је, наравно, одговорно, али у процесу планирања потребно је укључити што више људи како би се проблем сагледао из што више перспектива. “(Испитаник Л)

Такође, постоји сагласност међу испитаницима да је сарадња са екстерним заинтересованим странама од великог значаја приликом планирања и реализације одговора:

- „Код сарадње са екстерним институцијама, ту је ствар двослојна, има два аспекта. Ти негде имаш потпуну законску обавезу у одређеним областима који нису наш корпус – МУП, Министарство одбране, а с друге стране одржавамо добре односе са њима, сарађујемо и размењујемо информације о планирању.“ (Испитаник А)
- „Наравно, ми сарађујемо највише са Министарством одбране, поступамо по њиховим решењима, поготово кад су протоколи о посети странаца, извођачи, подизвођачи, БИА је више инволвирана у наше процесе, запошљавање лица, по било ком основу. Такође, Управа за ванредне ситуације. Они имају сав преглед наших капацитета, грађевинских машина, механизације, стручног кадра, узорковања. Имамо задатак у тој области и они су упознати са свим детаљима којим располажемо.“ (Испитаник Б)
- „Овде су безбедности секори укључени, од обезбеђења КЦ, полиције. (...) Што се тиче сектора права и финансија, они се тек касније укључују.“ (Испитаник В)
- „У случају мигрантске кризе имали смо сјајну сарадњу с МУП-ом на нивоу министарства и полицијских управа. Са свим осталим инспекцијским службама – заштита од пожара, заштита здравља, животне средине, цивилне заштите – имали смо редовне контакте кроз инспекцијски надзор и блиско смо сарађивали. Кроз размену мишљења родиле су се нове идеје за побољшање рада система сигурности организације.“ (Испитаник Д)
- „Када је у питању Босна и Херцеговина, постоји јако подељен ниво одговорности и надлежности везаних за сардњу са агенцијама из спектра система националне безбедности. Корпоративно су разрађени различити путеви комуникације са различитим нивоима система безбедности Босне и Херцеговине, у зависности од претње или хазарда. Примера ради, ако се ради о терористичкој претњи, активира се чак и сарадња са највишим елементима система безбедности, мислећи на државно Министарство сигурности и Обавештајно-сигурносну агенцију.“ (Испитаник Ђ)
- „Имамо сарадњу са релевантним институцијама и организацијама на националном и наднационалном нивоу. Они нису увек директно укључени у планирање, али их по потреби консултујемо“. (Испитаник Е)
- „У подручју управљања хитним ситуацијама значајна је сарадња са хитним службама (ватрогасци, полиција, хитна медицинска помоћ), а што је видљиво и код организовања вежби где су ванјски чиниоци укључени. Код кризног менаџмента је ситуација мало сложенија. Планирање, припреме и планови су интерни, а развој ситуације и захтеви који се могу појавити, као и сложеност ситуације диктира укључивање и сарадњу с највишим телима државне управе.“ (Испитаник Ж)

Комуникација ризика је важан сегмент меког аспекта антиципаторног капацитета. Другим речима, адекватна, двосмерна комуникација претњи и уважавање повратне информације од високог је значаја за јачање приправности и, последично, за пружање ефикасног и правовременог одговора. Премда се концепт комуницирања ризика пре свега односи на комуникације јавног сектора према грађанима, што је детаљно описано у теоријском делу дисертације, испитаници су имплицитно прихватили значај ове комуникационе праксе на нивоу своје организације.

- „Постоји двосмерна комуникација. Ни ја не знам све проблеме запослених и ја од њих тражим неки фидбек, морам са сњима да се консултујем јер ово је огроман систем. Ослањамо се јако на комуникацију, заједно процењујете и доносите закључке.“ (Испитаник А)

- „Имамо тај интерни систем комуникације којима обавештавамо запослене о свим мерама поступања. Оно што ми радимо кад делегирамо обавезе на друге секторе, ми их уредно обавештавамо, организујемо радне састанке. У тој селекцији, сви су упознати са тим. Имамо тај правилник којима их обучавамо, обавештавамо, али не идемо сад по дубини сваког запосленог. Они које сматрамо битнима, они су свакако упознати са тим стварима.“ (Испитаник Б)
- „Да, ту увек тражимо повратну информацију, осим ако баш неко из централе нешто не нареди. Ми имамо ИНФО портал и тамо су све информације које требају, употства, годишњим одморима, бонусима, најављујемо мере, тренинге итд. Сада иде сезона годишњих одмора и сада се јавља више инцидента јер се људи опусте. Сада смо имали неку кампању на порталу. Други канал комуникације је слање мејлова, да ли циркуларних мејлова свим запосленима или идемо на циљано слање на Тимсу (*Microsoft Teams*), па се селективно пушта одређеним људима. Онда, често се путем телефона чујемо, комуницирамо. Системи комуникације су распрострањени и увек тражимо повратну информације да покажемо да нисмо кочничари, него желимо да нађемо решење.“ (Испитаник Г)
- „Комуникација је увек двосмерна. При процени ризика и планирању одговора критички се усваја повратна информација, а у кризама се на темељу повратне инфромације дају даље инструкције..“ (Испитаник Е)
- „Комуникација је увек двосмерна. Прима се повратна информација те се процењује да ли она мења прописани приступ с обзиром на околности које се јављају у конкретној кризној ситуацији, нарочито на лицу места где се догађа кризна ситуација или њена последица.“ (Испитаник Ђ)
- Ради се на подизању свести радника о претњама и опасностима путем комуникацијских канала, едукација, оспособљавања, плаката, штампаних материјала, учествовања на вежбама у улози учесника (као чланови екипа или тимова) или посматрача на показним вежбама. Наравно, ослушкује се пулс, размишљања и коментари током вежби, реакције на материјале, имплементирана правила па се, на основу оцена и анализа предлажу побољшања. У складу с интерним документима сви радници, уговорни извођачи радова и сви који бораве и раде на одређеној локацији морају бити упознати с могућим опасностима на одређеној локацији и начинима одговора на ситуацију. (Испитаник Ж)
- „Ако мислите да ли се консултујемо са запосленима, одговор је да. Нарочито када су у питању нека осетљива и компликована питања на која један човек не може имати добар одговор. Наравно, не са свим запосленим, то би било немогуће, али знамо ко је стручан у којој области, ко можда има нека знања ван описа свог радног места, а која могу бити релевантна. Уважавамо и искусне запослене који можда нису на некој функцији, али су можда имали лично искуство које други немају, па је и њихово мишљење релевантно.“ (Испитаник И)
- „Користимо разне канале интерне комуникације. Добијамо повратне информације од запослених, а мере заштите се преиспитују у складу са њима.“ (Испитаник Л)

Из одговора интервјуисаних испитаника видимо да се у операторима критичне инфраструктуре доста пажње поклања антиципаторном капацитету. Ако посматрамо тврди аспект – активности видимо да су сви испитаници (n=15) потврдили да у њиховим организацијама постоје формализовани процеси анализе ризика, као и израде кризних планова и планова континуитета пословања.

Велика већина испитаника (n=12) потврдила је да се у њиховом организацијама развијају сценарија за одговоре на идентификоване ризике, односно сценарија усмерена на претње, док

три испитаника нису одговорила на ово питање. Једанаест испитаника навело је да постоје сценарији усмерена на ризике са највећом вероватноћом (највероватнији сценарио) и на оне са највећим последицама („најгори могући“ сценарио), док је један испитаник истакао да се бирају они којима је организација највише изложена.

Нешто мањи број (n=10) навео је и да се у организацијама развијају и сценарији усмерена на последице, односно на штићене вредности, један испитаник је одговорио негативно, док три испитаника нису дала одговор на ово питање. Иако је број испитаника који су потврдили да су развијали сценарија усмерена на последице једнак броју испитаника који су одговорили да у њиховој организацији постоји имплементиран систем менаџмента континуитетом пословања у складу са међународним стандардом, овим истраживањем нисмо могли доћи до закључка да је имплентиран стандард гаранција планирања сценарија усмерених на последице. Наиме, два испитаника, која су потврдно одговорила о постојању планова и формализованих процеса континуитета пословања усаглашених са стандардом, нису дала одговор на ово питање. Два испитаника дала су негативан одговор на ово питање, а одговор није добијен ни од испитаника који нису дала одговор на питање о постојању система менаџмента континуитета пословања у својим организацијама.

Сви испитаници (n=15) су потврдно одговорили да у њиховим организацијама постоје обуке, тренинзи, едукације и активности подизања свести за кључне и некључне запослене за одговор на ризике са највећом вероватноћом. Ипак, када је реч о резултатима тих обука, то јест о степену обучености и спремности запослених за реаговање постоје различита мишљења. Нешто преко половине испитаних (n=8) истакло је да је задовољно нивоом обучености како кључних, тако и некључних запослених, четворо испитаника је рекло да није задовољно нивоом обучености некључних запослених, док је троје навело да је ниво обучености индивидуална ствар запослених.

На питање о постојању слободних, генеричких ресурса одговори су варирали, међутим чини се да је појам генеричких ресурса недовољно разумљив испитаницима. Неразумевање питања и концепта слободних ресурса као једног од фактора за постизање организационе отпорности може се приписати различитим личним, образовним и професионалним својствима испитаника, као и њиховим позицијама и улогама у оквиру организација, а која не улазе у опсег овог истраживања. Један испитаник је навео да постоје људски, материјални и финансијски слободни ресурси који се могу активирати у случају непредвиђене ситуације. Шест испитаника слободне ресурсе протумачило је као наменске капацитете у смислу потребних људских, материјалних и финансијских ресурса за одговор на кризну ситуацију предвиђених контингентним плановима. Три испитаника разумела су слободне ресурсе искључиво као материјалне залихе (опреме, лекова, интернет сервере итд.). Два испитаника су навела да њихове организације поседују резервна финансијска средства. Напокон, два испитаника су навела да њихове организације немају такве ресурсе, док два испитаника нису одговорила на ово питање.

Велика већина (n=14) испитаника је изјавило да су представници различитих сектора укључени у процес менаџмента ризиком, кризама и континуитетом пословања. Један испитаник није одговорио на ово питање. Од тог броја (n=14) шест испитаника је експлицитно потврдило да су у процес планирања укључени и некључни запослени у свим секторима. Остали (n=8) су истицали да се процеси врше секторски, не улазећи у даље детаље, што даје простора за тумачење да су у оквиру сектора у процес планирања укључени и некључни запослени.

Такође, укључивање екстерних заинтересованих страна у процесе планирања присутно је у пословној пракси већине (n=9) оператора критичне инфраструктуре у региону. Два испитаника нису одговорили на ово питање, док је четворо одговорило негативно. Представници оператора критичне инфраструктуре у власништву објеката од посебне важности за одбрану (n=6) наводили су да се према законској обавези у процесе израде и ревидирања планова укључују и представници Министарства одбране. Од осталих екстерних страна испитаници су најчешће помињали Министарство унутрашњих послова, укључујући ватрогасну службу и управу за ванредне ситуације (n=8), Министарство здравља (n=5), Безбедносно-информативну агенцију и њене еквиваленте у региону (n=3). С друге стране, два испитаника су направила јасну дистинкцију између планирања одговора на ризик и управљања ванредним ситуацијама у које су укључене екстерне заинтересоване стране (хитне службе), и кризног планирања у које екстерне стране нису укључене.

Комуницирање ризика јесте један аспект партиципативног приступа управљању ризиком (Renn 2010). Велика већина испитаника (n=12) истакла је да у њиховим организацијама постоји дворсмерно комуницирање са запосленима. Два испитаника која су интервјуисана писаним путем изједначила су комуницирање ризика са кризним комуницирањем, тако да су њихови одговори на ово питање анализирани у сегменту посвећеном ресорптивном капацитету. Један испитаник није дао одговор на ово питање. Конкретни примери које су испитаници давали су консултовање са запосленима око могућих ризика и нежељених ефеката мера заштите (n=10), едукација путем обука, семинара и презентација (n=4), информисање коришћењем интерних канала комуникација (n=7), те праћење реакција запослених у току тих активности и уважавање повратних информација (n=3).

2.2.2. Ресорптивни капацитет

Капацитет	**Аспект**	**Индикатори**
Ресорптивни	Тврди	1. Кризни и други контингентни планови 2. Кризно комуницирање
	Меки	1. Осмишљавање (Sensemaking) и изоштреност (Accuity) 2. Креативност и флексибилност

У организационој димензији отпорности идентификовали смо два индикатора тврдог, и два индикатора меког аспекта отпорности. Пре свега, формални планови и процедуре за одговор на нежељени догађај, било на инцидент мањег интензитета, било на сложену и непредвиђену кризу темељ су ресорптивног капацитета. Ипак, како би одговор на нерутински догађај био ефикасан, осим формалних планова и процедура потребно је разумети и карактеристике тог одговора, другим речима „како се на кризу одговара?“.

2.2.2.1. Тврди аспект

Адаптирајући Гибсонов и Тарантов модел „рибље кости“, међу тврдим аспектима ресорптивног капацитета идентификовали смо постојање формалних процедура управљања кризама и кризног комуницирања.

Сви испитаници (n=15) су навели да у њиховим организацијама постоје формализоване процедуре кризног планирања на нивоу организације, као и различити контингентни планови на нивоима организације, али и организационих јединица.

- "Свакако, велики систем мора имати формализован процес кризног менаџмента. То је устаљена пракса. Постоји кризни тим на нивоу организације, а постоје и процедуре за његову активацију, редовност састанака, и тако даље." (Испитаник Б)
- „Постоје формални процеси управљања кризом. Постоје одговорне особе и њихови заменици, а што је регулисано писаним именовањима." (Испитаник Е)
- „Да, постоје формални процеси кризног менаџмента. За планирање и спровођење је директно одговорна управа компаније." (Испитаник Ђ)
- „Кризни менаџмент је у надлежности корпоративне безбедности која осигурава моделирање система, имплементацију, оспособљавање, радионице, вежбе, координирање активности у свим фазама, пре, за време и после кризе." (Испитаник Ж)
- „Управљање кризама је формализовано кроз планове који постоје за различите сценарије. Наравно, не може се свака ситуација предвидети, па планови нису толико детаљни, оставља се простора за импровизацију. Оно што је фиксно то су састав кризног тима и конкретна задужења чланова." (Испитаник З)
- „Да, у организацији постоји кризни тим на нивоу највишег руководства, кризни планови и сценарији, како на нивоу организације, тако и на нивоу организационих јединица " (Испитаник И)
- „Да, наравно. Кризни менаџмент је важан сегмент пословања и управљања ризиком. Ми томе приступамо озбиљно и наше руководство, али и запослени су прилично обучени и оспособљено за реаговање у кризним ситуацијама. " (Испитаник Л)

Код кризне комуникације са запосленима већина испитаника се слаже да је потребно уважити повратну информацију и на њеном основу адаптирати одговор.

- „Комуникација у досадашњим кризним ситуацијама била двосмерна, користећи све системе везе и јасно дефинисан поступак и начин комуникације. Као пример, навео бих комуницирање око корона вируса. Наиме, прописан поступак за поверенике цивилне заштите, који су свакодневно комуницирали са руководиоцима запослених на подручју за које су били задужени и извештавање сектора за корпоративну безбедност по тачкама дефинисаним упутством. Сектор за корпоративну безбедност је даље о прикупљеним подацима свакодневно мејлом извештавао тим за кризно управљање и надлежне државне службе" (Испитаник А)
- „Нама је увек потребан фидбек од сектора технике, људи из интернет саобраћаја, људи из оптике, и тако даље, овиси шта је била мета напада, да бисмо знали како и ми реагујемо. Друго, по слову закона морамо да обавештавамо и неке друге институције, тако да нам је та повратна информација врло битна, некада и важнија од онога што ми имамо." (Испитаник В)
- „Комуницирање са запосленима у току криза и значајних инцидената је свакодневно и без тога одговор не може да функционише. Сам тај облик комуникације је био константан. У току двадесет четири часа примимо информације шта се дешава, да ли на нашим објектима, да ли на улицама, на пример, код затварања саобраћајница. То је жив процес и ми морамо стално да будемо упознати са тим." (Испитаник Г)
- „Приликом криза се на основу повратне информације издају даље инструкције – налози." (Испитаник Ђ)

- „Интерна комуникација и укљученост, ангажман свих радника за време кризе од пресудног је значаја. Интерно комуницирање спроводи се кроз разне интерне канале комуникације. Комуникаца се одвијала директно с радницима, али и посредством линијских руководилаца, надлежних менаџера, након чека су се осигурале и повратне информације, размишљања и евентуалне препреке с којима се сусрећу радници. На основу повратних информација, а када је то било могуће и прихватљиво, притом мислећи на добробит свих, долазило је до одређених модификација активности и поступака.“ (Испитаник Ж)
- „Хитност је од кључног значаја при одговору на кризу, тако да се издају наредбе. Међутим, те наредбе су засноване на живим подацима који се добијају од запослених. Тако да је у принципу комуникација двосмерна.“ (Испитаник З)
- „ Постоје формализоване процедуре за екстерно и интерно комуницирање. То није у мојој надлежности, па ми нису познати сви детаљи. Из искуства знам да се тражи и уважава повратна информација, нарочито када је реч о већим инцидентима, то јест кризама, којима је узрок технички проблем. “ (Испитаник И)

Међутим, приметна је и тенденција код појединих испитаника да се комуницирање са запосленима за време кризне ситуације изједначава са издавањем наредби.

- „Приликом кризе постоји хијерархија и када би се све свело на повратне информације, не би се никад ништа завршило. Зна се ко одлучује, ко доноси одлуке и то је крајње једноставно.“ (Испитаник Б)
- „Уколико је релевантна повратна информација је укључена за прилагођавање одговора. Али поступање мора бити ауторитативно – наредбодавно.“ (Испитаник Е)

2.2.2.2. Меки аспект – карактеристике

Како би се избегла непрецизност у истраживању осмишљавању и изоштрености, ови индикатори су у интервјуима анализирани кроз одговор на конкретна питања о почетку кризе COVID-19:

1. Да ли се пандемија налазила у регистру ризика и да ли је по вашем мишљењу организација била приправна за одговор?
2. „У ком тренутку је било јасно да ће COVID-19 прерасти у пандемију и имати велики утицај на пословање“

Највећи број испитаника одговорио је да није имао пандемију у регистру ризика:

- „Пандемија није била у регистру ризика, али као појам заразне болести јесте третирана као могући ризик. Схватили смо озбиљност ситуације тек када је уведено ванредно стање. Компанија је врло брзо трансформисала своје пословање у циљу предузимања мера заштите запослених и стварања организационих услова за одржавање континуитета пословања“. (Испитаник А)
- „Нисмо имали пандемију у регистру ризика (...) Од самог почетка јер су прва два забележена случаја у држави били радници испод функције корпоративне безбедности.“ (Испитаник Ђ)
- „Одговор је „не“, нисмо то имали у регистру ризика. Но, врло брзо смо схватили да ће пандемија имати велики учинак на пословање организације када су забележени први случајеви у Европи. “ (Испитаник Е)

- „Нисмо имали пандемију у регистру ризика. Сећам се да је када смо чули прве вести из Кине да смо мислили да се то неће далеко проширити. Међутим, како се приближавало нашем региону и како су стизале вести о преминулима мишљење се променило.“ (Испитаник К)
- „Искрено, нисмо се толико бавили епидемијама, посебно не у сектору корпоративне заштите. Већи је акценат на класичним претњама од противправног деловања, сајбер криминала, техничко-технолошких несрећа, терористичких напада и слично. Почели смо да размишљамо какав утицај ће имати на наше функционисање када је вирус дошао у Европу и када су стизале застрашујуће вести из Италије. Опет, и тада је било опречних ставова у руководству, што није ни чудно јер су стизале опречне информације.“ (Испитаник Л)

Други испитаници истакли су да су имали пандемију у регистру ризика што је допринело бољој приправности на почетни одговор:

- „Имате неке планске ситуације, кад је био онај свињски грип, па смо правили план преношења, па смо имали као у ратној систематизацији и организацији посла. Тај домумент детаљно анализира наше потребе, да ми функционишемо са хиљаду осамсто људи, да систем функционише. Ми смо се ослањали на тај документ како смо радили са четрдесет посто капацитета. Систем је функционисао и са тако смањеним капацитетом. Смањили смо могућност преношења вируса. Иста је ситуација била и кад је избило ванредно стање и епидемија.“ (Испитаник Б)
- „Пандемија је увек била и биће у нашем регистру ризика. Ипак, знате шта, нисмо били припремни од првог дана, али временом је све било боље и били смо спремнији од неких других система.“ (Испитаник В)
- „Изненађујуће је било да смо имали унапред разрађен и сценарио за случај заразних болести. Наравно, корона је била изненађење за све те смо сви успутно учили о њој кроз едукације ангажовањем епидемиолога и вирусолога. (...) У тренутку када је ова претња дошла на територију Европе, тј. већ средином јануара смо покренули активности набавке првог контингента опреме за заштиту од заразних болести – маски и средстава за дезинфекцију“ (Испитаник Д)
- „Пандемија/епидемија је била укључена као ризик који се разматрао, те је за такву ситуацију направљен одређени генерички план који је био у надлежности сектора за безбедност и здравље на раду. Разрађени су одређени оперативни поступци, потребна материјална средства, сарадња с телима државне управе, здравственим системом на разним нивоима итд. Да, можемо рећи да је тај план у одређеној мери помогао и био примењив, али развој ситуације и размера утицаја ситуације и ескалација тражили су врло прилагодљив одговор, а посебно у повезаном процесу одржавања континуитета пословања“. (Испитаник Ж)
- „ Да, епидемија је стални ризик који треба да постоји у регистру ризика. Сад, планови су генерички, нисмо ми били нешто посебно приправни на то и поред чињенице да је епидемија била присутна у регистру. Од самог почетка смо се трудили да тај план освежимо и прилагодимо ситуацији будући да је вирус представљао врло озбиљну претњу по здравље свих запослених.. Колико смо били успешнији у одговору то је тешко закључити, али ни у једном тренутку нам пословање није долазило у питање.“ (Испитаник Љ)

У нашем истраживању испитаници су махом давали предност поступању према плановима, док се флексибилност и креативност у примени решења приликом криза прихвата као крајња нужност:

- „Увек постоје правилници који се поштују. У случају да постоји нешто што није предвиђено правилником, тек тада можете да се окупите и да видите шта ћете даље. Али, то је крајња инстанца.“ (Испитаник Б)
- „Увек се ради према интерним процедурама и препорукама надлежних органа. (...) Али, увек се врше анализе конкретне ситуације, јер се увек понове изнова нове околности које дају ново светло и димензију одговора на већ обрађене и третиране кризне ситуације“. (Испитаник Д)
- „Увек се превасходно треба придржавати законских и интерних процедура, а онда, наравно, овисно о претњи и импровизовати. Ја сам увек заговорник израде процедура на претње и константно преиспитивање истих, али није увек могуће све предвидети.“ (Испитаник Е)
- „До сада се увек поступало по плановима и процедурама, прихватајући развој ситуације“. (Испитаник Ђ)
- „У принципу се поступа према плановима и процедурама. Ми се трудимо да оне не буду превише детаљне, јер свака криза има своје специфичности које се не могу предвидети.“ (Испитаник З)
- „Поступа се према закону и према интерним правилницима, а у оним случајевима када је потребно импровизује се одговор. “ (Испитаник Љ)

Мањи број испитаника истакао је немогућност прецизног планирања одговора:

- „Ви кренете од плана, а онад вам се деси нешто што одскаче од тога. Не можете предвидети све околности. Била је и епидемија ковида, па су то непредвиђени ризици. Имате неке планске ситуације, кад је био онај свињски грип, па смо правили план преношења, па смо имали као у ратној систематизацији и организацији посла.“ (Испитаник Б)
- „Приступ кризном менаџменту, па тако и плану кризног менаџмента је генерички, општи. Модел који смо применили показао се као учинковит, јер свака је криза специфична и манифестује се на врло различите начине, па тако и на примеру недавне епидемије. Тим кризног менаџмента је управљао „животом“ и пословањем организације. Рад тима кризног менаџмента је покренут а улога тима је да на основу доступних или у недостатку кључних информација процени утицај ситуације на људе, имовину, животну средину и углед компаније и донесе одговарајуће одлуке о деловању. С обзиром да нам је план кризног менаџмента општи, сажет документ, разумљив и употребљив, њиме је одређена структура, именовани чланови тима и њихове замене, одређена улога тима и задаци чланова, одређена комуникација и начини комуникације, критеријуми и механизми за активирање плана и тима, кључни детаљи за контакт, где се треба састати – с одређеном алтернативном локацијом или начином састанка, потребна опрема и подршка за рад, као и овлашћења и одговорности за доношење одлука. План је довољно флексибилан и прилагодљив изазовима ситуације.“ (Испитаник Ж)
- „Свака криза је специфична, те прецизно планирање корака одговора није решење које гарантује успешан исход. Важно је да су људи упознати са тим шта је њихово задужење, ко је ко у кризном тиму, ко је овлашћен да активира кризни одговор. Постоје, наравно, процедуре али увек се деси нешто непредвиђено па се изналазе решења у ходу. Имали смо ситуацију са короном, ко је ту могао да предвиди све кораке?“ (Испитаник И)

- „Планови морају бити флексибилни да би се могли мењати у складу са развојем кризе. Ја нисам заговорник крутих, детаљних планова, поготово када говоримо о дуготрајним и непредвидивим догађајима са којима немамо искуства.“ (Испитаник Ј)

Ипак, суочени са конкретним примером пандемије COVID-19 испитаници су једногласно истицали важност флексибилности и креативности у одлучивању и управљању кризом:

- „Да, у смислу доношења одлука за стварање услова за рад од куће, обезбеђивања потребних средстава за заштиту запослених, промена начина организације пословних посета, праћења стања заражених и извештавања о томе тима за КП и пословодства компаније, спровођења наложених мера надлежних државних органа, итд.“ (Испитаник А)
- „Планови су се мењали јер свака пандемија има своје карактеристике и специфичности и морате да организујете систем како ће да ради, ко може од пацијената да буде у додиру, ко не може, шта је за које пацијенте неопходно и онда доносите одлуке у складу с тим. Све те ствари морате да узмете у обзир, и у односу на своје капацитете.“ (Испитаник В)
- „Планови су мењани јер смо морали да се прилагодимо да што више људи ради од куће. Морали смо свим људима да обезбединимо адекватно опрему, инсталацију одређених програма на лаптоповима.“ (Испитаник Г)
- „Мењали су се више пута, јер је ова претња била новина која није само направила удар на здравље људи, него и на процесе рада и начин и функционисање приватног и пословног живота“ (Испитаник Д).
- „Мењали су се планови из разлога непостојања предметних сценарија и сталног, претежно непредвидивог развоја ситуације.“ (Испитаник Ђ)
- „Наравно, одлуке о смеру, начину одговора, поступцима и активностима мењале су се и прилагођавале врло динамичној и променљивој ситуацији, узроковано интерним, а исто тако и екстерним факторима, одлукама кризног штаба, ситуацији у суседним државама, у државама с којима послујемо, добављачима и пружаоцима услуга, извођачима радова, ситуацији с ланцима снабдевања итд. Састанци тима кризног менаџмента редовно су се одржавали према плану, а и ванредно, након разматрања ситуације доносиле су се одлуке о смеру деловања.“ (Испитаник Ж)
- „Као што сам напоменуо, крути и детаљни планови не би имали употребну вредност током ковида. Ми нисмо здравствена институција, а и да јесмо, видели смо да је и код њих владала конфузија, не само код нас, него и у свету. Прилагођавали смо се ситуацији, кризни тим се редовно састајао, дискутовао, гледао шта раде друге организације па је то примењивано и код нас.“ (Испитаник Ј)
- „Наравно, све се мењало у ходу. На пример, раније нисмо имали искуства са радом од куће, односно на даљину. Видели смо да је то могуће за одређен број запослених, па смо њима обезбеђивали услове за то. Нисмо имали сценарио за епидемију, поготово не оволико дуготрајну и која је погодила цео свет, али смо се снашли.“ (Испитаник К)
- „Мењали смо и адаптирали планове и процедуре. Имали смо епидемију у регистру ризика, али њена распрострањеност, трајање и интензитет утицала је на то да је наш план врло брзо постао неприкладан, па је константно мењан.“ (Испитаник Љ)

Капацитет за ресорпцију у контексту одговора на нерутинске ризике представља прву реакцију на манифестацију ризика. Тврди аспект, према Гибсону и Таранту су активности, дакле оно „шта се ради“ у том случају. Као индикаторе смо идентификовали постојање структура и процедура за кризно управљање и кризно комуницирање.

Узевши у обзир профил организација, величину и значај система из којих су одабрани испитаници, не треба да зачуди налаз да су сви (n=15) испитаници потврдили да у њиховим организацијама постоје успостављене формалне структуре (кризни тимови) као и процедуре (кризни планови). Два испитаника су навела да кризни планови и структуре постоје и на нивоу организационих и/или територијалних јединица.

Формални процеси кризног комуницирања такође постоје у већини оператера критичне инфраструктуре обухваћених интервјуима (n=13). Одговор на ово питање није добијен од два испитаника. Евоцирајући комуникациону праксу током пандемије COVID-19 десет испитаника је навело да је комуникација често била двосмерна, будући да ни доносиоци одлука, тј. чланови кризног тима нису имали довољно знања, ни довољно јасних информација. Дакле, и кризна комуникација је имала одлике партиципативног процеса у коме су информације са терена и увиди некључних запослених имали улогу у креирању порука које су слате од стране кризног тима.

На питање о присуству ризика пандемије, односно епидемије у регистру ризика, позитиван одговор је дало осам испитаника, пет је дало негативан одговор, а на питање нису одговорила два испитаника. Међу испитаницима који нису имали пандемију у регистру ризика, два испитаника су одговорила да су схватили да је реч о наступајућем реметилачком догађају изузетно великих последица тек када је у држави уведено ванредно стање, док су три организације то схватиле нешто раније – када су смртни случајеви забележени у Европи. Међу испитаницима осам оператора критичне инфраструктуре који су имали епидемију или пандемију у регистру ризика, двоје је истакло да је ситуација праћена од пристизања првих вести о новој епидемији у Кини, четворо – од ширења епидемије на тло Европе, док два испитаника није одговорило на питање.

Друго питање везано за осмишљавање и изоштреност тицало се спремности на реаговање на новонасталу ситуацију, односно шта је потребно чинити у одговору на нерутински ризик. Један испитаник чија организација није имала пандемију у регистру ризика, односно четири у чијим је регистрима ризика била уврштена, одговорили су да су пандемију дочекали спремно, у смислу набавке заштитне опреме. Два испитаника која су потврдно одговорила на претходно питање, такође су навела да су генерички планови за управљање ризиком пандемије обухватала и сарадњу са експертским институцијама и едукације за запослене, док је један од њих као позитивно истакао детаљни план разрађен за пандемију тзв. „свињског грипа“ H2N2 који је био примењив и ефикасан на почетку пандемије COVID-19.

Други индикатор меког аспекта, то јест карактеристика ресорптивног капацитета односи се на присуство лидерства и толеранције вишесмислености а које охрабрује креативност и флексибилност одговора и планирања, насупрот традиционалном стилу војне команде. Већина (n=9) испитаника начелно је дала предност праћењу планова и процедура у току кризног одговора, док је пет испитаника навело да планови и процедуре не могу предвидети све ситуације. Два испитаника није одговорило на ово питање. Међутим, упитани за одговор на пандемију COVID-19, свих тринаест испитаника које је дало одговор на ово питање било је сагласно да је планирање и спровођење одговора морало бити креативно и флексибилно. Наиме, према испитаницима постојећи планови и процедуре су се морали мењати у ходу, а одговор је константно морао бити прилагођаван непредвидивом развоју ситуације и проблемима узрокованим поремећајима у глобалном ланцу снабдевања.

За разлику од антиципативног капацитета у којем смо задобили одговоре који махом потврђују добру праксу преовлађујућу у корпусу академских и стручних истраживања, из индикатора ресорптивних капацитета теже је извести валидне закључке. С једне стране постоје формализовани процеси кризног менаџмента, фокус на планско и процедурално реаговање на ванредне и кризне ситуације, те партиципативни приступ кризног комуницирања, што је у

складу са добром праксом. С друге стране, одговори добијени на питања о карактеристикама, меком аспекту, ресорптивног капацитета указују нам потенцијално на неколико изазова:

1. Препознавање и правовремено осмишљавање неочекиваних догађаја;
2. Повезивање нових неочекиваних догађаја, тј. актуализација нерутинских ризика, са претходним сличним догађајима (изоштравање - accuity).
3. Дискрепанција између преовлађујућег уверења испитаника да се прецизни планови и процедуре могу применити на нерутинске ризике и реалне ситуације приликом његове манифестације (пандемија COVID-19).

2.2.3. Ресторативни капацитет

Капацитет	**Аспект**	**Индикатори**
Ресторативни	Тврди	1. Систем менаџмента континуитетом пословања
	Меки	1. Суочавање са стресом 2. Међуповезаност (Сарадња са екстерним заинтересованим странама - другим оператерима критичних инфраструктура, експертском заједницом и хитним службама).

Тврди аспект ресторативног капацитета представља постојање система менаџмента континуитетом пословања, пре свега свеобухватних планова континуитета пословања и његових сегмената (процена ризика, анализа утицаја на пословање, план одговора итд.).

2.2.3.1. Тврди аспект

Постојање система менаџмента континуитетом пословања или еквивалентног специфичног главни је индикатор тврдог аспекта ресторативног капацитета отпорности организација. Управљање континуитетом пословања након ремећења врши се спровођењем активности и процедура предвиђеним планом континуитета пословања. План континуитета пословања значајан је за постизање отпорности и првог (услед постојања процене ризика као саставног елемента плана), и другог реда, будући да је менаџмент континуитета пословања превасходно приступ усмерен на штићене вредности, без обзира на претње.

Сви испитаници су одговорили да имају план континуитета пословања или интерне еквиваленте у складу са специфичним законским обавезама, будући да су често у питању објекти од посебног значаја за одбрану Републике Србије (Службени Гласник РС, бр. 112/2008) или еквиваленти објекти у суседним државама у складу са њиховим законским оквиром. Будући да су у питању сложени системи, планови постоје и на секторским нивоима.

- „У компанији је 2015 године имплементиран стандард (BCMS – ISO 22301) управљања континуитетом пословања и у складу са тим у компанији се спроводе активности којима се испуњавају захтеви утврђени наведеним стандардом.“ (Испитаник А)
- „Ми сарађујемо са Министарством одбране, они нам долазе у инспекцијски надзор, шаљемо им документацију и ми имамо обавезу и у ратним и ванредним околностима да наставимо и одржавамо производњу. Ми то зовемо план континуитета, а војници су мало мање софистицирани, али је термин сличан и намера иста.“ (Испитаник Б)

- „Да, то спада у сектор безбедности иако је некада било у коорпоративним пословима. То је касније нама све обједињено. Ми смо власници тог процеса иако тај систем превазилази оквире секјуритија, али неко то мора да надгледа и координише, те прописе, сертификате, провере. Ми имамо цео низ сертификата.“ (Испитаник Г)
- „Имамо планове континуитета пословања, у складу са међународним стандардима, домаћим прописима и техничким правилима везаним за специфичне делатности критичне инфраструктуре“. (Испитаник Е)
- „Изградња отпорности организације поред управљања хитним ситуацијама и кризног менаџмента, заокружује се имплементираним системом управљања континуитетом пословања, код нас опет у надлежности корпоративне безбедности, али наравно, бизнис је тај који је власник процеса.“ (Испитаник Ж)
- „Да, поред осталих стандарда имплементирали смо и стандард менаџмента континуитета пословања пре неколико година. Ресертификујемо се редовно, обучили смо једног запосленог за послове интерне ревизије, озбиљно приступамо томе. По мом мишљењу, то је врло користан систем јер вас дубински упознаје са организацијом и свим њеним елементима.“ (Испитаник И)
- „Имамо план континуитета у складу са међународним стандардом. То је релативно нов појам, нисам баш сигуран колико су просечни запослени упознати са њим, али вршимо обуке за оне запослене који су укључени у планирање и одговор.“ (Испитаник К)

2.2.3.2. Меки аспект – карактеристике

Карактеристике ресторативног капацитета, то јест оне карактеристике које се испољавају у фази опоравка су суочавање са стресом које је у овом истраживању посредно истраживано путем индикатора присуства, односно одсуства запослених са посла током реметилачког догађаја изазваним нерутинским ризиком и квалитет везе са екстерним заинтересованим странама, карактеристика коју следећи Гибсона и Таранта називамо међуповезаност..

Као прва карактеристика (меког аспекта) ресторативног капацитета отпорности узето је суочавање са стресом запослених. Индикатор за ову карактеристику било је одсуство запослених након реметилачког догађаја, конкретно одсуства током пандемије услед немедицинских разлога (Riddle 2015). Разлог за издвајање овог капацитета јесте што нерутински ризици, нарочито они окарактерисани негативним атрибутима хазарда, попут непознате заразне болести, могу узроковати недолазак запослених услед бројних физичких препрека али и психолошких разлога.

Испитаници су позитивно одговарали на питање о одсуству запослених за време корона вируса:

- „Од самог почетка усвојена је процедура о свакодневном извештавању свих оперативних центара компаније о стању здравља запослених. Евидентиран је сваки запослени који је оболео и праћен је његов ток опоравка. Применом мера заштите (маске, дезинфекција руку, поштовање дистанце, рад од куће, упућивање заражених на боловање и изолацију, рад у сменама, итд.) постигнуто је да и у највећим пиковима заразе компанија успела да у потпуности одржи континуитет пословања.“ (Испитаник А)
- „Не у значајној мери. Да је било, било је, али не у том мери да би се угрозио систем функционисања. Видите, неће нико да каже да су се уплашили и да неће доћи, него отворе боловање, кажу не осећају се добро, нешто се дешава. Ми знамо о чему се ту ради, али то је људски и ми то разумемо.“ (Испитаник Б)

- „Било је људи који су имали паничне нападе, заразиће се, умрећу, и ви ту не можете ништа. Правили смо зато селекцију запослених и ви када направите добар план, када избалансирате полну структуру, онда можете све да компензујете. Ми ћемо се онда прилагодити и систем ће функционисати.“ (Испитаник В)
- „Било је, у оним пиковима је било. Имаш неких послова који могу да раде у кући, али су проблем били ти шопови и продаја јер ту људи морају да долазе на посао. Ми смо на улазу пратили статитичке податке колико људи долази на посао, пратили смо и анализирали на дневном нивоу. Ми смо то пратили статистички. Било је пикова који су били страшни и велики број заражених, тако да је било и велики број одсутних. Било је отпора запослених (према доласку на посао). То су били људи са неким болестима. Ми смо им рекли да се пријаве сви који имају неке болести. Било је срчаних или онколошких болесника, неко је имао проблема са бубрезима, било је разних ствари. Једна колегиница је имала тешко болесног оца, па смо њој омогућили да месец дана не долази на посао. Имали смо колегиницу која је била вантелесном оплодњом у другом стању, и њој смо омогућили рад од куће. Били смо максимално коректни и ко год је могао да ради на тај начин, излазили смо му у сусрет.“ (Испитаник В)
- „У једном моменту је било одсутно око 20% запослених, било као последица заражавања или као превентивни превентивни начин да се не направе кластери заражених у компанији. Посебан изазов је била чињеница да запослени наше организације по пословној потреби имају обавезу да улазе у станове корисника услуга. Нарочито када је требало ући у станове клијената у којима је постојао формиран кластер или карантин, наши запослени су користили заштитна одела, средства, рукавице, маске. Напомињем да се у самој компанији није формирао ниједан кластер, нити се обуставио пословни континуитет пружања услуга.“ (Испитаник Д)
- „У критичним секторима корпорације постоји усвојена и проверена пракса и култура личне одговорности за себе и за одржавање критичних процеса на потребном нивоу, те је утолико било лакше превладати кризне периоде с већим бројем заражених у околини“. (Испитаник Ђ)
- „Сваки сектор је предложио која радна места могу обављати своје активности од куће, а у складу с предлогом Управа је донела одлуку. Мислим да је то био једини логичан и адекватан одговор за успешан континуитет пословања.“ (Испитаник Е)
- „Није било учесталог, у смислу неоправданог, одсуствовања, или да је неко нашао прилику за злоупотребу. Било је изостанака у складу с целом ситуацијом: болесни, карантин, изолације, нега чланова породице, деце... Све смо успели држати под контролом, захваљујући заиста одговорном понашању радника, доброј интерној комуникацији на свим нивоима, као и сарадњи с телима здравственог система“. (Испитаник Ж)
- „Знате како, људи различито реагују у таквим ситуацијама, небитно на којој су позицији.. Нарочито у почетку, неки су паничили, а неки су одлазили у другу крајност и правили се да се ништа не дешава. Показивали смо разумевање према запосленима који су спадали у ризичне категорије, као и онима који имају малу децу, или живе са старијим или болесним особама. Било је повремених изостанака, али добро смо се организовали па није било већих проблема, чак ни у пиковима. “ (Испитаник Л)

Међуповезаност, односно сарадња са екстерним заинтересованим странама, пре свега хитним службама, другим секторима критичне инфраструктуре као и експертским институцијама у значајној мери је допринео бржем опоравку након иницијалног догађаја, тј. акутне фазе. У случају пандемије коронавируса, нарочито је истакнута сарадња са сектором

здравства као фацилитатора и генератора брзог и ефикасног опоравка. Иако није експлицитно исказано, може се наслутити да је та сарадња позитивно утицала и на суочавање са стресом запослених, што је други меки аспекат ресторативног капацитета отпорности.

- „Ми смо један од највећих и најкритичнијих, ако тако могу да кажем, система у држави, те смо одмах добијали све податке од Института за јавно здравље. Имали смо добру сарадњу са њима, као и са хитним службама, министарствима унутрашњих послова и одбране. То је ипак давало неку сигурност запосленима, иако је значајан број њих свакодневно био изложен пандемији.“ (Испитаник А)
- „Сарадња током пандемије са свим релевантним институцијама је била задовољавајућа.“ (Испитаник Г)
- „Ми нисмо медицинска установа, тако да су информације и савети који су доспевали са стране, највише од Института за јавно здравље били од изузетног значаја.“ (Испитаник З)
- „Наравно, ми имамо тесну сарадњу са разним институцијама у мирнодопским условима, што је наравно важно у кризним ситуацијама. Тако и током пандемије. Знате, било је разних информација у медијима, па је сарадња са медицинским институцијама била важна за креирање порука и обавештавање запослених и прилагођавање планова и процедура. За то су били важни и контакти са другим организацијама са којима сарађујемо, консултовали смо се, на пример, око набавке заштитне опреме, добре праксе у организовању сменског рада и тако даље. “ (Испитаник И)
- „Пандемија је била комплексна криза и ситуација. Дуго је трајала и погодила је цео свет, пореметила је ланце снабдевања, покренула многа питања о дотадашњем начину пословања… Сами не бисмо могли испливати из такве ситуације, не само ми, него и свака друга организација. Било је потребно организовати много тога, адаптирати планове, борити се са разним информацијама и дезинформацијама. У таквом случају је свакако било јако важно имати поуздане савезнике и партнере у виду стручних институција и министарстава.“ (Испитаник Ј)
- „Не само ми, сви су били затечени развојем ситуације. Били смо са разним институцијама и службама стално на вези. Размењивали смо искуства и савете, добијали смо стручне савете који су нам користили за обавештавање запослених. Важно је успоставити и одржавати добре односе, то се показује у току кризних ситуација. “ (Испитаник Љ)

Систем континуитета пословања у складу са међународним стандардом ISO 22301 успостављен је у већини испитиваних оператора критичне инфраструктуре (n=10), док су три испитаника који су истакли да су објекти у њиховом власништву идентификовани као објекти од посебног значаја за одбрану рекла да постоје сличне процедуре у складу са прописима Министарства одбране. Два испитаника нису дала одговор на ово питање. Десет од тринаест испитаника потврдили су да је сектор корпоративне безбедности или његов еквивалент власник овог процеса, док су у другим организацијама за руковођење овим процесом, док је један испитаник навео да је власник процеса сектор корпоративних послова. Ово је значајно за интегративан приступ безбедности и отпорности организације будући да су сви индикатори тврдог аспекта, односно активности у три капацитета – антиципаторном, ресорптивном и ресторативном концентрисани у једној организационој функцији.

Као што је наведено суочавање са стресом је посредно анализирано путем питања о присутности, односно одсутноси кључних и некључних запослених током пандемије COVID-19, а у складу са налазима докторске дисертације Ридлове (Riddle 2015). Свих петнаест испитаника је изјавило да није било већих проблема у пословању њихових организација услед недоласка

већег броја запослених на посао. Фактори који су могли утицати на позитиван одговор запослених детаљно су анализирани су у наредном поглављу – Дискусија.

Други испитивани индикатор меког аспекта ресторативног капацитета отпорности тиче се међуповезаности, то јест сарадње са релевантним екстерним субјектима током и након трајања кризног догађаја. У случају пандемије коронавируса, нарочито је истакнута сарадња са сектором здравства као фацилитатора и генератора брзог и ефикасног опоравка. Наиме од тринаест испитаника који су дали одговор на ово питање, њих дванаест је посебно истакло здравствене институције, а осам испитаника је навело институте за јавно здравље, и у Србији и у региону. Сарадњу са ресорним министарствима поменуло је седам испитаника, а са хитним службама пет испитаника. Испитаници нису помињали сарадњу са другим организацијама из истог сектора, нити сарадњу са другим операторима критичне инфраструктуре.

Дакле, на основу интервјуа са њиховим представницима можемо закључити да оператори критичне инфраструктуре доста пажње поклањају ресторативном капацитету отпорности. Наиме, велика већина испитаника (n=13) је потврдила да у њиховим организација постоји систем менаџмента континуитетом пословања, сви испитаници су потврдно одговорили да у њиховим организацијама није било масовнијег одсуства кључних и некључних запослених које би утицало на функионисање система (n=15), док је такође велика већина (n=13) истакла сарадњу са екстерним заинтересованим странама. Напоменимо поново да се ово односи само на организациону димензију отпорности, те да је могуће да би се другачији одговори добили на питања о инфраструктурно-техничкој, финансијској и социјеталној димензији отпорности.

2.2.4. Адаптивни Капацитет

Капацитет	**Аспект**	**Индикатори**
Адаптивни	Тврди	1. Динамичко адаптивно планирање
	Меки	1. Организационо учење

Адаптација обухвата прилагођавање ресурса, интерперсоналних процеса и организационих рутина у циљу третирања утицаја реметилачког догађаја (Danes et al. 2009; Glover 2012). Адаптацију такође неки аутори изједначавају са способношћу организационог учења (Brewin, Andrews & Valentine 2000; Bonanno, Westphal & Mancini 2011). У литератури углавном постоји сагласност да је адаптација главно дистинктивно својство отпорности. Адаптивни капацитет присутан је у свим темпоралним фазама кризе или реметилачког догађаја (пре-кризе „t-1“, током „t“, и након „t+1“), а који у мањој или већој мери одговарају антиципативном, ресорпционом и ресторативном капацитету.

Нерутински ризици по својој дефиницији приморавају систем да функционише у нерутинском модусу, дакле системи се морају прилагодити новонасталој ситуацији будући да ће они утицати и на системе који га окружују и са којима имају односе зависности и/или међузависности. Тако, организациони системи морају привремено (t и/или t+1) или стално променити своју мисију, визију, дугорочне и краткорочне циљеве, начин функционисања, величину, организациону схему, број запослених, улоге запослених, измене у ланцу снабдевања и/или укључивање нових, емергентних технологија.

Литература о адаптивном капацитету отпорности организација најчешће анализира понашање организација као актера на тржишту. Међутим, специфичност организационих

система оператора критичне инфраструктуре је у томе што се услед њихове кључне улоге, а често и монополистичког положаја на географској територији на коме пружају своје услуге и производе, код њих неће одвијати крупне промене у смислу измене мисије, визије и дугорочних циљева. На пример, аеродром, електроенергетска мрежа, или банка не могу трајно променити своју основну мисију нити делатност, а што може бити случај са неким другим, тржишно оријентисаним организационим системима (малим и средњим предузећима, холдинг компанијама итд.).

Сумирајући налазе из литературе о адаптивном капацитету организације, а користећи Гибсонов и Тарантов аналитички модел „рибље кости“ као тврди аспект идентификовали смо динамичко адаптивно планирање, док је као меки аспект идентификована способност организационог учења.

2.2.4.1. Тврди аспект

Адаптивни капацитет може се посматрати кроз динамичко адаптивно планирање у свим кризним фазама – приправности, одговора и опоравка, то јест директно утицати на антиципативни, ресорптивни и ресторативни капацитет. Испитаници су махом одговорили да у њиховој организацији постоји пракса динамичког адаптивног планирања, то јест да се планови развијају тако да буду флексибилни, са високим степеном општости, те самим тим примењиви на велики број могућих сценарија:

- „Законска је обавеза да се планови редовно ажурирају, а и захтеви стандарда предвиђају надзорне провере на годишњем нивоу и сертификациону након три године. (...) Током пандемије коронавирусом редовно су се адаптирали, у смислу доношења одлука за стварање услова за рад од куће, обезбеђивања потребних средстава за заштиту запослени, промена начина организације пословних посета, праћења стања заражених и извештавања о томе тима за КП и пословодства компаније, спровођења наложених мера надлежних државних органа, итд.“ (Испитаник А)
- „Ви кренете од плана, а онад вам се деси нешто што одскаче од тога. Не можете предвидети све околности. Била је и епидемија ковида, па су то непредвиђени ризици. Имате неке планске ситуације, кад је био онај свињски грип, па смо правили план преношења, па смо имали као у ратној систематизацији и организацији посла. Тај домумент детаљно анализира наше потребе, да ми функционишемо са хиљаду осамсто људи, да систем функционише. (...) Ми добијамо структуру плана, али ми имамо толико специфичности да морамо да уђемо у наш неки оквир, да предочимо шта су наше могућности, специфичности, начин на који ми можемо да реализујемо, нпр. Имамо план производње вршења услуга у ванредним ситуацијама, од тога да вам 50 посто производње искочи из погона, у неким ратним ситуацијама како се сналазимо. Е сад, колико они имају употребну вредност, то је питање, али кад је било бомбардовање, то је било од користи.“ (Испитаник Б)
- „Увек постоје правилници који се поштују. У случају да постоји нешто што није предвиђено правилником, тек тада можете да се окупите и да видите шта ћете даље. Али, то је крајња инстанца. (...) Током пандемије правилници су се мењали јер свака пандемија има своје карактеристике и специфичности и морате да организујете систем како ће да ради, шта може од пацијената да буде у додиру, шта не може, шта може од пацијената да буде у додиру, шта не може, шта је за које пацијенте неопходно и онда доносите одлуке у скалду с тим. Све те ствари морате да узмете у обзир, и у односу на своје капацитете.“ (Испитаник В)

- „Не правимо их толико детаљне, не може се предвити свака ситиација темељно и то може да ти се врати као бумеранг. Дакле, то је грешка. А адаптибилни су и мењамо их, бар једном годишње, да ли је ово у складу са прописима, реалним потребама. Или то радимо ад хок или једном годишње. (...) Ево на пример ми имамо један сектор где раде само даме и оне рапортирају само генералном директору, раде ревизију свих процеса, прикупљају податке и оне нам некада предлажу јер оне раде ревизију. Баш скоро смо имали један њихов предлог који је био јако добар. Интерне ревизије су јако добре да се из постојећих стања изведу неки процеси. Нема ограничења да се планови мењају или апдејтују. Можда ми из секјуритија то најчешће иницирамо, али су проактивни и други сектори. (...) За време пандемије планови су мењани јер смо морали да се прилагодимо да што више људи ради од куће. Морали смо свим људима да обезбединимо адекватно опрему, инсталацију одређених програма на лаптоповима.“ (Испитаник Г)
- „Планови се понекад раде кампањски. Не може се све предвидети. (...) Стожер цивилне заштите је доносио мере одговора на пандемију, а ми смо их прилагођавали нашим условима.“ (Испитаник Д)
- „Планови су адаптибилни. Власник документа, то јест процеса, а по правилу је то функција корпоративне безбедности, ажурира релевантне документе (Стратегију, политике, планове, правилнике), које потом критички евалуирају релевантни чиниоци и експертно надлежни сектори. Високи менаџмент, то јест Управа која је ултимативно одговорна, их коначно усваја. (...) За време пандемије планови су се константно мењали и ревидирали из разлога непостојања предметних сценарија и сталног претежно непредвидивог развоја ситуације.“ (Испитаник Ђ)
- „Планови су се током пандемије корона вируса мењали више пута, јер је ова претња била новина која је направила удар на здравље људи, али и на процесе рада, слободу и начин функционисања приватног и пословног живота.“ (Испитаник Е)
- „Планови се редовно прегледају, ажурирају, мењају и допуњују, узроковано организацијским променама, кадровским променама, променама у одређеним производним процесима и активностима, променама унутрашњег и/или спољашњег контекста. Оно што је важно, ажурирају се и након спроведених вежби и тестирања планова и прописаних процедура кроз анализе и закључке, а ово је примењиво код управљања хитним ситуацијама, то јест довољно за довољно предвидиве сценарије, и код континуитета пословања. Код кризног менаџмента кад говоримо о плану, приступ је израда генеричког, општег плана, без разматрања посебних сценарија, а у складу с дефинијом кризе коју смо прихватили: неочекивана, неуобичајена и нестабилна ситуација која прети стратешким циљевима, угледу и одрживости, односно опстанку пословног система.“ (Испитаник Ж)
- „Да, као што сам напоменуо, не радимо планове кризног одговора превише детаљно јер су то превише комплексне ситуације, увек нешто крене другачијим током од предвиђеног. Ето, на пример, за време пандемије оно што смо мислили да имамо за пандемију је било довољно само за почетак, касније се то константно мењало и прилагођавало.“ (Испитаник З)
- „Морали су се мењати у ходу, у питању је била сасвим нова и неочекивана ситуација. Нисмо претходно имали искуства са пандемијским ризиком па смо кренули од нуле.“ (Испитаник Л)

2.2.4.2. Меки аспект

Адаптација се у литератури често повезује са појмом организационог учења. Претходна искуства са нежељеним догађајем у вези је са потоњом отпорношћу, мада постоји значајна

варијанца у природи овог односа (Brewin, Andrews & Valentine 2000; Bonanno, Westphal & Mancini 2011). Студија Бонана и сар. показала је да индивидуална отпорност на одређени догађај зависи од сличности тог догађаја са неким догађајем доживљеним у прошлости, али не са неким различитим типом догађаја (Bonanno et al. 2010). Отпорност, дакле, може бити олакшана искуственим „наученим лекцијама“. Ипак, то учење није линеарно нити статичко (Williams et al. 2017, 749).

У интервјуима, испитаници су махом одговарали да су учили током кризе и да су приправни на могућу будућу пандемију:

- „Главна научена лекција јесте да све изворе ризика и наступања реметилачких догађаја није могуће предвидети, али је важно брзо деловати и предузимати мере за смањење последица, трансформисати организацију појединих процеса у циљу налажења решења за настало стање. (...) У плановима континуитета пословања треба предвидети средства за набавку виталних делова, опреме, уређаје и систем (минимум и максимум резерве), без којих се не би могли одвијати кључни процеси, а поготову ако је за набавку исте потребно дуже време.“ (Испитаник А)
- „Добро је то искуство. Ја сам у том периоду из МУП-а прешао у ову организацију. Ми у МУП-у смо морали да долазимо на посао. Овде су биле ригорозне мере, маске апарати за дезинфекцију. Била је то добра школа, искушење, да човек може да види с чим се св суочава. Ја сам био убеђен да то никад неће доћи код нас, гледајући оне људе у Кини. Што се тиче фирме, било је тешко све то организовати, на пример, некоме цркне рачунар, па онда мора неко да оде лично, да инсталира систем, шифре. Сада је све лако, а тада је све била импровизација.“ (Испитаник Г)
- „Као кључан фактор за одговор на угрожавања показали су се устројење организације, едукованост радника, постојање процедура поступања као и комуникација са надлежним државним телима. (...) Конкретно током пандемије примарно је формирање залиха дезинфекцијског материјала и заштитних масти, а непосредно и дефинисање радних места без којих се не могу обављати редовне радне активности и наставити успешан континуитет пословања.“ (Испитаник Д)
- „Вишеструке су научене лекције, посебно је ојачан и конкретизован план заштите од епидемија. (...) Учење и спознавање је кључ сталног напретка, не само у безбедности него и у свим сферама живота. (...) Управљање и руковођење у кризним ситуацијама могу радити искључиво професинално оспособљене особе, које поред стручних компетенција и знања одликују и лидерске вештине. То су људи који никада не престају да читају и побољшавају безбедност у складу са актуелним и надолазећим трендовима и ризицима.“ (Испитаник Е)
- „Генерално гледано увек је потребно имати на уму да сваки део система треба да извршава свој део задатака и одговорности, да буде добро увезан и комуницира с другим подсистемима, а припрема и контрола, оспосабљавање и сарадња масовних медија од пресудне је важности. Неконтролисано ширење злонамерних, нетачних, непроверених информација, покушаји остваривања партикуларних интереса ствара додатну штету у напорима за овладавање ситуацијом. Добра комуникација, сарадња и сарађивање свих учесника увек мора одговорити на питања: ко, шта, када, где, зашто и како“. (Испитаник Ж)
- „Учење је било у најмању руку свакодневно, бар у почетку. За све у организацији је то била нова ситуација. На сву срећу нисмо имали преминулих, иако је неколико запослених имало теже симптоме. Вођена је евиденција и на крају смо урадили елаборат

у којем смо сумирали научене лекције, тако да сматрам да ћемо бити приправнији на неку нову сличну ситуацију.“ (Испитаник Ј)

- „Стечено је искуство за неке наредне пандемије и епидемије. Наравно, увек треба имати на уму да се сценарио из прошлости никада неће дословно поновити. Такође, ово је био добар тест и за нашу комуникациону праксу, поготову у светлу врло конфузних, а понекад и злонамерних информација које су се ширили медијима и друштвеним мрежама.“ (Испитаник К)

Само је један испитаник навео да су приликом пандемије корона вируса искористили научене лекције из пандемије свињског грипа (вирус H1N1):

- „Имате неке планске ситуације, кад је био онај свињски грип, па смо правили план преношења, па смо имали као у ратној систематизацији и организацији посла. Тај домумент детаљно анализира наше потребе, да ми функционишемо са хиљаду осамсто људи, да систем функционише. Ми смо се ослаљали на тај документ како смо радили са четрдесет посто капацитета. Систем је функционисао и са тако смањеним капацитетом. Смањили смо могућност преношења вируса. Иста је ситуација била и кад је избило ванредно стање и епидемија. Они који су могли, радили су од куће и то им је омогућено решењима. Ми који смо долазили и флуктуисали, чували смо се. С обзиром да је био локдаун, ми смо имали рекордно низак ниво кварова на мрежи. То су неке ствари које су нам ишле од руке, али смо трпили друге притиске од града да им промажемо у прављењу тих пирвремених смештаја, да им повезујемо канализацију. Имали смо проблеме са набављањем техничких средстава, маски, али у тим првим таласима. Морали смо да се довијамо и сналазимо. Свињски грип је био увертира.“ (Испитаник В)

Испитаник из сектора јавног здравља представља специфичан случај будући да одговор на пандемију представља једну од основних делатности организације:

- „Сад кад је прошла корона, људи не треба да се опусте, заправо већина треба, а они који су задужени за те ствари и који очекују да се може десити нешто слично, треба да буду на опрезу и да имају прегледе чиме располажете од људских ресурса, материјала и капацитета. Најгоре је када немате тај увид и ту се праве највеће грешке, а треба да оставите будућим генерацијама да се баве тиме.“ (Испитаник Б)

На питање о пословној пракси планирања, које је идентификовано као тврди аспект адаптационог капацитета, већина испитаника (n=12) је потврдила да се планови и процедуре праве да буду општи, флексибилни и лако измењиви, што је у складу са теоријом динамичког адаптивног планирања, док три испитаника нису одговорила на ово питање. Као разлог изменама планова у „мирнодопским условима“ пет испитаника је навело законске и сертификационе обавезе, док је осам истакло реалне потребе и измене у интерном и екстерном контексту. Током пандемије COVID-19 сви испитаници који су одговорили на питање (n=13) сагласили су се да је било константних измена и адаптирања планских докумената.

Као индикатор меког аспекта адаптационог капацитета идентификовали смо способност организационог учења. Узимајући у обзир хеуристику доступности, питање смо фокусирали на научене лекције током пандемије COVID-19. Сви испитаници (n=15) су одговорили да су из недавно завршене пандемије извучене лекције које им могу користити за унапређење планирања и одговора на будућу епидемију. Један испитаник је навео да је главна научена лекција да се не могу предвидети све претње и ризици, док је други навео да нова слична ситуација није немогућа и незамислива. За шест испитаника се главне научене лекције тичу потребе прибављања редундантних материјално-техничких средстава. Остале наведене лекције су

разноврсне – неопходност лидерских вештина током криза, тријаже информација у медијима, сарадња организационог система са подсистемима. Један испитаник је навео да су искуство и научене лекције током пандемије свињског грипа H1N1 помогле организацији да осмисли почетни одговор на нову пандемију.

2.2.5. Закључак

Теренско истраживање подразумевало је петнаест (n=15) полуструктурисаних интервјуа са представницима операторе критичне инфраструктуре у Републици Србији, Републици Хрватској и Босни и Херцеговини. Пет интервјуа је спроведено писаним путем, четири су спроведена лично, а шест путем рачунарских апликација Skype и Zoom. Услед ограниченог времена за интервјуе, као и понуђене опције да се на питања одговара писаним путем коришћењем електронске поште, нису сви испитаници одговорили на сва питања. Поједини испитаници који су одговарали писаним путем нису детаљно образлагали своје одговоре, нити су одговарали на пратећа питања која им је аутор слао. Будући да су се интервјуи организовали углавном током радног времена, три интервјуа су морала да буду завршена пре предвиђеног времена, тако да су испитаници нека питања или прескакали или су давали кратке одговоре. Услед тога, као и релативно малог узорка, истраживање неће покушати да изврши компарације између различитих сектора критичне инфраструктуре, јавног и приватног сектора, или различитих држава. Истраживање је пре свега усмерено на анализу ставова и мишљења особа које су укључене у процесе управљања кризама и континуитетом пословања по питањима пословне праксе, као и претходних и претпостављених когнитивних и бихејвиоралних одговора кључних и некључних запослених у случају актуализације нерутинских ризика.

Анализом интервјуа спроведених током теренског истраживања међу оператерима критичне инфраструктуре у Републици Србији, Републици Хрватској и Босни и Херцеговини дошли смо до следећих закључака у односу на постављене хипотезе:

Основна хипотеза овог истраживања јесте да је *стратегија отпорности имплицитно препозната као стратегија избора за управљање нерутинским ризицима у организационим системима оператора критичне инфраструктуре*. Добијени резултати су потврдили основну хипотезу истраживања. Наиме, сви или велика већина испитаника одговорили су позитивно на постављена питања у вези са системима менаџмента имплементираним у њиховим организацијама (систем менаџмента ризиком, континуитета пословања и кризног менаџмента и комуницирања). Затим, у организацијама постоји примена принципа динамичког адаптивног планирања, система обука и едукација за кључне запослене. Такође, у организацијама оператера критичне инфраструктуре усмерава се пажња и на меке аспекте отпорности у сва четири капацитета, што доприноси отпорности другог реда, то јест отпорности на нерутинске ризике и неизвесности.

Прва посебна хипотеза (*Х1 – Усмереност планирања одговора у оператерима критичне инфраструктуре је на рутинским ризицима на које се примењује стратегија антиципације*) је потврђена будући да су присутне праксе планирања одговора, планирања сценарија заснованим на сценаријима усмереним на претње (са највећом вероватноћом и/или са највећим последицама), те ставови већине испитаника о неопходности израде и придржавању формалних планова и процедура приликом одговора на кризу узроковану нерутинским ризиком. Исту усмереност видимо и у одговорима који се тичу слободних генеричких ресурса, као и организационог учења, а у којима се предност даје прибављању конкретних наменских и планских ресурса. Такође, имплицитно препознајемо усмереност на постизање отпорности првог реда у смислу одржавања односа међуповезаности са ресорним министарствима и хитним

службама, док се односи са експертском заједницом и операторима критичне инфраструктуре из истих или других сектора критичне инфраструктуре мање помињу.

Х2 - *За нерутинске ризике и неизвесности имплицитно се примењује стратегија отпорности кроз примену неформалних пословних пракси усмерених на карактеристике или меки аспект отпорности.* – Већина испитаника дала је позитивне одговоре на питања о карактеристикама капацитета отпорности. Постоје, ипак, разлике између ставова испитаника када су им постављена уопштена питања и на питања о искуствима током кризе COVID-19 (нпр. Да ли се у кризном одговору придржавате процедура или се импровизује? Да ли су се планови мењали и адаптирали током одговора на кризу индуковану пандемијом COVID-19?). Затим, карактеристике осмишљавања и изоштравања су различито оцењене од стране испитаника. Овај индикатор је такође посредно испитан питањима о COVID-19, а одговори нам указују на то да се надолазећа криза касно препознала, што је утицало и на почетни одговор. Питање усмерено на међуповезаност, то јест на односе са екстерним заинтересованим странама, показује усмереност на традиционалне сарадњу са хитним службама, надлежним министарствима и, у случају пандемије COVID-19 и експертским институцијама. С друге стране комуникација и сарадња са другим операторима критичне инфраструктуре није изричито поменута. Самим тим, ова хипотеза је само делимично потврђена и потребни су даљи истраживачки напори у том циљу.

Х3 - Напори доносиоца одлука и надлежних организационих јединица су равномерно усмерени на јачање сва четири капацитета отпорности. Одговори испитаника показују да је са мањим одступањима пажња усмерена на јачање сва четири капацитета отпорности:

Антиципаторни капацитет – Из одговора интервјуисаних испитаника видимо да се у операторима критичне инфраструктуре доста пажње поклања антиципаторном капацитету. Наиме, сви испитаници (n=15) су потврдили да у њиховим организацијама постоје формализовани процеси анализе ризика, као и израде кризних планова и планова континуитета пословања. Затим, велика већина испитаника (n=12) потврдила је да се у њиховом организацијама развијају сценарија за одговоре на идентификоване ризике, а такође (n=10) и да се у организацијама развијају и сценарија усмерена на последице, односно на штићене вредности. Сви испитаници (n=15) су потврдно одговорили да у њиховим организацијама постоје обуке, тренинзи, едукације и активности подизања свести за кључне и некључне запослене за одговор на ризике са највећом вероватноћом, иако одговор испитаника о ефикасности едукативних активности за запослене, то јест о степену њихове обучености и спремности за одговор на идентификоване ризике неусаглашен.

У оквиру антиципативног капацитета, партиципативни приступ планирању и комуникација ризика су идентификовани као меки аспекти или карактеристике, тј. на који начин се активности („тврди аспект“) извршавају. Треба напоменути да под комуникацијом ризика овде не подразумевамо комуникационе праксе формализоване кроз планове и интерне процедуре, већ као комуникациони сегмент партиципативног приступа управљању ризицима који смо издвојили због његове важности за развој приправности на неочекиване и нерутинске догађаје. Већина испитаника дала је одговоре који указују на примену принципа двосмерне комуникације ризика са запосленима и уважавања повратних информација. Код неких испитаника постоји недовољно разликовање комуницирања ризика и кризног комуницирања, тако да су њихови одговори на ово питање кодификовани као одговори на питање о кризном комуницирању.

Из одговора испитаника можемо извести закључак да оператори критичне инфраструктуре у Републици Србији и региону посвећују доста пажње антиципативном капацитету отпорности.

На четири од пет индикатора (три у оквиру тврдог и два у оквиру меког аспекта) већина испитаника дала је одговоре који су у академским истраживањима препознати као добра пракса у оснаживању организационе отпорности. Индикатор који смо негативно оценили јесте присуство слободних генеричких ресурса, за шта постулирамо три могућа разлога:

1. Неразумевање појма слободних генеричких ресурса;
2. Недовољан увид у стратешко пословање организације у којој су запослени;
3. Пословна пракса које се ослањају на принципе LEAN менаџмента.

Партиципативни приступ планирању одговора на ризик, укључивање различитих перспектива, као и добра пракса двосмерне комуникације ризика такође преовлађују у добијеним одговорима што је оцењено као позитивно у смислу постизања адекватне отпорности другог реда (отпорности на неочекиване догађаје и неизвесности), на индивидуалном, тимском и системском нивоу.

Ресорптивни капацитет - Капацитет за ресорпцију у контексту одговора на нерутинске ризике представља прву реакцију на његову манифестацију. Тврди аспект, према Гибсону и Таранту су активности, дакле оно „шта се ради“ у том случају. Као индикаторе смо идентификовали постојање структура и процедура за кризно управљање и кризно комуницирање.

Узевши у обзир профил организација, величину и значај система из којих су одабрани испитаници, не треба да зачуди налаз да су сви (n=15) испитаници потврдили да у њиховим организацијама постоје успостављене формалне структуре (кризни тимови) као и процедуре (кризни планови). Два испитаника су навела да кризни планови и структуре постоје и на нивоу организационих и/или територијалних јединица.

Формални процеси кризног комуницирања такође постоје у већини оператера критичне инфраструктуре обухваћених интервјуима (n=13). Одговор на ово питање није добијен од два испитаника. Евоцирајући комуникациону праксу током пандемије COVID-19 десет испитаника је навело да је комуникација често била двосмерна, будући да ни доносиоци одлука, тј. чланови кризног тима нису имали довољно знања, ни довољно јасних информација. Дакле, и кризна комуникација је имала одлике партиципативног процеса у коме су информације са терена и увиди некључних запослених имали улогу у креирању порука које су слате од стране кризног тима.

Карактеристике одговора на реметилачки инцидент које унапређују организациону отпорност другог реда односе се на способности доносилаца одлука (осмишљавање и изоштреност) да препозна претњу која раније не мора бити идентификована, то јест не налази се у регистру ризика и да јој прида смисао, односно да је повеже са неким другим ризиком који има слична својства. Друга карактеристика се односи на лидерски стил одражен у организационој култури која допушта креативност размишљања и флексибилност одговора и планирања.

Осмишљавање и изоштреност доносиоца одлука (појединаца и тимова, то јест руководства) анализирани су посредно, путем питања о препознавању могућности актуализације ризика пандемије. Прецизније, у ком је тренутку за доносиоце одлука вероватноћа избијања нерутинског реметилачког догађаја препозната као висока и на њу је требало реаговати, или користећи данас популарне термине Талеба и Вукерове, када је за доносиоце одлука „Црни лабуд“ постао „Сиви носорог“, предвидиви догађај изузетно високог утицаја.

На питање о присуству ризика пандемије, односно епидемије у регистру ризика, позитиван одговор је дало осам испитаника, пет је дало негативан одговор, а на питање нису одговорила два испитаника. Међу испитаницима који нису имали пандемију у регистру ризика, два испитаника су одговорила да су схватили да је реч о наступајућем реметилачком догађају изузетно великих последица тек када је у држави уведено ванредно стање, док су три организације то схватиле нешто раније – када су смртни случајеви забележени у Европи. Међу испитаницима осам оператора критичне инфраструктуре који су имали епидемију или пандемију у регистру ризика, двоје је истакло да је ситуација праћена од пристизања првих вести о новој епидемији у Кини, четворо – од ширења епидемије на тло Европе, док два испитаника није одговорило на питање.

Друго питање везано за осмишљавање и изоштреност тицало се спремности на реаговање на новонасталу ситуацију, односно шта је потребно чинити у одговору на нерутински ризик. Један испитаник чија организација није имала пандемију у регистру ризика, односно четири у чијим је регистрима ризика била уврштена, одговорили су да су пандемију дочекали спремно, у смислу набавке заштитне опреме. Два испитаника која су потврдно одговорила на претходно питање, такође су навела да су генерички планови за управљање ризиком пандемије обухватала и сарадњу са експертским институцијама и едукације за запослене, док је један од њих као позитивно истакао детаљни план разрађен за пандемију тзв. „свињског грипа“ H2N2 који је био примењив и ефикасан на почетку пандемије COVID-19.

Други индикатор меког аспекта, то јест карактеристика ресорптивног капацитета односи се на креативност и флексибилност одговора и планирања. Већина (n=9) испитаника начелно је дала предност праћењу планова и процедура у току кризног одговора, док је пет испитаника навело да планови и процедуре не могу предвидети све ситуације. Два испитаника није одговорило на ово питање. Међутим, упитани за одговор на пандемију COVID-19, свих тринаест испитаника које је дало одговор на ово питање било је сагласно да је планирање и спровођење одговора морало бити креативно и флексибилно. Наиме, према испитаницима постојећи планови и процедуре су се морали мењати у ходу, а одговор је константно морао бити прилагођаван непредвидивом развоју ситуације и проблемима узрокованим поремећајима у глобалном ланцу снабдевања. Такође, упркос релативно касном осмишљавању новонастале ситуације већина испитаника (n=10) је истакла да је врло брзо по избијању пандемије у Србији имплементиран адекватан одговор те да није било већих проблема у функционисању организација.

За разлику од антиципативног капацитета, у којем смо задобили одговоре који махом потврђују добру праксу преовлађујућу у корпусу академских и стручних истраживања, из индикатора ресорптивних капацитета теже је извести валидне закључке. С једне стране постоје формализовани процеси кризног менаџмента, фокус на планско и процедурално реаговање на ванредне и кризне ситуације, те партиципативни приступ кризног комуницирања, што је у складу са добром праксом. С друге стране, одговори добијени на питања о карактеристикама, меком аспекту, ресорптивног капацитета указују нам потенцијално на неколико изазова:

1. Препознавање и правовремено осмишљавање неочекиваних догађаја;
2. Повезивање нових неочекиваних догађаја, тј. актуализација нерутинских ризика, са претходним сличним догађајима (изоштравање - accuity).
3. Дискрепанција између преовлађујућег уверења испитаника да се прецизни планови и процедуре могу применити на нерутинске ризике и поступања у реалним ситуацијама (пандемија COV-2).

Ресторативни капацитет - Систем континуитета пословања у складу са међународним стандардом ISO 22301 успостављен је у већини испитиваних оператора критичне инфраструктуре (n=10), док су три испитаника који су истакли да су објекти у њиховом власништву идентификовани као објекти од посебног значаја за одбрану рекла да постоје сличне процедуре у складу са прописима Министарства одбране. Два испитаника нису дала одговор на ово питање. Десет од тринаест испитаника потврдили су да је сектор корпоративне безбедности или његов еквивалент власник овог процеса, док су у другим организацијама за руковођење овим процесом, док је један испитаник навео да је власник процеса сектор корпоративних послова. Ово је значајно за интегративан приступ безбедности и отпорности организације будући да су сви индикатори тврдог аспекта, односно активности у три капацитета – антиципаторном, ресорптивном и ресторативном концентрисани у једној организационој функцији.

Као што је наведено, суочавање са стресом је посредно анализирано путем питања о присутности, односно одсутности кључних и некључних запослених током пандемије COVID-19, а у складу са налазима докторске дисертације Ридлове (Riddle 2015). Свих петнаест испитаника је изјавило да није било већих проблема у пословању њихових организација услед недоласка већег броја запослених на посао. Ови одговори нам указују на неколико фактора који су могли допринети овако позитивном исходу. Према проширеном моделу паралелних процеса (ПМПП) четири фактора утичу на спремност за рад запослених током пандемије: перцепција озбиљности претње, перцепција личне подложности претњи, уочена ефикасност одговора и перципирана самоефикасност. Према неким ауторима (Barnet et al 2009; Balicer et al. 2010) поузданији предиктори одговора запослених су они који се односе на ефикасност одговора и самоефикасност. Што се тиче ефикасности одговора, оператори критичне инфраструктуре су, као и други пословни организациони системи, морали да се прилагоде тзв. „новој реалности“ пре свега омогућавању хибридног режима рада (рада на даљину), сменског рада, обезбеђивању организационих и физичких мера „дистанцирања“, као и заштитне и хигијенске опреме. Овакав одговор указује и на креативност и флексибилност, што је допринело осећању поверења према организацији. Перципирана самоефикасност је могуће производ обука и едукација, као и двосмерне комуникације ризика и кризне комуникације која је забележена у претходним одговорима у анализи антиципаторног и ресорптивног капацитета. Такође, као фактори који утичу на сагласност запослених да се појаве на радном месту током актуализације нерутинских ризика одликованих високим степеном негативних атрибута хазарда, у литератури се помињу конфликт улога (најчешће у смислу недоласка на радно место услед личне перцепције запослених о својим улогама као родитеља, деце старих и/или болесних родитеља, старатеља итд.) (Killian, 1952), идеје о важности своје професионалне улоге у одговору на ризик (Di Giovanni et al. 2003), те идентификацији са организацијом (Lee 1971; Mael & Tetrick 1992; Riddle 2015). Напокон, треба истаћи да је суочавање са стресом изузетно комплексан појам, чији је само један од аспеката долазак запослених на радно место.

Други испитивани индикатор меког аспекта ресторативног капацитета отпорности тиче се међуповезаности, то јест сарадње са релевантним екстерним субјектима током и након трајања кризног догађаја. У случају пандемије коронавируса, нарочито је истакнута сарадња са сектором здравства као фацилитатора и генератора брзог и ефикасног опоравка. Наиме од тринаест испитаника који су дали одговор на ово питање, њих дванаест је посебно истакло здравствене институције, а осам испитаника је навело институте за јавно здравље, и у Србији и у региону. Сарадњу са ресорним министарствима поменуло је седам испитаника, а са хитним службама пет испитаника. Испитаници нису помињали сарадњу са другим организацијама из истог сектора, нити сарадњу са другим операторима критичне инфраструктуре.

Адаптациони капацитет - На питање о пословној пракси планирања, које је идентификовано као тврди аспект адаптационог капацитета, већина испитаника (n=12) је потврдила да се планови и процедуре праве да буду општи, флексибилни и лако измењиви, што је у складу са теоријом динамичког адаптивног планирања, док три испитаника нису одговорила на ово питање. Као разлог изменама планова у „мирнодопским условима“ пет испитаника је навело законске и сертификационе обавезе, док је осам истакло реалне потребе и измене у интерном и екстерном контексту. Током пандемије COVID-19 сви испитаници који су одговорили на питање (n=13) сагласили су се да је било константних измена и адаптирања планских докумената.

Као индикатор меког аспекта адаптационог капацитета идентификовали смо способност организационог учења. Узимајући у обзир хеуристику доступности, питање смо фокусирали на научене лекције током пандемије COVID-19. Сви испитаници (n=15) су одговорили да су из недавно завршене пандемије извучене лекције које им могу користити за унапређење планирања и одговора на будућу епидемију. Један испитаник је навео да је главна научена лекција да се не могу предвидети све претње и ризици, док је други навео да нова слична ситуација није немогућа и незамислива. За шест испитаника главне научене лекције се тичу потребе прибављања редундантних материјално-техничких средстава. Остале наведене лекције су разноврсне – неопходност лидерских вештина током криза, тријаже информација у медијима, сарадња организационог система са подсистемима. Један испитаник је навео да су искуство и научене лекције током пандемије свињског грипа H1N1 помогле организацији да осмисли почетни одговор на нову пандемију.

Из одговора запослених можемо закључити да се пажња имплицитно поклања јачању адаптивног капацитета. Испитаници су свесни, нарочито у поводу пандемије COVID-19, да планирање мора уважити многоструке будућности и неизвесности, те је самим тим неопходно да планови буду што флексибилнији и адаптабилнији. Међутим, поједини испитаници су навели да је пракса ажурирања планова потреба у циљу испуњавања законских обавеза и захтева сертификације, односно усаглашавања са стандардима. Добијени одговори ипак не указују на формалну праксу динамичког адаптивног планирања које би укључивало експлицитно истицање потребе за прилагођавањем планова, спецификације система за надзор над променама у окружењу, те спецификације активности које треба предузети када се догоде одређени догађаји окидачи (Walker et al. 2001; Walker et al. 2019). Формални процес динамичког адаптивног планирања можемо повезати са стимулисањем организационог учења, односно анализе научених лекција. Другим речима, способност учења и извлачења правилних закључака из криза узрокованих нерутински ризицима позитивно утиче на праксу динамичког адаптивног планирања. Ово је у складу са моделом „рибље кости“ Гибсона и Таранта у којем је поред тога „шта се ради“ (тврди аспект – активности и способности) битно и „како се то ради“ (меки аспект - карактеристике). У овом погледу индикативни су одговори мањине испитаника (n=2) на питање о наученим лекцијама из пандемије COVID-19 који су истакли да су главне лекције немогућност предвиђања свих претњи и ризика и могућност избијања нових непредвиђених догађаја, што би следствено томе могло утицати на усвајање или даље формализовање праксе динамичког адаптивног планирања. Такође, ставови двоје испитаника да је потребно унапредити лидерске вештине и сарадње системима са подсистемима, те поклонити пажњу могућим дезинформација током комплексних нерутинских криза, указују на усмерење ка отпорности другог реда. С друге стране, већина испитаника је предност дала предузимању конкретних мера, пре свега прибављања заштитне опреме, што може указивати на усмереност ка постизању отпорности првог реда, то јест антиципацији познатих претњи.

2.3. Дискусија

Анализа 15 (n=15) интервјуа показала је да особе задужене за корпоративну безбедност, кризни менаџмент и континуитет пословања у операторима критичне инфраструктуре имају широк спектар мишљења и веровања о истраживаним тврдим и меким аспектима и капацитетима отпорности. Ова мишљења и ставови испитаници заснивају на личном искуству и конвенционалним приступима управљању безбедносним ризицима, кризама и континуитетом пословања, пре него на академским истраживањима.

2.3.1. Антиципаторни капацитет

Погледи су били углавном усаглашени у одговорима на питања која се тичу тврдих аспеката отпорности у свим капацитетима. Сви испитаници су се сложили да је планирање и имплементација планова управљања ризиком, планова одговора на инцидент, кризних планова и планова континуитета пословања од значаја за организације. Ово је у складу са Старковим налазима према којима кризни менаџери у ЕУ и УК осећају потребу да покажу компетентност кроз постојање планова и процедура без обзира на то да ли унапред смишљени планови и процедуре помажу или штете у одговору на сложене и динамичне ризике (Stark, 2014). Испитаници су у одговорима објашњавали организационе структуре својих система, као и њихова задужења у одговору на реметилачки догађај, што је било корисно за разумевање и тумачење њихових одговора на питања. Наиме, примећене су одређене разлике у одговорима оних испитаника који су искључиво задужени за процену и управљање безбедносним ризицима и кризни одговор, од оних чија улога такође укључује и менаџмент континуитета пословања.

Сви испитаници су се такође сагласили да је потребно развијати сценарије у циљу адекватног планирања одговора. Ово је позитиван став будући да је у литератури прихваћено да се приправност може постићи кроз размишљање о многоструким будућностима (Välikangas & Romme 2012, Ramirez et al. 2010), те да планирање и увежбавање сценарија може унапредити способност за препознавање или предосећање будућих ситуација код доносиоца одлука и запослених (Fink et al. 2005). Вогус и Сатклиф наглашавају да су организације које настоје да предвиде будуће догађаје склоније да предузимају континуирани надзор (скрининг) окружења и/или да врше симулације могућих неочекиваних догађаја (Vogus & Sutcliffe 2007, 2). Сагласно овим становиштима, Међународни стандард о организационој отпорности наводи да „високо отпорне организације отпорности имају капацитет да антиципирају и одговоре на претње и прилике и да се измене у условима неизвесности како би постигле своје стратешке и операционе циљеве“ (ISO 22316:2017).

Међутим, мањи број испитаника истакао је да је примаран фокус у креирању и изради сценарија усмерен на претње, док им приступ усмерености на штићене вредности својствен пре свега менаџменту континуитетом пословања није у фокусу. Ово свакако негативно утиче на отпорност другог реда (отпорност на неизвесности и нерутинске ризике) јер, како Хилманова и Гинтерова истичу, покушај предвиђања могућих будућности путем сценарија и планирања одговора на ризике и кризе може довести до слепила према другим догађајима који нису очекивани (Hillmann & Guenther 2020, 6). Ипак, треба истаћи да су такве одговоре давали они испитаници који нису задужени за континуитет пословања у својој организацији.

Још једна нијанса испитана интервјуом, јесте да ли су идентификовани сценарији засновани на највећој вероватноћи или на највећим последицама, које су испитаници називали и „најгори могући сценарији“. Испитаници су потврдно одговорили да узимају и један и други тип (највећа вероватноћа и највеће последице) догађаја у обзир. Међутим, испитаници су показали тенденцију у мишљењу да су сценаријима обухваћени сви могући догађаји, а што је

касније негирано приликом одговора на конкретна питања о пандемији, а што је у сагласности са поменутом тврдњом Хилманове и Гинтерове.

Наредни индикатор тврдог аспекта антиципативног капацитета отпорности јесте постојање слободних, генеричких ресурса. Ово питање је утемељено на тези Вилдавског да је располагање слободним, генеричким ресурсима од кључног значаја за одговор на неизвесности и нерутинске ризике, а што је он засновао на студијама о организацијама високе поузданости (High Reliability Organizations – HRO) које успостављају организационе праксе за импровизацију и употребу слободних ресурса када и како су им потребни, иако претходно нису имали сазнања да ће им бити потребни (Wildavsky 1989, 433).

Осим тога, као што је напоменуто, појам генеричких ресурса је био недовољно разумљив испитаницима, те су се углавном наводили примери планских и наменских додатних материјално-техничких ресурса и редундантности: као материјалне залихе у случају одговора на конкретни догађај из њиховог домена пословања (нпр. лекови, сервери, механизација), или користећи се хеуристиком доступности евоцирајући догађаје из пандемије COVID-19 (заштитне маске, дезинфекциона средства итд.). Испитаници су такође помињали нужност додатних финансијских ресурса које је потребно активирати у случају кризе, а што је у сагласности са ставовима из литературе (Wildavsky 1989, Williams et al. 2017). Друга тенденција присутна у одговорима јесте мишљење да су сви додатни наменски ресурси предвиђени кризним плановима и, нарочито, плановима континуитета пословања. Ово може бити недовољно у случајевима дуготрајних манифестација нерутинских ризика, попут пандемије COVID-19

Из одговора на ово питање можемо извести још две претпоставке. Прва је да је концепт слободних генеричких ресурса недовољно познат у професионалној заједници менаџера безбедности у региону, тако да би у неким наредним истраживањима питање било потребно расчланити на више засебних питања везаних за људске (укључујући и когнитивне), материјалне и финансијске ресурсе.

До другог закључка су нас навели одговори три испитаника. Испитаник запослен у јавном сектору нагласио је да код њих постоји већа „комоција“ за постојање слободних људских и материјалних ресурса него у приватном сектору. С друге стране два испитаника из приватног сектора су истакла да постоји врло ограничен простор за запошљавање и непланске набавке, користећи и термин „луксуз“. Такође, поједини аутори истичу да притисак ка штедњи у јавном сектору ограничава способност организација за улагање у структурне елементе отпорности као што су слободни генерички ресурси и стратешке резерве (Longstaff, 2012; Stark, 2014; Walker & Salt, 2006). Ово може бити показатељ да се организације у приватном власништву више него у јавном сектору руководе принципима тзв. LEAN менаџмента, у чијој основи јесте елиминација и смањење свих врста губитака и вишкова. Однос између принципа LEAN менаџмента и организационе отпорности јесте предмет интересовања и професионалне и академске заједнице. Истражујући примену овог концепта у управљању ланцем снабдевања Масларић и сар. закључују да LEAN стратегија умањује трошкове и расходе, али исто тако умањује и отпорност ланца снабдевања (Maslarić et al. 2013). Подаци које смо добили овим истраживањем ипак не омогућавају доношење конкретних закључака о односима између усмерености на LEAN менаџмент и приступа који би допустио више редундантности у смислу слободних генеричких ресурса у операторима критичне инфраструктуре, али би то свакако била препорука за даља истраживања.

У поређењу наших резултата са тим истраживањима, испитаници из нашег јавног сектора истицали су да постоји редундантност и „комоција“ са бројем запослених што је било од велике помоћи за време пандемије и претходних кризних ситуација. Испитаници и из јавног и приватног сектора истакли су важности обука и едукација запослених како би се могле покривати разне улоге, међутим постоји свест да се кључни запослени (стручна

високообразована лица) не могу лако заменити у случају недоступности, нити обучити некључне запослене за обављање њихових послова. Конкретно, у случају пандемијске кризе, сви испитаници су се сложили да је примена нових технологија за рад на даљину у великој мери унапредила доступност и кључних и некључних запослених.

Према неким ауторима организација може бити отпорна само колико су то појединци коју њу чине (Hillman & Guenther 2020, 3). Такође, Ленгник-Холова и сар. наводе да је разумевање индивидуалне отпорности почетна тачка за разумевање организационе отпорности, а која представља адитивни композит индивидуалних способности и деловања (Lengnick-Hall et al. 2011). Отпорност на индивидуалном нивоу може се унапредити кроз обуке и едукације запослених. Обуке и увежбавања одговор на сценарија и уопште подизања свести о ризицима присутне су у одговорима свих оператора критичне инфраструктуре обухваћеним истраживањем. Осим индивидуалних обука и вежби, према другим ауторима, сличне активности могу се вршити и на нивоима тимова, организационих јединица и самих организација, истичући истичући да се активности и одлуке доносе и извршавају на колективном нивоу (Salanova et al. 2012). Наиме, ови аутори разликују ресурсе на индивидуалном (индивидуална знања и вештине, те обуке које воде ка индивидуалној ефикасности и компетентности у обављању задатака који превазилазе рутинска задужења), тимском (акумулирано знање, диверзитет знања и варијабилност у саставу тимова, колективна ефикасност која у складу са теоријом емергентности није једнака збиру ефикасности чланова тима) и организационом нивоу (склоност ка организационом учењу, организациона култура која стимулише слање повратних информација, флексибилне процедуре и флексибилан трансфер знања, вештина и ресурса), те сматрају да се отпорност може постићи само њиховом интеграцијом (Sutcliffe & Vogus 2003). Већина испитаника навела је да су обуке присутне на индивидуалном, тимском и на организационом нивоу, док је мањи број испитаника поменуо и обуке на тимским нивоима. Такође, дистинкција је направљена између запослених у сектору корпоративне безбедности и осталих запослених. Испитаници су задовољни нивоом обучености и вештина запослених у сектору корпоративне безбедности, док поједини сматрају да остали запослени нису довољно обучени и освешћени за правилан и правовремен одговор на реметилачке догађаје присутне у сценаријима. Такође, један испитаник је навео и да се не може правити генерализација о дистинкцији између обучености у сектору безбедности и осталих запослених будући да се ради о индивудиалним когнитивним и бихејвиоралним разликама и склоностима ка учењу, праћењу протокола и процедура.

Према Реновом концепту, отпорност је инклузивни и дискурзивни приступ управљању ризиком који укључује јаке везе са заинтересованим странама, при чему квалитет размене информација игра одлучујућу улогу (Renn 2015). Партиципативни приступ у управљању ризицима утиче на умањење вишесмислености ризика, који су нарочито проминентни код нерутинских ризика (Lorenz 2010). Партиципативни приступ посматрамо као укључивање интерних и екстерних заинтересованих страна у процес планирања. Овакав приступ омогућава богатство перспектива и увида што је од великог значаја за квалитет одговора, нарочито када говоримо о комплексним, нерутинским ризицима и неизвесностима. Осим добијања корисних информација и мишљења са терена, на овај начин уважавају се запослени и тиме посредно уверавају о квалитету организационог одговора, а који је један од четири фактора ПМПП модела који утиче на расположивост запослених за извршавање радних задатака током догађаја одликованих високим степеном негативних атрибута хазарда, попут пандемије.

Већина испитаника дала је потврдне одговоре на учествовање различитих интерних сектора и лица, у процесима процене и планирања ризика, те израде кризних планова и планова континуитета пословања. Поједини испитаници су истакли да у процесу планирања не учествују искључиво представници високог руководства, већ да се укључују и стручна лица запослена на

нижим позицијама. Допринос некључних запослених јесте у томе што они обављају свакодневне задатке и „најбоље знају шта и како“.

Пажња коју организација поклања сарадњи и комуникацији са другим институцијама, организацијама и заинтересованим странама у процесу планирања такође доприноси на бољем одговору на кризе, то јест бољој отпорности организације. (Therrien, Tanguay & Beauregard-Guérin 2015). Специфичности организација оператора критичне инфраструктуре из којих су долазили испитаници у овом истраживању јесте да су они легислативним актима обавезни да у активности планирања одговора на ризик и кризних одговора укључе надлежна државна тела – Министарство унутрашњих послова, Безбедносно-информативну агенцију и, за оне организације које су идентификоване као објекти од посебног значаја за одбрану, односно одређене као велики технички системи од значаја за одбрану, Министарство одбране. Еквивалентни оквир примењује се и у другим земљама окружења чији су испитаници учествовали у истраживању. Наведено је да се, такође, кроз блиску сарадњу у оквиру инспекцијског надзора развијају нове идеје за побољшање система безбедности организација. Напокон, у случају пандемија позитивно је истакнута сарадња са експертским институцијама из области јавног здравља, а што је у сагласности са налазима докторске дисертације Ридлове (Riddle 2014).

Комуницирање ризика је важан сегмент меког аспекта антиципаторног капацитета. Бројне студије су показале да негативни атрибути хазарда, попут пандемије, могу бити ублажени адекватном комуникацијом ризика. Према Бороџичу, у сфери управљања ризицима, допринос комуникације ризика смештен је у контекст смањења друштвених конфликата кроз процес међусобног разумевања и уважавања мишљења. (Borodzicz 1996, 135) Проучавање и пракса комуникације ризика треба да у обзир узме различите перцепције ризика и тиме фундаментално смањи могућност настајања конфликта. Четири кључна аспекта за постизање овог циља су: информисање и едукација, утицање на промену понашања, обезбеђивање упутстава приликом инцидената и обезбеђивање решења конфликата. (Ibid) Главна сврха комуникације решења није да произведе неко свеважеће решење, већ да унапреди дијалог и сарању успостављањем заједничких циљева за људе са различитим очекивањима. (Кешетовић и сар. 2008, 525) Премда се концепт комуницирања ризика пре свега односи на комуникације јавног сектора према грађанима, приликом истраживања увидели смо да испитаници имплицитно прихватају значај ове комуникационе праксе на нивоу организације. Како смо детаљно изложили у теоријском делу истраживања, непружање свих потребних информација запосленима може резултирати неефикасним одговором (Rogers and Pearce 2011), као и до губитка поверења и статуса поузданог извора информација. (Riddle 2015, 38). Другим речима, адекватна, двосмерна комуникација претњи и уважавање повратне информације од високог је значаја за јачање приправности и, последично, за пружање ефикасног и правовременог одговора.

Испитаници су одговорили потврдно да се двосмерна комуникација уз уважавање повратне информације („фидбека“) примењује у њиховим организацијама, што је евалуирано као позитивно. Закључујући према одговорима испитаника, фокус комуникације ризика у редовним условима на ризицима са највишом вероватноћом са којима се организација сусреће (нпр. сајбер напади, екстерни и интерни имовински деликти, хазарди који потичу из услова рада или природе делатности организације). Нерутински ризици (нпр. „свињски грип“ или терористички напади) се комуницирају у случајевима њихове манифестације на другом географском подручју или у другој организацији из исте или сличне индустрије. Комуникација ризика пандемије COVID-19 извршавана је по упутствима из надлежних експертских установа, будући да је реч о новом и непознатом хазарду о којем запослени и надлежни нису имали довољно знања да формулишу своје препоруке. Како су се повратне информације узимале у

обзир, и како је корпус знања о COVID-19 растао на глобалном нивоу, тако су се упутства и препоруке мењале. Ово је у складу са налазима из докторске дисертације Ридлове да искрено и прецизно извештавање запослених о озбиљном инциденту, нарочито о оном који је окарактерисан негативним атрибутима хазарда, као што су непостојање личног искуства с ризиком и тешкоће у поимању изложености и будућих ефеката ризика, (нпр напади биолошким агенсима), могло повољно утицати на спремност запослених да дођу на посао и тиме у знатној мери унапреде континуитет пословања, а у случају критичних инфраструктура и позитивно утичу на националну безбедност и отпорност. (Riddle 2015) Налази из овог истраживања, такође, у складу су са препорукама истраживања усмерених на тему интерног комуницирања ризика са запосленима (Maule AJ 2009; Conchie & Burns 2008).

2.3.2. Ресорптивни капацитет

Способност за реаговање на догађај, односно ресорпциони капацитет, укључује истрајавање и подношење утицаја реметилачког догађаја уз одржавање функционисања и минимизирање настале штете (Fleming 2012; Gilly et al. 2014, Starr et al. 2003; Stephenson 2010; Weick & Sutcliffe 2007) Ресорпциони капацитет обухвата развијање могућих опција за одговор у што краћем временском року (Acquaah et al. 2011; Mallak 1998), са посебним нагласком на способност импровизовања (Weick 1993, Ray et al 2011), придавање смисла новонасталој, неочекиваној ситуацији (осмишљавање) и деловање како би се доносиоци одлука упозорили на развој ситуације и пословање задржало у оквиру прихватљивих перформанси, односно активно развили кризни одговори (Schulman et al. 2004,Weick et al. 1999).

У складу са овим тврдњама из академских истраживања као индикатори тврдог аспекта ресорптивног капацитета идентификовани су постојање структура и процедура за кризно управљање и кризно комуницирање. Кризни менаџмент и кризно комуницирање је оно „шта се ради“ у одговору на актуализацију нерутинског ризика.

Кризни менаџмент се може одредити као скуп функција или процеса који имају за циљ да идентификују, изуче и предвиде могуће кризне ситуације и успоставе посебне начине које ће организацији омогућити да спречи кризу или да се са њом избори и да је превазиђе уз минимизирање њених последица и што бржи повратак у нормално стање (Кешетовић 2018. 124). Сви испитаници су навели да у њиховим организацијама постоје формализоване процедуре кризног планирања на нивоу организације, као и различити контингентни планови на нивоима организације, али и организационих јединица. Такође, у организацијама постоје успостављене структуре – кризни тимови, сачињени од представника разних сектора. Ово је у складу са налазима Јохансена и сар. који наводе да је величина организационог система главни предиктор постојања формализованих процедура кризног менаџмента и комуникације (Johansen et al. 2011). Постоје разлике у „власништву“ над процесом кризног менаџмента, велика већина испитаника одговорила је да је директно одговорна управа компаније, док су два испитаника истакла да је кризни менаџмент у надлежности корпоративне безбедности или његових еквивалената. Питања о структури и начину функционисања кризних тимова, „окидачима“ за активирање кризног одговора и другим активностима током кризе нису ушла у опсег овог истраживања.

Будући да је кризно комуницирање, за разлику од комуницирања ризика, формализован комуникациони процес, праксе планирања кризног одговора и кризног комуницирања укључили смо као један од два индикатора тврдог аспект ресорптивног капацитета. Према Старџису (Sturges 1994), кризна комуникација препознаје три врсте информација које имају различите функције: инструктивне информације, којима се људи упућују у то како да се понашају и

реагују у смислу сопствене заштите; прилагођавајуће информације, које помажу људима да се боре са неизвесношћу; и интернализирајуће информације, којима организација настоји да очува своју репутацију. Иако су истраживачки напори до сада махом били усмерени на очување репутације (Holladay 2010), за тему овог истраживања прве две функције су важније. У свакој од четири фазе управљања ванредним ситуацијама или кризама (тј. митигацији, припреми, одговору и опоравку) комуникација има различите циљеве и примењују се различите стратегије. Фазе митигације и припреме се у великој мери преклапају са комуникацијом ризика, јер су усмерене на едукацију и информисање прималаца о потенцијалним ризицима и ванредним догађајима. Комуникација у фазама митигације и припреме утиче на јачање антиципативног капацитета отпорности организације. Према Кумбсу и Холадају, комуницирање током одговора обезбеђује кључне информације које јавност може искористити за предузмање акције у циљу спасавања и преживљавања у случају непогоде или несреће, док је у фази опоравка нагласак на информисању јавности о типовима помоћи намењене за опоравак погођених подручја. Циљ ове комуникације јесте навођење појединаца и заједница на предузимање акције (Coombs & Holladay, 2010: 59).

Код кризне комуникације са интерним запосленима већина испитаника се слаже да је потребно уважити повратну информацију и на њеној основи формирати и адаптирати одговор. Такође, поједини испитаници су навели да је за формулисање прецизних упутстава и препорука од кључне важности била двосмерна комуникација са експертским установама и другим екстерним институцијама. Сектор за корпоративну безбедност најчешће служи за прикупљање података са терена, њихову анализу и информисање тимова за кризно управљање који су потом формулисали наредбе, упутства и препоруке запосленима. Та пракса била је присутна и за време пандемије COVID-19 током које су запослени у сектору корпоративне безбедности свакодневно комуницирали са повереницима цивилне заштите, а затим извештавали тим за кризно управљање и надлежне државне службе. Информације које су тимови за кризно управљање слали својим запосленима током пандемије COVID-19 биле су инструктивне (налози, наредбе, упутства и препоруке) и прилагођавајуће (у складу са информацијама добијеним од екстерних експертских установа). Налази из нашег истраживања поклапају се са резултатима квантитативне студије Јохансена и сар. о праксама интерног кризног комуницирања у Данској (Johansen et al. 2011).

Лидерство посебно долази до изражаја у току фазе одговора на реметилачки догађај узрокован нерутинским ризиком, а која, уопштено говорећи, кореспондира са ресорпционим капацитетом отпорности. Овај аспект идентификован је у складу са Гринтовом тезом да је у сусрету са новим проблемима и ситуацијама, то јест нерутинским ризицима и неизвесностима, када нема познатих одговора или процедуралног приоритета потребно је лидерство. (Гринт 2005) Гринт лидерство посматра као супротност принципу војне команде (command and control) при којем се управљање спроводи путем исказивања и извршавања наредби. Командовању се може дати предност приликом суочавања са рутинским ризицима, за чије третирање постоје конкретни планови и процедуре. Услед инхерентних ограничења приступа „војне команде“ (command and control) у кризном одговору лидерска понашања и развој нових норми су од кључног значаја за адресирање захтева организације. (Schneider 1992; Wenger 1992; Auf der Heide 1989) Актуализације нерутинских ризика представљају амбивалентне подстицаје који захтевају сарадњу и постављање правих питања како би помогли организацијама да схвате и управљају непознатом новонасталом ситуацијом.

Лидери помажу другим члановима тима у разумевању и осмишљавању обиља информација у току кризе (Christianson et al 2009) и доприносе стабилности упркос потенцијалу

за хаос (Schneider 1992). Како Вилијамсон и сар. истичу, способност функционисања након значајног поремећаја зависи од когнитивних и бихејвиоралних одговора организације, а које је такође контекстуално одређено (Williams et al. 2017, 747). Когнитивни одговор на поремећај укључује способност актера да примети, тумачи и анализира промене у окружењу и да формулише одговоре (Dewald & Bowen 2010). Међу карактеристике отпорности Гибсон и Тарант (Gibson & Tarrant 2010) укључују толеранцију вишесмислености која се односи на начин на који појединац или група перципира и процесуира информације о нејасним ситуацијама или стимулусима, суочен са низом непознатих, комплексних или неусклађених трагова (Furnham & Ribchester 1995, 179). Бројне студије из научних дисциплина психологије (White & Shullman 2010) и организационих наука (Furnham & Ribchester 1993, 2015; O'Connor et al. 2021; Sung et al. 2017.) показале су да је толеранција вишесмислености лидера од кључног значаја за стимулисање креативног одговора на организационе изазове, укључујући и кризне ситуације. Дакле, толеранција вишесмислености представља пожељно когнитивно својство лидера које резултира когнитивним одговорима придавања смисла или осмишљавања и изоштравања. Толеранција вишесмислености, даље, утиче на креативан и флексибилан бихејвиорални одговор.

Толеранција вишесмислености није у овом истраживању непосредно испитивана, већ посредно кроз индикаторе осмишљавања/изоштравања и креативности/флексибилности одговора.

Осмишљавање подразумева препознавање промена и потенцијалних ремећења и њихово правилно тумачење (Burnard and Bhamra 2011; Weick 1993; Weick & Sutcliffe 2007; Whiteman & Cooper 2011). Осмишљавање претходи решавању проблема или деловању (Weick 1993), и од суштинског је значаја за избегавање грешака (Chan 2011). Осмишљавање даје објашњење како новонастала ситуација, неочекивани догађај или промене у окружењу могу утицати на циљеве и успех организације (Hamel and Välikangas 2003; Weick & Sutcliffe 2007; Whiteman & Cooper 2011). Узимајући у обзир природу нерутинских ризика, о којима може бити мало информација, односно непостојећег личног и организационог искуства, а последице могу бити изузетно високе, лидери помажу другим члановима тима у разумевању и осмишљавању обиља информација (Christianson et al 2009) и доприносе стабилности упркос потенцијалу за хаос (Schneider 1992).)

Сличан концепт осмишљавању, како наводе Гибсон и Тарант у свом моделу „рибље кости" је и изоштреност (acuity), односно осетљивост на промене. Висок ниво изоштрености (разумевање прошлости, надзор над садашњошћу и предосећање будућности) омогућава препознавање индикатора који могу довести до драматичних промена (Gibson & Tarrant 2007).

У условима манифестације нерутинских ризика доносиоци одлука налазе се пред бројним изазовима. Они често не могу да процесуирају опсег и број информација потребних за доношење правовремене одлуке неопходне за адекватан одговор и координацију између бројних компоненти система. Што су доносиоци одлука у бољој позицији да разумеју садржај и трајање поремећаја, затим начине на који промене индуковане поремећајем утичу на шире окружење, и напокон које структуралне, процедуралне или друге организационе промене треба предузети, вероватније је да ће систем одржати позитивно функционисање у новом окружењу (Lengnick-Hall & Beck 2005).

Како би се избегла непрецизност у истраживању осмишљавању и изоштрености, а и будући свесни ефекта хеуристике доступности, ови индикатори су у интервјуима анализирани кроз одговор на конкретна питања о почетку кризе COVID-19:

1. Да ли се пандемија налазила у регистру ризика и да ли је по вашем мишљењу организација била приправна за одговор?

2. „У ком тренутку је било јасно да ће COVID-19 прерасти у пандемију и имати велики утицај на пословање“

У нашем истраживању већина испитаника (n=8) је имала пандемију/ешидемију у регистру ризика, док пет испитаника није (n=5). У оним системима у којима пандемија није била присутна у регистру ризика лидери су се ослањали на, препознавање индикатора и интерпретирање сигнала поремећаја у окружењу. Код оних оператора критичне инфраструктуре који су имали пандемију у регистру ризика, или су имали искуство са вирусом H1N1 („свињски грип“) на самом почетку пандемије су препознате сличности са претходним ситуацијама и са анализираним ризиком из регистра те су планови и процедуре активирани и адаптирани за конкретну претњу. Индикативно је да су сви испитаници који нису имали пандемију у регистру ризика, надолазећу прењу COVID-19 идентификовали прилично касно, након бележења случајева у Европи и након успостављања ванредног стања. Осмишљавање и изоштравање пандемије као наступајућег поремећаја са високим последицама регистровано је раније у системима код којих је фигурирала у регистру ризика, мада су тек два од осам испитаника истакли да је пандемија праћена као могућа претња од ширења вируса у Кини. Ово је у складу са налазима малобројних емпиријских студија чији налази указују на тешкоће у осмишљавању актуализације нерутинских ризика у организационим системима. Тако, Кањиле и Клует, говоре о тешкоћама доносиоца одлука да препознају сигнале, па чак и о занемаривању јасних сигнала, који су указивали на предстојеће терористичке нападе (Khanyile and Cluett 2017). Емпиријска студија Настецкиене која је анализирала осмишљавање оперативних ризика у свакодневним пословним рутинама вишег и средњег менаџмента дошла је до позитивнијих резултата (Nasteckiene 2021). Из налаза овог истраживања које је у складу са постојећом малобројном литературом можемо закључити да правовремено осмишљавање и изоштрености представља тежак задатак за доносиоце одлука за оне ризике који су остали ван регистра.

Након иницијалног разумевања и придавања смисла реметилачком догађају, доносиоци одлука се налазе у недоумици о активностима које је неопходно предузети, те настоје да генеришу лепезу могућих одговора (Williams et al. 2017, 747). Најефектнији бихејвиорални одговори су они који укључују иновативно и спонтано понашање, као и способност импровизације (Stacey 1995, 478; Shepherd & Williams 2014, 977). Слично томе, Рињо и Њустед истичу: „Непредвиђене, непознате и заиста нове кризе захтевају карактеристичан одговор руководства који често укључује флексибилност и прилагодљивост, брзо доношење добрих одлука и прикупљање ресурса у кратком року.“ (Riggio & Newstead 2023, 202)

У нашем истраживању испитаници су махом давали предност поступању према плановима и праћењу процедура, док се флексибилност и креативност у примени решења приликом криза прихвата као крајња нужност. Треба напоменути да су приликом одговора на питања испитаници углавном наводили примере из праксе који могу бити окарактерисани као рутински ризици. Налази овог истраживања у складу су са емпиријским истраживањима димензија организационе културе у Републици Србији, Хрватској и Босни и Херцеговине у којима је присутан висок степен избегавања неизвесности, а што се огледа у преференцији ка поступању по правилима (Vukonjanski et al. 2012; Nedeljkovic et al. 2018). Саговорници су наводили да је важно да планови кризног одговора буду општи јер се не могу предвидети све околности. Важност флексибилности планирања, те флексибилних и креативних истакнута је у одговорима на конкретан случај пандемије COVID-19, услед константног прилива нових информација које су утицале на одлуке највишег руководства, организацију рада и тимова, као и

на наредбе, упутства и препоруке саопштаване запосленима, а што је у складу са ставовима у консултованој литератури (Williams et al. 2017, Lengnick-Hall & Beck 2005, Shepherd & Williams 2014, Stacey 1995). Иако је реакција услед касног осмишљавања наступајуће ситуације углавном каснила, велика већина испитаника је наводила да није било већих дилема у пружању иницијалног одговора, нити озбиљнијих проблема у функционисању система а што може указати на висок степен креативности и флексибилности у пружању одговора, насупрот тенденцији ригидног планирања. Такође, ово је у складу са Клајновим моделом одлучивања препознавања прве прихватљиве одлуке (Recognition Primed Decision Making - RPDM) (Klein 1993), према којем доносилац одлуке прикупља могуће правце деловања, упоређује их с ограничењима која намеће ситуација и бира први правац деловања који, с обзиром на постојећа ограничења, није одбачен. (Kešetović i Toth 2011, 122) Како Кешетовић и Тот закључују, овај модел одлучивања добро функционише у условима временског притиска када се располаже делимичним информацијама, а циљеви нису јасно дефинисани. (Ibid) Ово је било очигледно нарочито почетком пандемијске кризе COVID-19 када доносиоци одлука и на државном, а нарочито на корпоративном нивоу нису располагали са довољно информација и када су упутства која су доспевала до њих често била опречна и нејасна.

2.3.3. Ресторативни капацитет

Постојање система менаџмента континуитетом пословања или еквивалентног система менаџмента главни је индикатор тврдог аспекта ресторативног капацитета отпорности организација. Како наводи Британски институт за континуитет пословања „континуитет пословања је кључна дисциплина за изградњу и унапређење организационе отпорности“. (BCI Statement on Organizational Resilience) Менаџмент континуитетом пословања усмерен је првенствено на ресорптивни (одговор на инцидент) и ресторативни капацитет организације, то јест на опоравак. Управљање континуитетом пословања након ремећења врши се спровођењем активности и процедура предвиђеним планом континуитета пословања. План континуитета пословања значајан је за постизање отпорности и првог (услед постојања процене ризика као саставног елемента плана), и другог реда, будући да је менаџмент континуитета пословања превасходно приступ усмерен на штићене вредности, без обзира на претње. За Фостера и Даја отпорност се може постићи кроз спровођење система менаџмента континуитетом пословања у смислу: 1) заштите запослених; 2) заштите кључног пословања предузећа (система, објеката, инфраструктуре и процеса); 3) заштите пословних мрежа (нпр. ланца снабдевања) (Foster & Dye 2005). Хербане такође уочава да сами менаџери, тј. доносиоци одлука сматрају да се организациона отпорност може унапредити кроз адекватан менаџмент кризама и континуитетом пословања (Herbane 2013), што је потврђено и овим истраживањем. Сви испитаници су одговорили да имају план континуитета пословања или интерне еквиваленте у складу са специфичним законским обавезама, будући да су често у питању објекти од посебног значаја за одбрану Републике Србије (Службени Гласник РС, бр. 112/2008) или еквиваленти објекти у суседним државама у складу са њиховим законским оквиром. Будући да су у питању сложени системи, планови постоје и на секторским нивоима. Ипак, само постојање система менаџмента континуитетом пословања није гаранција успешног опоравка, како показују новије студије. Наиме, у лонгитудиналној студији спроведеној у Уједињеном Краљевству, организације које су имале имплементиран систем менаџмента континуитетом пословања којима су руководили или координирали чланови Института за континуитет пословања (Business Continuity Institute - BCI) током прве године пандемије COVID-19 показале су нешто слабији опоравак од просека (Roberts 2022). Аутор поменуте студије не улази у разматрање закључака таквог понашања организација, међутим као могући разлог можемо навести превелико ослањање на планове континуитета пословања, што може довести до занемаривања „меких аспеката“ отпорности.

Карактеристике ресторативног капацитета, то јест оне карактеристике које се испољавају у фази опоравка су суочавање са стресом које је посматрано кроз индикатор одсуства некључних запослених са посла као и међуповезаност која је посматрана кроз питање о сарадњи са екстерним заинтересованим странама током пандемије COVID-19.

Као што смо поменули у теоријском оквиру истраживања, стратегије које се у менаџменту континуитета пословања препоручују усмерене су на континуитет рада путем обука и дообука, сменског рада, географске сепарације запослених са истим вештинама и обезбеђивање подршке екстерних страна („outsourcing“). Међутим, мање пажње се поклања ситуацијама када већи број „некључних“ запослених није спреман да се појави на радном месту током и након екстремних догађаја, не због физичке онемогућености (недостатка превоза, оштећења саобраћајница, повреда итд.) већ услед психолошких баријера (неповерење у организацију да ће им омогућити све предвиђене мере заштите, неадекватна комуникација ризика, неразумевање своје улоге у одговору на инцидент, неразумевање важности своје организације за безбедност и добробит заједнице и државе) (Riddle 2015). Нерутински ризици, нарочито они окарактерисани негативним атрибутима хазарда, попут непознате заразне болести, могу узроковати недолазак запослених услед бројних физичких препрека али и психолошких разлога. Одсуство већег броја „некључних“ запослених, свакако може утицати на опоравак функција оператора критичне инфраструктуре и њихових производа и услуга од кључног значаја за безбедност државе и добробит становништва.

Свих петнаест испитаника је изјавило да није било већих проблема у пословању њихових организација услед недоласка већег броја запослених на посао за време пандемије COVID-19 која је узета као студија случаја и због временске доступности података, лакоће евоцирања утисака, али и услед тога што се хазард пандемије непознатог вируса одликује високим негативним атрибутима. Ниједан испитаник није навео да је број запослених у било ком тренутку био испод минимума потребног за одржавање континуитета пословања. Истраживање се није директно бавило мотивацијом запослених за долазак, односно изостанак са посла, међутим, према речима испитаника поједини запослени су имали паничне нападе и страх, нарочито они који болују од хроничних обољења или који живе са старим и/или болесним особама.

Ови одговори нам указују на неколико фактора који су могли допринети овако позитивном исходу. Можемо претпоставити на основу претходних одговора испитаника да је налаз Ридлове да искрено и прецизно извештавање запослених о ризицима окарактерисаним негативним атрибутима хазарда, као што су непостојање личног искуства с ризиком и тешкоће у поимању изложености и будућих ефеката ризика, (конкретно, садашњи и будући ефекти вируса COVID-19), позитивно утиче на спремност запослених да дођу на посао. (Riddle 2015) Такође, узимајући у обзир Проширени модел паралелних процеса (ПМПП) можемо претпоставити да су запослени који су долазили на радно место у операторима критичне инфраструктуре током пандемије имали висок степен уверења о ефикасности одговора и перципираној самоефикасности, а што опет може бити плод конкретних решења за одговор на кризу, адекватних обука, лидерства и праксе комуникације ризика.

Према проширеном моделу паралелних процеса (ПМПП) четири фактора утичу на спремност за рад запослених током пандемије: перцепција озбиљности претње, перцепција личне подложности претњи, уочена ефикасност одговора и перципирана самоефикасност. Према неким ауторима (Barnet et al 2009; Balicer et al. 2010) поузданији предиктори одговора запослених су они који се односе на ефикасност одговора и самоефикасност. Што се тиче ефикасности одговора, оператори критичне инфраструктуре су се одлучивали да поред

обезбеђивања довољних количина заштитне опреме нарочито за запослене који су због природе пословних активности морали да имају контакт са клијентима и широм популацијом, организационих мера (нпр. правилника о одржавању дистанце) оним запосленима који су исказивали виши степен анксиозности омогуће рад на даљину колико год је то било могуће. Овакав одговор указује и на креативност и флексибилност, што је допринело осећању поверења према организацији.

Можемо претпоставити да је перципирана самоефикасност производ обука и едукација, као и двосмерне комуникације ризика и кризне комуникације која је забележена у претходним одговорима у анализи антиципаторног и ресорптивног капацитета. Такође, као фактори који утичу на сагласност запослених да се појаве на радном месту током актуализације нерутинских ризика одликованих високим степеном негативних атрибута хазарда, у литератури се помињу конфликт улога (најчешће у смислу недоласка на радно место услед личне перцепције запослених о својим улогама као родитеља, деце старих и/или болесних родитеља, старатеља итд.) (Killian, 1952), идеје о важности своје професионалне улоге у одговору на ризик (Di Giovanni et al. 2003), те идентификацији са организацијом (Lee 1971; Mael & Tetrick 1992; Riddle 2015). Напокон, треба истаћи да је суочавање са стресом изузетно комплексан појам, чији је само један од аспеката долазак запослених на радно место.

Гибсонов и Тарантов термин „међуповезаност“, који смо усвојили у овом истраживању односи се на успостављање односа поверења и реципроцитета са заинтересованим странама. Како Харисон и сарадници наводе, организације које управљају односима са заинтересованим странама имају потенцијал за развијање добрих односа са њима, то јест, односе поверења и реципроцитета (Harrison et al. 2010). Добар однос са заинтересованим странама охрабрује дељење визија, вредности, информација и материјалних ресурса, а што доприноси међузависности између организације и њеног ширег окружења. Лију и Ђин сматрају да међузависност доприноси бржем и флексибилнијем организационом одговору и опоравку (Liu & Jin 2020). По мишљењу већине испитаника сарадња са екстерним заинтересованим странама, пре свега хитним службама, ресорним министарствима и експертским тимовима у значајној мери је допринео бржем опоравку након иницијалног догађаја, тј. акутне фазе. У случају пандемије коронавируса, нарочито је истакнута сарадња са сектором здравства као фацилитатора и генератора брзог и ефикасног опоравка. Иако није експлицитно исказано, може се наслутити да је та сарадња позитивно утицала и на низак степен одсуства са посла, што је један од тврдих аспеката ресторативног капацитета отпорности. Оно што ниједан испитаник није поменуо јесте сарадња са организацијама из истог сектора критичне инфраструктуре. Остају отворена питања о томе да ли је у питању била сарадња са другим системима услед законских обавеза (сарадња са надлежним министарствима и чињеница да су у питању организације критичне инфраструктуре и, неке од њих, објекти од посебног значаја за одбрану), односно услед свести надлежних државних институција о значају оператора критичне инфраструктуре за безбедност земље, те сарадња из нужности са хитним службама, или је та сарадња заснована на проактивном управљању односима са заинтересовима странама.

2.3.4. Адаптивни капацитет

У литератури углавном постоји сагласност да је адаптација главно дистинктивно својство отпорности. Премда неки аутори истичу значај адаптације превасходно током фазе ресторације, мишљења смо да је адаптација значајна за све три темпоралне фазе кризе или реметилачког догађаја (пре-кризе „t-1“, током „t“, и након „t+1“), а који у мањој или већој мери одговарају антиципативном, ресорпционом и ресторативном капацитету. Наиме, флексибилно, односно

динамичко адаптивно планирање важно је у фази антиципације, док је креативан и флексибилан одговор неопходан у фази опоравка.

Нерутински ризици по својој дефиницији приморавају систем да функционише у нерутинском модусу, дакле системи се морају прилагодити новонасталој ситуацији будући да ће они утицати и на системе који га окружују и са којима имају односе зависности и/или међузависности. Тако, организациони системи морају привремено (t и/или t+1) или стално променити своју мисију, визију, дугорочне и краткорочне циљеве, начин функционисања, величину, организациону схему, број запослених, улоге запослених, измене у ланцу снабдевања и/или укључивање нових, емергентних технологија.

Адаптација обухвата прилагођавање ресурса, интерперсоналних процеса и организационих рутина у циљу третирања утицаја реметилачког догађаја (Danes et al. 2009; Glover 2012). Адаптацију такође неки аутори изједначавају са способношћу организационог учења (Brewin, Andrews & Valentine 2000; Bonanno, Westphal & Mancini 2011). Сумирајући налазе из литературе о адаптивном капацитету организације, а користећи Гибсонов и Тарантов аналитички модел „рибље кости“ као тврди аспект идентификовали смо динамичко адаптивно планирање (а које узима у обзир потребе прилагођавања ресурса, интерперсоналних процеса и организационих процеса), док је као меки аспект идентификована способност организационог учења. Према Галопину адаптивни капацитет система повезан је са капацитетом за одговор, а дефинисан је као способност система за еволуирање како би се прихватиле претње или промене из окружења, као и способност за проширивање опсега варијабилности (Galopin 2006). Варијабилност је битан појам у кибернетици и теорији система. Такозвани „Ешбијев закон“ гласи да што је већа разноликост акција доступних систему, то је већа разноликост пертурбација, које он може да прихвати (Ashby 1956). Динамичко планирање и учење утиче на повећање варијабилности и способности система за евалуирање. Организације које су усмерене на адаптивни капацитет нису пасивне према променама у окружењу, већ континуирано развијају и примењују нова знања у односу на њихово оперативно окружење. Самим тим, адаптивни капацитет организације боље помаже приправности за поремећаје и неизвесности (Bhamra et al. 2011, 21).

Литература о адаптивном капацитету отпорности организација најчешће анализира понашање организација као актера на тржишту. Међутим, специфичност организационих система оператора критичне инфраструктуре је у томе што се услед њихове кључне улоге, а често и монополистичког положаја на географској територији на коме пружају своје услуге и производе, код њих неће одвијати крупне промене у смислу измене мисије, визије и дугорочних циљева. На пример, аеродром, електроенергетска мрежа, или банка не могу трајно променити своју основну мисију нити делатност, а што може бити случај са неким другим, тржишно оријентисаним организационим системима (малим и средњим предузећима, холдинг компанијама итд.).

Динамичко адаптивно планирање је препознато као тврди аспект адаптационог капацитета организационе отпорности. Прихваћен је став аутора (Walker et al. 2019 ; Barasa et al. 2018; Pike, Dawley & Tomaney 2010) према којима су флексибилност политика, планова и процедура од највишег значаја за функционисање организације у суочавању са изазовима. Према Вокеру и сар. већина стратешких планова имплицитно претпоставља да се будућност може предвидети. Статички план се развија коришћењем једне будућности, често засноване на екстраполацији трендова, или се развија статички „робустан“ план који ће произвести прихватљиве резултате у малом скупу веродостојних будућих светова. Међутим, ако се покаже да је будућност другачија од претпостављене будућности, план би могао пропасти. Штавише, не

само да је будућност веома неизвесна, већ се и услови са којима се планери морају суочити мењају током времена (Walker et al. 2019).

Већина испитаника је одговорила да у њиховој организацији постоји имплицитна пракса динамичког адаптивног планирања, то јест да се планови кризног одговора и планови континуитета пословања развијају тако да буду флексибилни, са високим степеном општости, те самим тим примењиви на велики број могућих сценарија укључујући и непредвиђене догађаје, односно нерутинске ризике. Позитивно је истакнута и улога екстерних тела као што су државне институције, надлежна министарства, као и акредитациона тела за стандарде. Ови одговори су у складу са ставовима оних аутора (Walker et al. 2019; Barasa et al. 2018; Pike, Dawley & Tomaney 2010), према којима су флексибилност политика, планова и процедура од највишег значаја за функционисање организације у суочавању са изазовима. Испитаници су навели и да се контингентни планови у складу са искуствима са тимских вежби сценарија уважавајући повратну информацију учесника. Ипак, треба напоменути да динамичко адаптивно планирање треба да буде формализовано и Поједини испитаници су, пак, предност давали што прецизнијим плановима, истичући да би требало да се мењају у крајњој инстанци онда када се деси нешто непредвиђено, а што је негативно перципирано од стране тих испитаника.

Одговарајући на питања о адаптирању планова и процедура у току пандемије COVID-19 сви испитаници су се сложили да су се они константно адаптирали у складу са новим информацијама и упутствима добијеним од експертских установа и државних институција, али и уважавајући повратне информације добијене од запослених. Најчешће помињане одлуке односе се на стварање услова за рад на даљину, набавку средстава за заштиту запослених, промене начина организационих посета, те праћење стања заражених у организацији и окружењу.

Као карактеристику, то јест меки аспект адаптивног капацитета, идентификовали смо организационо учење. Према бројним ауторима претходна искуства са реметилачким догађајем повезана су са организационом отпорношћу (Brewin, Andrews & Valentine 2000; Bonanno, Westphal & Mancini 2011). Према Полу Мартину активна отпорност представља јачање система путем учења и извлачења поука из нежељених догађаја и унапређивање спремности на будуће поремећаје. (Martin 2019, 76). У интервјуима, испитаници су махом одговарали да су учили током кризе и да су приправни на могућу будућу пандемију. Врло индикативне су и изјаве да је међу наученим лекцијама и да се не могу сви ризици предвидети, што је позитивно у смислу јачања отпорности другог реда, у смислу спремности да се прихвати пракса динамичког адаптивног планирања и флексибилности и креативности у управљању. Из одговора се може закључити да се учење вршило на основу личних, организационих искустава, али и из искустава других организација у различитим географским оквирима. Један испитаник је одговорио да су његовој организацији у третирању ризика помогла претходна искуства са пандемијом H1N1, тзв. „свињским грипом“.

Ипак, према неким ауторима, организационо учење, односно способност учења из криза има своја ограничења. На пример, студија Бонана и сар. показала је да индивидуална отпорност на одређени догађај зависи од сличности тог догађаја са неким догађајем доживљеним у прошлости, али не са неким различитим типом догађаја (Bonanno et al. 2010). Отпорност, дакле, може бити олакшана искуственим „наученим лекцијама“, али постоји опасност да се научене лекције трансферирају на будуће догађаје линеарно или статички (Williams et al. 2017, 749). Из одговора видимо да код испитаника постоји тенденција линеарног трансфера, односно пресликавања искустава из пандемије COVID-19 на неке будуће догађаје (нпр. планирање набавке заштитних маски и течности за санитизацију).

3. Закључци и препоруке

Екстремни догађаји узроковани нерутинским ризицима попут природних катастрофа, терористичких напада, ратних дејстава и епидемија или пандемија могу узроковати озбиљне поремећаје у функционисању критичних инфраструктура на тлу Републике Србије и земљама у региону, а последично и озбиљне последице по безбедност и одбрану земље и добробит њених грађана. Како критичне инфраструктуре посматрамо као комплексни-адаптивни социо-технички систем, кључна компонента њихове отпорности припада организационој димензији, другим речима, шта и како њихови доносиоци одлука и запослени раде у циљу превазилажења поремећаја и опоравка након поремећаја.

У том циљу покушали смо да понудимо један иновативни начин моделирања организационе отпорности уваживши његове капацитете (антиципативни, ресорптивни, ресторативни и адаптивни) и аспекте (тврди и меки) који смо пилотирали у операторима критичне инфраструктуре на тлу Републике Србије, Републике Хрватске и Босне и Херцеговине. Организациону отпорност у овом истраживању посматрамо као стратегију управљања нерутинским ризицима и неизвесностима, насупрот традиционалном, антиципативном приступу управљања ризицима. Наша је претпоставка да се ова стратегија интуитивно и имплицитно примењује, за разлику од антиципативне стратегије засноване на формалним структурама, процедурама, буџетима и метрици.

Као студију случаја одабрали смо пандемију COVID-19 будући да је у питању типичан пример нерутинског ризика који се одликује ниском вероватноћом, великим последицама и приморава систем да функционише у нерутинском модусу. Такође, пандемијски ризик одликује висок степен негативних атрибута хазарда, што може негативно утицати на одговор на поремећај, нарочито у организационој димензији која је и била предмет истраживања.

Велики број студија третирао је елементе овог истраживања (перцепцију и комуникацију ризика заразне болести, управљање пандемијским кризама, кризно комуницирање са интерном публиком, обучености запослених, израда сценарија, приступ континуитета пословања, отпорност критичних инфраструктура организациона отпорност, организационо учење и култура, лидерство, суочавање са стресом). Међутим, до сада није било студија усмерених на интегрисање ових елемената и анализу специфичности отпорности организација идентификованих као оператера критичне инфраструктуре.

Примењујући аналитички модел на организације идентификоване као оператери критичне инфраструктуре у Републици Србији, Републици Хрватској и Босни и Херцеговини, стекли смо иницијални увид мишљења, ставове и претпоставке чланова кризних тимова и доносиоца одлука, као и у формалне и имплицитне пословне праксе и културу тих организација од значаја за елементе организационе отпорности које су ушле у опсег овог истраживања. Такође, стекли смо увид и у конкретне активности и карактеристике одговора примењених у операторима критичне инфраструктуре током пандемијске кризе COVID-19. Ови налази су примењени за разумевање и повремену критику академског оквира и концепата организационе отпорности. Резултати ове студије су такође примењени за развој низа практичних препорука за операторе критичних инфраструктура.

3.1. Преглед истраживања

Циљеви ове дисертације били су да:

- Понуди нову дефиницију организационе отпорности у циљу њене примењивости у студијама безбедности
- Понуди нови аналитички апарат за анализу организационе отпорности
- Идентификује претпоставке које доносиоци одлука имају о неизвесностима и нерутинским ризицима.
- Анализира праксе управљања ризиком у смислу фокуса на отпорност првог или другог реда.
- Анализира потенцијалне разлике у пажњи коју доносиоци одлука поклањају тврдим (активностима) и меким аспектима (карактеристикама) отпорности.
- Анализира антиципаторне, ресорптивне, ресторативне и адаптивне капацитете отпорности критичне инфраструктуре током пандемије COVID-19.
- Идентификује примере добре праксе у организацијама критичне инфраструктуре које буду учествовале у истраживању.
- Упореди резултате добијеним овим истраживањем са налазима истраживања спроведених у другим просторним и временским оквирима.

Ови циљеви су постигнути путем анализе 15 полуструктурисаних интервјуа са представницима оператора критичне инфраструктуре укљученим у планирање одговора на ризик, кризно планирање и планирање континуитета пословања. Један испитаник је начелник организације, два су техничка лица инжењерске струке која припадају високом руководству својих организација, док су тринаест испитаника припадала сектору корпоративне безбедности и њених еквивалената (једанаест руководиоци сектора, два припадника средњег менаџмента). Теоријски циљеви као и компарација резултата постигнути су секундардном анализом података, поређењем налаза из ове дисертације са резултатима сличних истраживања из других временских, просторних и организационих оквира.

У наставку овог последњег поглавља синтетизоваћемо емпиријске налазе са налазима из литературе из релевантних академских теорија представљених у првом поглављу како бисмо формирали свеукупне закључке.

3.2. Научни допринос истраживања

Сматрамо да смо у овом истраживању успели да постигнемо неколико доприноса развоју теорије организационе отпорности и њеном утемељавању у студијама безбедности:

1. Потврда адекватности појма „нерутинског ризика“ у анализи организационе отпорности.
2. Потврда адекватности концептуализације отпорности као стратегије управљања нерутинским ризицима и неизвесностима.
3. Интегрисање два модела анализе организационе отпорности – анализе капацитета и модела „рибље кости“.
4. Систематизација елемената организационе отпорности идентификованих у литератури, а затим и груписање по капацитетима и аспектима организационе отпорности.
5. Понуђена је нова концептуализација адаптације, као капацитета који прожима све фазе кризног одговора, а не као засебне фазе која следи фази опоравка.

Потврда адекватности појма „нерутинског ризика“ у анализи организационе отпорности извршена је анализом секундарне литература која третира сличне појмове као што су „екстремни догађај“, „екстремни ризик“, „неочекивана криза“ у којима смо наишли на

неконзистентности детаљније описане у теоријском делу дисертације, те поређењем са појмом „нерутинског ризика“. Нерутински ризик односи се на оне ризике који се одликују ниском вероватноћом а високим последицама, које приморавају систем да функционише у нерутинском моду и на које се не могу применити стандардне процедуре управљања ризиком. Самим тим, овај појам је плодан за примену у истраживањима отпорности, нарочито за укључивање у аналитички оквир истраживања отпорности другог реда, то јест отпорности на неизвесности.

Потврда адекватности концептуализације отпорности као стратегије управљања нерутинским ризицима и неизвесностима извршена је комбиновањем налаза из секундарне литературе и теренског истраживања спроведеног за потребе ове дисертације. Перспективу отпорности као стратегије увео је још осамдесетих година прошлог века Арон Вилдавски (Wildawsky 1987), међутим сразмерно мали број истраживања отпорност тематизује на овај начин. Сматрамо да је посматрање отпорности као стратегије управљања нерутинским ризицима веома користан угао гледања за истраживачке напоре у научним областима студије безбедности и различитим приступима менаџмента ризиком. Ова стратегија може бити експлицитно формулисана и формализована, али знатно чешће имплицитно и интуитивно имплементирана у организацијама.

Интегрисање два аналитичка модела организационе отпорности – анализе капацитета и модела „рибље кости“. Анализом ова два модела закључено је да би њихово интегрисање могло довести до унапређења академских и стручних напора у смислу прецизнијег и свеобухватнијег сагледавања капацитета и аспеката организационе отпорности. Овај модел омогућава анализу индикатора груписаних по капацитетима (антиципативни, ресорптивни, ресторативни, адаптивни) и аспектима, у смислу примењених активности организације („шта се ради?“) и карактеристика тих активности („како се то ради?“) у циљу оснаживања организационе отпорности првог (отпорности на познате претње и ризике) и другог реда (отпорности на нерутинске ризике и неизвесности).

У вези са претходним доприносом, понуђена је нова *систематизација индикатора организационе отпорности идентификованих у литератури, а затим и груписање по капацитетима и аспектима организационе отпорности* што ће убудуће омогућити њихово даље и дубље изучавање, рафинирање, поређење, оцењивање, приоритизацију, али и критику, будући да је ово тек први покушај примене интегративног модела са овим идентификованим елементима.

Понуђена је нова концептуализација адаптације, као капацитета који прожима све фазе кризног одговора, а не као засебне фазе која следи фази опоравка. У литератури о кризном менаџменту и континуитету пословања адаптација се често посматра као засебна темпорална фаза која следи након опоравка, а у којој се систем адаптира на новонастале околности. У теоријском делу и у дискусији показали смо да то није нужно закључак до којег смо дошли, будући да се адаптациони капацитет манифестује и током фаза припреме, одговора и опоравка, те самим тим утиче на и прожима антиципаторни, ресорптивни и ресторативни капацитет.

Емпиријски налази ове студије омогућили су допринос нашем разумевању ставова, мишљења, искустава и уверења чланова кризних тимова и доносиоца одлука о пословним праксама и елементима организационе културе од значаја за организациону отпорност, као и конкретних искустава о одговору на нерутински ризик индукован пандемијом COVID-19.

На најопштијем нивоу, узимајући у обзир сложеност појмова који су тематизовани у овом истраживању коришћена је литература која тематизује управљање ризицима, организациону отпорност и проблематику заштите и отпорности критичне инфраструктуре.

Појму ризика пришли смо консултујући широк спектар научних истраживања који тематизују перцепцију, комуникацију и менаџмент ризиком из различитих углова – когнитивне психологије, социологије, комуникологије, наука о безбедности и менаџмента. Фокус нам је био на досадашња истраживања која тематизују феномен нерутинских ризика и неизвесности, негативних атрибута хазарда, као и Проширени модел паралелних процеса који нам је био значајан за анализу теренских података. Литература консултована из ове области допринела је одабиру студије случаја пандемије COVID-19, затим формулисању питања и анализи одговора о управљању и комуникацији ризика, као и суочавања са стресом посредно анализирано путем одговора о одсуствовању са посла током пандемије.

Појам критичне инфраструктуре, као и заштите и отпорности критичне инфраструктуре, истраживан је кроз академска и стручна истраживања, али и кроз национална и наднационална легислативна и стратегијска документа. Литература из ове области послужила нам је да идентификујемо организације из којих смо контактирали потенцијалне учеснике интервјуа, као и да обезбедимо боље разумевање контекста у којима оператори критичне инфраструктуре послују.

Промишљању појма отпорности и организационе отпорности посветили смо највећи део теоријског оквира истраживања. Овај појам покушали смо да сагледамо путем различитих концептуализација – отпорности као жељеног стања система, отпорности као процеса и отпорности као стратегије. У овом поступку користили смо се академским радовима из разних научних области: социологије, екологије, психологије, теорије комплексних система, организационих наука, наука безбедности, кризног менаџмента и комуницирања и менаџмента континуитетом пословања. Такође су консултовани и релевантни међународни ISO стандарди (22301, 22306, 22316), британски стандарди (BSI) и стандарди америчке асоцијације за индустријску безбедност (ASIS). Консултована литература послужила нам је за формулисање аналитичког модела, идентификовање индикатора те формулисања питања и анализи одговора о индикаторима обука и едукације, сценарија одговора, слободних генеричких ресурса, лидерства, организационе културе и учења, као и праксе динамичког адаптивног планирања.

Консултовањем разнородне литературе о ризику, отпорности и критичној инфраструктури, дошли смо до аналитичког модела који смо применили на анализу организационе отпорности у оператерима критичне инфраструктуре у Републици Србији и земљама у окружењу (Република Хрватска и Босна и Херцеговина). Као што је напоменуто, аналитички модел представља интеграцију два постојећа модела – модела капацитета (Biringer et al, 2013; Keković et al. 2014) и модела „рибље кости“ (Gibson & Tarant 2010). У сваком капацитету одређени су индикатори тврдог (активности) и меког (карактеристике) аспекта:

1. Антиципаторни капацитет:
   - Тврди аспект: формализовани систем управљања ризиком, обуке и едукације, сценарија одговора на ризик, присуство слободних генеричких ресурса.
   - Меки аспект: партиципативни приступ планирању, комуникација ризика.
2. Ресорптивни капацитет:
   - Тврди аспект: формализовани систем кризног менаџмента и менаџмента ванредним ситуацијама, кризно комуницирање.

- Меки аспект: осмишљавање и изоштравање, креативност и флексибилност одговора.

3. Ресторативни капацитет:
   - Тврди аспект: систем менаџмента континуитетом пословања.
   - Меки аспект: суочавање са стресом, међуповезаност.
4. Адаптивни капацитет:
   - Тврди аспект: динамичко адаптивно планирање.
   - Меки аспект: организационо учење.

Налази овог истраживања потврдили су основну хипотезу истраживања да је стратегија отпорности имплицитно препозната као стратегија избора управљања нерутинским ризицима и неизвесностима у организационим системима оператера критичне инфраструктуре. Две од три посебне хипотезе су такође потврђене

1. X1 - Усмереност планирања одговора у операторима критичне инфраструктуре је на рутинским ризицима на које се примењује стратегија антиципације и
2. X3 - Напори доносиоца одлука и надлежних организационих јединица су равномерно усмерени на јачање сва четири капацитета отпорности

Друга хипотеза X2 - За нерутинске ризике и неизвесности имплицитно се примењује стратегија отпорности кроз примену неформалних пословних пракси усмерених на на меки аспект отпорности – је делимично потврђена, будући да се из одговора испитаника није могло доћи до јасног закључка.

Резултати овог истраживања довели су до бољег разумевања организационих пракси које се предузимају у фазама припреме, одговора и опоравка од кризе, укључујући и адаптивне процесе. Такође, применом полуструктурисаног интервјуа стекли смо дубинске увиде у ставове и мишљења испитаника укључених у ове процесе. Дубинском анализом одговора и њиховом кодификацијом у теме и подтеме овог истраживања дошли смо до следећих закључака:

1. Национални законски и стратегијски документи, директиве Европске уније, те захтеви стандарда, директно утичу на унапређивање отпорности првог реда (отпорности на познате ризике) у операторима критичне инфраструктуре. Закони и подзаконски акти наведени у теоријском делу, као и директиве Европске Уније и Европске Комисије, те међународни (ISO) стандарди прописују активности (тврди аспект) које се морају или које је потребно извршити у циљу управљања ризицима, ванредним ситуацијама, кризама и континуитетом пословања. Стандарди, такође, предлажу добру праксу усмерену на обуке и едукацију запослених, као и комуникацију током инцидената. Одговори испитаника указују на присуство свести о важности примене стандарда, као и поступања у складу са легислативним актима и стратегијским документима који регулишу ову област.
2. Располагање слободним генеричким ресурсима је у колизији са LEAN приступом менаџменту који је нарочито присутан у приватном сектору. Из одговора испитаника из оператера критичне инфраструктуре можемо донекле закључити да постоји одређена редундантност у погледу људских и материјалних ресурса која се може искористити у случајевима већих поремећаја и продужених криза. Ипак, концепт слободних генеричких ресурса је недовољно познат и разумљив већини испитаника, будући да се не односи искључиво на опипљиве ресурсе, већ и на когнитивне ресурсе у организацијама о којима они, узимајући у обзир њихове позиције у организацији, не морају имати довољно знања. Даља истраживања разумевања концепта слободних генеричких ресурса у операторима

критичне инфраструктуре, њиховог присуства и одсуства, као и односа са организацијама које се ослањају на праксу LEAN менаџмента би могла дати потпунији одговор на ову проблематику.

3. Активност, то јест тврди аспект организационе отпорности који може бити додатно регулисан стандардима је уграђивање приступа или појединих елемената динамичког адаптивног планирања (ДАП) у планове управљања ризицима, кризне планове и планове континуитета пословања. Приступ ДАП се до сада експлицитно примењивао за стратешко планирање, док је његово присуство на нивоу менаџмента ризиком, кризама и континуитетом пословања ограничена. Сматрамо да би укључивање принципа ДАП у ове планове допринело оснаживању организационе отпорности другог реда, то јест отпорности на нерутинске ризике и неизвесности. Из одговора испитаника закључујемо да постоје уверења да планови требају бити флексибилни и отворени како би се прилагодили развоју догађаја или се адаптирали на нову и неочекивану претњу. Формализација приступа ДАП би дакле превела у формалну пословну праксу ових, правилних уверења и ставова.
4. Отпорност другог реда, то јест отпорност на нерутинске ризике и неизвесности имплицитно је препозната и примењена кроз неформалне и неписане корпоративне праксе које се односе на сегменте организационе културе као што су партиципативни приступ у планирању и комуницирању ризика и криза, креативан и флексибилан одговор, лидерски капацитети за осмишљавање и изоштравање, међуповезаност са екстерним заинтересованим странама као и склоност организационом учењу.
5. Оператери критичне инфраструктуре у Републици Србији и региону примењују партиципативни приступ у управљању и комуникацији ризика, што је позитивно оцењено по антиципативни капацитет – у смислу добијања различитих перспектива за идентификовање ризика и планирање одговора на ризик, те јачања спремности запослених, а такође посредно по ресорптивни капацитет – унапређивања могућности раног осмишљавања и изоштравања новонастале ситуације, те ресторативни капацитет – унапређивање суочавања са стресом и односа међуповезаности са екстерним заинтересованим странама.
6. Осмишљавање (sensemaking) и изоштреност су термини који се односе на рано препознавање и придавање смисла реметилачким догађајима. Постојање ризика у регистру може позитивно утицати на правовремено осмишљавање реметилачког догађаја индукованог нерутинским ризиком. Овај закључак произлази из поређења одговора испитаника који су имали пандемију у регистру ризика чије организације су у већем броју случајева раније препознале надолазећу претњу у односу на испитанике чије организације то нису имале. Такође, испитаници који су имали искуства са претходном пандемијском кризом „свињског грипа“ H1N1 истакли су да су пандемију COVID-19 дочекали спремно. Ови налази су засновани на малом узорку тако да препоручујемо даља истраживања у овом смеру.
7. Код већине испитаника постоји тенденција ка ослањању на планове и процедуре, док се импровизовање и креативност посматра негативно, као крајња инстанца. Ово је у складу са димензијом „избегавања неизвесности“ проминентној у националним организационим културама у Републици Србији и региону, а која се одликује ослањањем на норме, правила и процедуре у суочавању са неизвесностима (Hofstede 1980; Vukonjanski et al. 2012.)
8. Суочавање са стресом запослених током криза дугог трајања, а индукованим нерутинским ризиком са високим степеном негативних атрибута хазарда, које смо испитивали путем питања усмерених на одсуство некључних запослених током

пандемије COVID-19 у складу је са налазима докторске дисертације Ридлове (Riddle 2015) која је Проширени модел паралелних процеса применила на хипотетички терористички напад биолошким оружјем, а према којима су фактори перцепције ефективног одговора организације и самопоуздања у лични одговор од кључног значаја за долазак некључних запослених на посао током кризе. Наиме, из одговора свих испитаника закључено је да су оператери критичне инфраструктуре пажњу полагали на обуке, едукације и информисање запослених што је могло допринети перцепцији личне способности за одговор. С друге стране, сарадња са експертским институцијама и хитним службама, те приоритизација ових организација од кључног државног значаја у набавци заштитне и санитетске опреме, те усмереност на креативан одговор у смисли омогућавања рада на даљину и сменског рада, могли су допринети уверењу запослених у ефикасан одговор организације. Други налаз Ридлове, о идентификацији запослених са организацијом као предиктором позитивног одговора у кризама индукованих нерутинским ризицима, те њиховом перцепцијом о важности своје улоге и важности организације за ширу заједницу није био предмет нашег истраживања.

9. Међуповезаност, то јест степен сарадње са екстерним заинтересованим странама у планирању и спровођењу одговора на кризу и у процесу опоравка је превасходно заснован на законским обавезама (сарадња са надлежним институцијама) и нужностима који проистичу из природе претње (у случају COVID-19 сарадња са хитним службама и експертским институцијама – нпр. Републички завод за јавно здравље). Анализом одговора испитаника нисмо могли доћи до закључка да ли постоји и на ком нивоу је сарадња са другим операторима критичне инфраструктуре у смислу размене информација, ресурса и пружања помоћи у процесу опоравка.
10. Организационо учење које је идентификовано као меки аспект адаптационог капацитета присутно је у одговорима свих испитаника на питање о наученим лекцијама из пандемије COVID-19. Међутим, на основу одговора већине испитаника, чини се да постоји усмереност на статичко учење, то јест тенденција да се искуства из пандемијске кризе линеарно трансферирају на неки будући догађај.

Свакако, свесни методолошких ограничења ове пилот студије, у смислу методологије (налази су искључиво засновани на интервјуима са особама укљученим у кризни одговор који не морају имати нужно довољно знања за одговор на сва наведена питања, ограничен број интервјуа), али и теорије (истраживачи могу пречистити постојеће и додавати нове индикаторе у свим капацитетима и аспектима) препоручујемо даља истраживања која би потврдила ове закључке.

3.3. Практични допринос - Кључне препоруке за организације

У овом делу закључка изнећемо препоруке за операторе критичне инфраструктуре али и друге организационе системе у циљу унапређења њихове организационе отпорности првог и реда. Препоруке су засноване на резултатима ове дисертације, примарних података добијеним путем интервјуа са петнаест представника оператера критичних инфраструктура, њиховом анализом и кодификацијом, те њиховим поређењем са налазима других академских истраживања. Препоруке су груписане по капацитетима организационе отпорности – антиципативном, ресорптивном, ресторативном и адаптационом.

Антиципативни капацитет

Препорука 1 – Планирање одговора за различите врсте нерутинских ризика може унапредити отпорност организације уколико се они реализују. Иако се одликују ниском вероватноћом, нерутински ризици попут пандемије, терористичког напада или природних катастрофа могу проузроковати значајне губитке људских живота, као и поремећаје пословања услед компликоване природе опоравка. Треба такође узети у обзир да нису сви ризици исти, те да врста ризика утиче и на понашање запослених. Ризици окарактерисани високим нивоом негативних атрибута хазарда, као што су епидемија непознатог вируса, те напади и акциденти који укључују отпуштање биолошких, хемијских и нуклеарних агенаса, могу довести до повишеног стреса међу доносиоцима одлука и запослених, што отежава одговор и опоравак организације. Напокон, планирање одговора за нерутинске ризике може допринети бољем осмишљавању и бољој изоштрености, те развијању креативних одговора.

Препорука 2 – Улагање у слободне генеричке ресурсе у нормалним, рутинским околностима исплати се у случају манифестације нерутинских ризика. Слободне генеричке ресурсе не треба схватати искључиво као материјалне редундантности. Како Вилдавски наводи „респонзивни системи су способни за конвертовање доступних генеричких ресурса, као што је богатство, знање и техничке вештине у прикладна решења ако му и када буду потребна“. (Wildavsky 1989, 71) Осим функционалне редундантности у критичним системима, те додатних финансијских средстава, значајан је и тзв. „концептуални вишак“, односно знања и вештине које нису директно везане за обављање радних задатака. Концептуални вишак унапређује могућност идентификовања претњи и сагледавања проблема из различитих перспектива и преиспитује наслеђено организационо знање (Sutcliffe & Vogus 2003, 105). Овај појам је корисно имати на уму приликом запошљавања, састављања тимова и едукације запослених.

Ресорптивни капацитет

Препорука 1 – Стимулисати креативност и импровизацију у одговорима. Из искуства са пандемијом COVID-19 уочено је да су најефектнији одговори били они који су подразумевали креативност, флексибилност и импровизацију, те да су се планови и процедуре константно прилагођавали на нове околности. Под креативношћу подразумевамо изналажење нових начина за решавање проблема брзином која прати његову променљивост. Неопходност креативног и флексибилног одговора једна је од карактеристика одговора на нерутински ризик. Према Гибсону и Таранту „организација треба да пружи довољно простора за креативност и флексибилност и на управљачком и на оперативном нивоу, како би се омогућило организација да ради на нове, иновативне начине, а што је неопходно у нерутинским условима.“ (Gibson & Tarrant 2010) Стимулисање креативности и флексибилности може се унапредити кроз увежбавање сценарија где се може охрабривати давање алтернативних решења од стране учесника, као и кроз обуке у којима ће се од учесника често захтевати коментари и повратне информације. Такође, отворена дискусија о алтернативним начинима спровођења процедура за третирање рутинских ризика приликом њихових ревизија и ажурирања може бити плодотворна.

Ресторативни капацитет

Препорука 1 – Укључити сценарио одсуства великог броја некључних запослених у план континуитета пословања. Одговор запослених може зависити од типа ризика, то јест од негативних атрибута хазарда. Запослени не само што могу бити физички онемогућени да се појаве на радном месту, услед болести (своје или својих најближих) или оштећења инфраструктуре, већ одређени ризици као што су пандемије, већи хемијски, нуклеарни или биолошки инциденти и терористички напади могу узроковати анксиозност и стрес. У студији

Ридлове, 41% запослених је изјавило да би физички могли да иду на посао током инцидента који би укључио намерно отпуштање вируса малих богиња, само 29% је потврдило да би било спремно да на посао и оде. (Riddle 2015, 241). Слични налази су добијени и у студији из САД у којој су запослени у хитним службама (здравствени радници, полиција и ватрогасци) у великој већини (80%) изјавили да би физички могли да оду на посао током пандемије непознатог вируса, док је 65% изјавило да би било спремно за то. (Gershon et al. 2010) Услед тога, организација би требало да укључи у планирање чињеницу да након нерутинског инцидента са високим степеном негативних атрибута хазарда запослени могу развити функционално нарушавајуће симптоме психичког здравља, а који их могу спречити да се појаве на радном месту.

Адаптивни капацитет

Препорука 1 – У планове управљања нерутинским ризицима укључити принципе Динамичког адаптивног планирања (ДАП). Приступ се заснива на спецификацији скупа циљева и ограничења, изради иницијалног плана који се састоји од краткорочних активности, као и успостављања оквира за будуће (контингентне) активности. Овакав план se експлицитно израђује у циљу адаптације на измењене околности. (Walker et al. 2019, 53) ДАП се изводи у две фазе: прва, у којој се даје нацрт плана, програма за мониторинг и различитих активности пре и после имплементације, те друга фаза имплементације у којој се спроводе плана и програм мониторинга те преузимају корективне акције у случају нежељених догађаја. (Walker et al. 2019, 53) Овакви планови су до сада били израђивани на стратегијском нивоу великих система и државних управа, међутим, сматрамо да би и поједностављене варијенте биле корисне за планирање одговора на нерутинске ризике. На пример, планови би могли да предвиде систем за праћење и надзор окружења у виду идентификације догађаја окидача који би онда довели до преиспитивања и ажурирања планова и препорученог одговора.

Препорука 2 – Обратити пажњу да научене лекције не буду преуско формулисане јер је вероватно да наредна криза неће бити једнака протеклој. Свакако, конкретне активности, добра и лоша пракса уочена током кризе, треба да буду документоване у виду научених лекција. Оно што такође треба имати на уму јесте да је свака криза, а нарочито она индукована нерутинским ризиком засебна, тако да је опасност уколико се из криза учи линеарно, то јест уколико постоји очекивање да ће бити могуће извршити линеарни трансфер научених лекција у неком наредном догађају (Williams et al. 2017, 749). Студија Бонана и сар. показала је да индивидуална отпорност на одређени догађаја зависи од сличности тог догађаја са неким догађајем доживљеним у прошлости, али не са неким различитим типом догађаја (Bonanno et al. 2010). Отпорност, дакле, може бити олакшана искуственим „наученим лекцијама“. Ипак, то учење није линеарно нити статичко. Друга потенцијална претња је учење из искуства других организација, нарочито уколико оне не припадају истом секторском, географском или временском оквиру. МекДоналд и Вестфал примећују негативне последице учења од других организација које су имале слична искуства, јер повратна информација може довести до погрешног тумачења сигнала о неповољним условима у окружењу што даље може довести до организационе кризе (McDonald & Westphal 2003) Исте препоруке важе и за адаптацију путем научених лекција током фаза одговора и опоравка.

3.4. Ограничења истраживања

У писању ове дисертације наишли смо на бројне отежавајуће факторе који су утицали на ограничења истраживања, како концептуална, тако и методолошка.

Управљање отпорношћу организација, то јест управљање нерутинским ризицима и неизвесностима у комплексним адаптивним системима представља тзв. „wicked problem“, тешко решив и комплексан проблем који је могуће сагледати из бројних перспектива, али је извлачење дефинитивних и општеважећих закључака и препорука готово немогућ задатак. Проблем отпорности предмет је вишедеценијских промишљања и дебата истраживача из различитих наука и научних дисциплина – медицине, психологије, социологије, инжењерских и организационих наука, менаџмента (стратешког, ризика, криза, природних катастрофа). Услед тога, ми смо овом концепту покушали да приђемо проблемски, уваживши различите научне перспективе и настојећи да их учинимо корисним за науке безбедности и практично примењивим за менаџере корпоративне безбедности и чланове кризних тимова оператера критичних инфрастурктура. Свакако, није било могуће уважити и емпиријски применити сваку теорију, перспективу и аналитички модел у огромном и непрестано нарастајућем корпусу истраживања које тематизују отпорност организација и менаџмент ризиком и неизвесностима.

Истраживање је ограничено на организациону димензију отпорности организација. Самим тим, изостављене су инфраструктура, техничка, економска и социјетална димензија, будући да су та питања, иако од изузетног значаја за организације, од индиректног значаја за корпоративни безбедносни менаџмент.

Предложени аналитички модел је дизајниран за потребе овог истраживања, дакле није био раније примењен. За понуђени интегрисани модел капацитета и аспеката отпорности било је потребно одабрати елементе - индикаторе који би били довољно свеобухватни, а опет довољно конкретни да би се могла извршити њихова дубинска анализа. Такође, индикатори су морали бити сведени на број за који је квалитативно истраживање могло бити организовано. Пошто је, како је већ наведено, организациона отпорност врло комплексан концепт, узимајући у обзир ограничења ресурса и времена за теренско истраживање, број анализираних индикатора је одабран тако да обезбеди довољну ширину како би се покрили сви капацитети и аспекти, али и довољну дубину да би се из примарних података могли извести закључци и препоруке.

Приликом теренског дела истраживања наишли смо на ограничења организационе природе. Прво, велики број потенцијалних испитаника (n=32), представника оператера критичне инфраструктуре у Републици Србији, одбио је или није одговорио на захтев за учешћем у истраживању. Као разлози су најчешће навођени осетљивост података, неповерење према сврси истраживања и немогућност учешћа у истраживању услед чињенице да су у питању објекти од посебног значаја за одбрану. Услед тога, контактирани су оператери критичне инфраструктуре из Републике Хрватске и Босне и Херцеговине. Сматрамо да је њихово укључивање оправдано будући да су у питању земље које су на упоредивом нивоу развоја концепта заштите и критичне инфраструктуре и његовом преношењу у законске и стратегијске оквире, односу оператера критичне инфраструктуре у јавном и приватном власништву, као и националним карактеристикама организационе културе – конкретно димензије избегавања неизвесности која је била од значаја за наше истраживање. Ипак, узорак је релативно мали (n=15) будући да је највећи број испитаника пристао на истраживање узорковањем „грудве снега“ – коришћењем личних и професионалних контаката.

Следеће ограничење односи се на начин интервјуисања. Шест интервјуа је спроведено писаним путем, коришћењем електронске поште. На нека питања добијали смо веома ограничене одговоре, а након поновљених питања нисмо успели да добијемо повратну информацију. Такође, два интервјуа – један спроведен физички, и један путем апликације за конференцијски позив „Zoom“ имали су веома ограничено време трајања због пословних

обавеза испитаника, тако да су нека питања морала бити изостављена, а на нека су добијени недовољно детаљни одговори.

Након сваког интервјуа, секвенцијалном анализом података, редефинисала су се стара и отварала нова питања која није било могуће уврстити у одобрени водич за интервју, те су формулисана као потпитања када су интервјуи спровођени уживо или путем рачунарских апликација. Каснији интервјуи су били усмеренији на поједина питања, што значи да нека питања нису била постављена испитаницима који су интервјуисани на самом почетку теренског дела истраживања.

Напокон, детаљнији увиди о појединим испитиваним индикаторима добили би се коришћењем мултиметодског приступа – анализе примарних података (интерних планова и процедура оператера критичне инфраструктуре који се односе на управљање ризицима, кризама и континуитетом пословања) као и анкетирања запослених о степену њихове укључености у планирање одговора и степену обучености, перцепцији ризика и ефикасности одговора, као и о корпоративним праксама комуницирања ризика и криза. Такође, организовање фокус група за представнике вишег менаџмента оператера критичних инфраструктура би било корисно за добијање даљих дубинских увида о њиховим ставовима и мишљењима, као и о пословним праксама усмерених на управљање нерутинским ризицима стратегијом отпорности. Из организационих и техничких разлога ове технике прикупљања података није било могуће организовати за потребе овог истраживања.

3.5. Препоруке за даље истраживање

Будући да је сврха овог истраживања била да осмисли и пилотира нови аналитички модел за анализу организационе отпорности, неопходна су даља и дубља концептуална и емпиријска истраживања. Такође, дајемо препоруке и како се може унапредити методолошки приступ.

У аналитички модел укључили смо одређен број елемената-индикатора идентификован у литератури који указују на капацитет и аспект отпорности организације. Бројни други елементи организационе отпорности постоје у досадашњим истраживањима, тако да се предлаже њихова анализа подобности за укључивање у модел, као и евалуација постојећих индикатора. Такође, како се капацитети отпорности у појединим фазама кризног одговора могу преклапати, предлажемо анализу постојећих индикатора у смислу њихове подобности за анализу капацитета предвиђеног овим пилот истраживањем, те њихово измештање у други капацитет (нпр. креативност и флексибилност могу се аргументовано посматрати као елементи антиципативног или ресторативног капацитета, међуповезаност је такође битна за антиципативни капацитет и укључивање екстерних заинтересованих страна у процес планирања, као и за могућност организационог учења из искуства других система).

Потребно је емпиријско истраживање које би обухватило већи број испитаника у форми фокус група или онлајн анкете како би се темељније утврдили налази овог истраживања. Таквим истраживањем могле би се утврдити разлике у организационој отпорности између различитих сектора критичне инфраструктуре, као и између оператера критичне инфраструктуре у јавном и приватном власништву, а што би могло бити корисно за законодавце. Такође, поређење резултата добијених у овом истраживању са организацијама које не припадају критичним инфраструктурама могло би довести до изналажења специфичних елемената отпорности својственим оператерима критичне инфраструктуре.

Сматрамо да би истраживања разумевања концепта слободних генеричких ресурса у операторима критичне инфраструктуре, њиховог присуства и одсуства, као и поређења расположивости између организација које се ослањају на праксу LEAN менаџмента и оних код којих тај приступ није заступљен, односно оператера у јавном и приватном власништву, могла дати потпунији одговор на ову проблематику. Препоручујемо да се питања о слободним ресурсима усмере примарно на људске ресурсе и постојање „концептуалног вишка", како у секторима корпоративне безбедности, континуитета пословања и кризног тима, тако и код некључних запослених који у случајевима актуализације нерутинских ризика могу бити укључени у организациони одговор.

Иако су испитаници дали потврдне одговоре на питања усмерена на партиципативни приступ планирању и комуницирању, ове налазе би било потребно тестирати анкетирањем запослених у операторима критичне инфраструктуре како би се могли извести валидни закључци. Такође, организовање даљих квалитативних истраживања у форми интервјуа и/или фокус група са доносиоцима одлука које би детаљније истражило елементе партиципативног приступа планирању и комуницирању довело би до дубљих увида у организациону праксу и културу оператера критичних инфраструктура. Даље, овде би се могла извршити секторска поређења, као и поређења између оператера критичне инфраструктуре који припадају јавном и приватном сектору.

Потребна су даља истраживања о повезаности партиципативног приступа управљању ризиком и правовременог осмишљавања, то јест препознавања и придавања смисла наступајућим реметилачким догађајима у циљу предузимања активности митигације. Истраживања о партиципативној изради регистра ризика, те повезаности присуства ризика у регистру и осмишљавања могу бити корисна у том смеру. За ова истраживања препоручујемо квалитативни приступ применом истраживачких техника интервјуа и фокус група.

Препоручујемо и истраживање димензије националних организационих култура „избегавања неизвесности" међу највишим руководством, менаџерима безбедности и континуета пословања у Републици Србији и региону, како би се на већем узорку добила потврда закључак из резултата добијених овим истраживањем о преференцији испитаника за стриктно поступање по плановима и процедурама. Концептуална и емпиријска истраживања повезаности појмова „избегавања неизвесности" и „толеранције на неизвесност" би такође могла довести до плодних закључака о могућности унапређења креативних одговора на кризни догађај узрокован нерутинским ризицима.

Суочавање са стресом запослених посредно је истражено у овој дисертацији путем питања о одсуству већег броја некључних запослених са посла током пандемије COVID-19, а у складу са налазима докторске дисертације Ридлове (Riddle 2015) и претходних истраживања које су тематизовале овај проблем (Gershon et al. 2010). Сматрамо да би било важно поновити њихова истраживања и у нашем територијалном оквиру како би се могли поредити резултати са поменутима истраживањима. Такође, свесни смо да је ово само једна од манифестација суочавања са стресом тако да би истраживања усмерена на друге манифестације стреса и реакције запослених на њих, узимајући у обзир и природу ризика била од значаја за даље утемељење овог елемента меког аспекта организационе отпорности. Напокон, организациона идентификација запослених у операторима критичне инфраструктуре би такође могла осветлити овај феномен из другог угла.

Истраживање међуповезаности, односно интензитета и типа сарадње између оператера критичних инфраструктура у току фаза кризног одговора и опоравка могло би допринети препорукама за унапређивање пословне праксе оператера, али и у односе међузависности сектора критичне инфраструктуре.

Потребно је анализирати могућности примене приступа динамичког адаптивног планирања за намене управљања нерутинским ризицима, те дизајнирати примењив модел који би се затим могао пилотирати у одређеним организационим системима, а затим и потенцијално уврстити у захтеве националних стандарда за управљање ризицима и систем менаџмента континуитетом пословања, као и у будуће безбедносне планове оператера критичне инфраструктуре предвиђене законом. На овај начин би се формализовала и олакшала пракса ажурирања и адаптирања планова која је неформално присутна у свим испитиваним операторима критичне инфраструктуре.

Предлажемо и истраживања усмерена на праксе организационог учења из криза, узимајући у обзир налазе овог истраживања који могу указивати на тенденцију статичког и линеарног учења из криза.

Напокон, предлажемо да емпиријска истраживања која буду тематизовала критичне инфраструктуре, или као узорак користила њихове запослене и доносиоце одлука, буду под покровитељством надлежних институција, у циљу лакшег и бржег прикупљања података.

Литература

1. Aberbach, J.D. & Rockman, B.A. (2002). Conducting and Coding Elite Interviews. *PS: Political Science and Politics*, 35, 673-676.
2. Acquaah, M., Amoako-Gyampah, K. and Jayaram, J. (2011). Resilience in family and nonfamily firms: An examination of the relationships between manufacturing strategy, competitive strategy and firm performance. *International Journal of Production Research*, 49: 5527– 5544
3. Albrechtsen, E. (2015). Major accident prevention and management of information systems security in technology-based work processes. *Journal of Loss Prevention in the Process Industries*, 36: 84-91.
4. Aldrich, D. P., & Meyer, M. A. (2014). Social capital and community resilience. *American Behavioral Scientist*, 59(2): 254–269.
5. Alessandri, T. M., Ford, D. N., Lander, D. M., Leggio, K. B. & Tazlory, M. (2004). Managing risk and uncertainty in complex capital projects. *The Quarterly Review of Economics and Finance*, 44: 751-767
6. Alexander. D.E. (2013). Resilience and disaster risk reduction: an etymological journey. *Natural Hazards and System Sciences*. 13(11): 2707:2716.
7. American Society for Industrial Security. (2017). *Security and Resilience in Organizations and their Supply Chains – Requirements and Guidance. (ASIS ORM.1-2017)*.
8. Andersen S. & Mostue B.A. (2012). Risk analysis and risk management approaches applied to the petroleum industry and their applicability to IO concepts. *Safety Science*, 50(10): 2010-2019.
9. Anderson, P.A. (1983). Decision making by objection and the Cuban Missile Crisis. *Administrative Science Quarterly*, 28(2): 201-222.
10. Andriani, P. (2003). *The emergence of self-organisation in social systems: the case of the geographic industrial clusters*. PhD Thesis, Durham University, 298pp.
11. Ashby, R.W. (1956). *An Introduction to Cybernetics*. Chapman & Hall, London.
12. Auf der Heide, E. (1989). *Disaster Response: Principles and preparation for coordination*. St Louis, MO: The CV Mosby Company.
13. Australian Government. (2010). *Critical Infrastructure Resilience Strategy*.
14. Australian Government. (2015). *Critical Infrastructure Resilience Strategy – Policy Statement*.
15. Australian Government. (2018). *The Security of Critical Infrastructure Act*.
16. Aven, T. (2011). On Different Types of Uncertainties in the Context of the Precautionary Principle. *Risk Analysis*. 31(10): 1515-1525.
17. Aven, T. (2014). The Concept of Antifragility and its Implications for the Practice of Risk Analysis. *Risk Analysis*. 35(3): 476-485.
18. Aven, T. (2019). The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Analysis*. 39(6): 1196-1203.
19. Aven, T. (2020). *The Science of Risk Analysis – Foundation and Practice*. New York: Routledge.
20. Aven, T. (2022). On Some Foundational Issues Concerning the Relationship Between Risk and Resilience. *Risk Analysis*. 42(9): 2062-2074.
21. Aven, T., and Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*. 12(1): 1-11.

22. Azadeh, A., Hassania, M. & Salehi, V. (2016). The impact of redundancy on resilience engineering in a petrochemical plant by data envelopment analysis. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 230: 1-12.
23. Balicer, R.D., Barnett, D.J., Thompson, C.B., Hsu, E.B., Catlett, C.L., Watson, C.M., Semon, N.L., Gwon, H.S., & Links, J.M. (2010). Characterizing Hospital Workers' Willingness to Report to Duty in an Influenza Pandemic through Threat- and Efficacy-Based Assessment. *BMC Public Health* 10: 436.
24. Barasa, E., Mbau, R., & Gilson, L. (2018). What is Resilience and How It Can Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience. *International Journal of Health Policy Management*. 7 (6): 491-503.
25. Barnett, D., Balicer, R., Thompson, C., Storey, D., Omer, S., Semon, N., Bayer, S., Cheek, L., Gateley, K., Lanza, K., Norbin, J., Slemp, C. & Links, J. (2009). Assessment of Local Public Health Workers' Willingness to Respond to Pandemic Influenza through Application of the Extended Parallel Process Model. *PloS one*. 4(7):1-8.
26. Barton, M.A. & Sutcliffe, K.M. (2009). Overcoming dysfunctional momentum: Organizational safety as a social achievement. *Human Relations*, 62(9): 1327-1356.
27. Barton, M.A., Sutcliffe, K.M., Vogus, T.J. & DeWitt, T. (2015). Performing under uncertainty: Contextualized engagement in wildland firefighting. *Journal of Contingencies and Crisis Management*, 23(2): 74-83.
28. Baum, S. (2015). Risk and Resilience for Unknown, Unquantifiable, Systemic and Unlikely/Catastrophic Threats. *Environment Systems and Decisions*, 35:229-236.
29. Bechky, B.A. & Okhuysen, G.A. (2011). Expecting the unexpected? How SWAT officers and film crews handle surprises. *Academy of Management Journal*, 54(2): 239-261.
30. Bento, F., Giglio Bottino, A., Cerchiareto Pereira, F., Forastieri de Almeida, J., & Gomes Rodrigues, F. (2021). Resilience in higher education: A complex perspective to lecturers' adaptive processes in response to the COVID-19 pandemic. *Education Sciences*, 11(9): 492.
31. Bento, F. & Garotti, L. (2019). Resilience beyond Formal Structures: A Network Perspective towards the Challenges of an Aging Workforce in the Oil and Gas Industry. *J. Open Innov. Technol. Mark. Complex.* 2019, *5*(1): 15
32. Berthod, O., Grothe-Hammer, M., Muller-Seitz, G., Raab, J. & Sydow, J. (2017). From High Reliability Organizations to High-Reliability Networks: The Dynamics of Network Governance in the Face of Emergency. *Journal of Public Administration Research and Theory*, 27(2): 352-371.
33. Berthod, O., Grothe-Hammer, M. & Sydow, J. (2015). Some Characteristics of High-Reliability Networks. *Journal of Contingencies and Crisis Management*, 23(1): 24-28.
34. Bhamra, R., Dani, S. & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research*, 49:5375–5393.
35. Bier, V. (2017). Introduction to Extreme Events. In: Bier, V (Ed.) *Risk in Extreme Environments: Preparing, Avoiding, Mitigating and Managing.* (pp.16-22). New York: Routledge.
36. Bier, V., Haimes, Y.Y., Lambert, J., Mathalas, N., & Zimmerman, R. (1999). A Survey of Approaches for Assessing and Managing the Risk of Extremes. *Risk Analysis*, 19(1): 83-94.
37. Bierly, P. E., & Spender, J.C. (1995). Culture and high-reliability organizations: The case of the nuclear submarine. *Journal of Management*, 21(4): 639–656.
38. Bigley, G. A. & Roberts, K. H. (2001). The incident command system: High-reliability organizing for complex and volatile task environments. *Academy of Management Journal*, 44(6): 1281–1299.

39. Biringer, B., Vugrin, E. & Warren, D. (2013). *Critical Infrastructure System Security and Resiliency.* Boca Raton, Fl: CRC Press, 230pp.
40. Boin, A. (2009). The new world of crises and crisis management: implications for policymaking and research. *Review of Policy Research*, 26(4): 367-377.
41. Boin, A., Comfort, L., & Demchak C (eds.). (2010). Designing Resilience: Preparing for Extreme Events. Pittsburgh, Pa : University of Pittsburgh Press. 349pp.
42. Boin, A. & Mcconnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management*. 15: 50 - 59.
43. Boin, A. & t'Hart, Paul. (2003). Public Leadership in Times of Crisis. *Public Administration Review*. 63: 544 - 553.
44. Boin, A. & van Eeten, M.J.G. (2013). The resilient organization: A critical appraisal. *Public Management Review,* 15: 29–445.
45. Boldog, P., Tekeli, T., Vizi, Z., Dénes, A., Bartha, F.A., Röst, G. (2020). Risk Assessment of Novel Coronavirus COVID-19 Outbreaks Outside China. *Journal of Clinical Medicine*, 9, 571.
46. Bonnano, G.A. (2004). Loss, trauma, and human resilience. *American Psychologist*, 59(1): 20-28.
47. Bonnano, G.A., Brewin, C.R., Kaniasty, K. & La Greca, A.M. (2010). Weighing the costs of disaster consequences, risk, and resilience in individuals, families, and communities. *Psychological Science in the Public Interest*. 11(1): 1-49
48. Bonanno, G. A., Westphal, M., & Mancini, A. D. (2011). Resilience to loss and potential trauma. *Annual Review of Clinical Psychology*, 7: 511–535.
49. Borgatti, S., Mehra, A., Brass, D. & Labianca, G. (2009). Network Analysis in the Social Sciences. Science 323(5916):892-5.
50. Borgatti, S., Johnson, J. & Everett. M. (2018). Analyzing Social Networks. NY, NY: Sage, 384pp.
51. Borodzicz, E. (2001): Security and risk, A theoretical approach to Managing Loss Prevention. *International Journal of Risk, Security and Crime Prevention,* 1(2): 131-143.
52. Braes, B., & Brooks, D.J. (2011). Organisational Resilience: understanding and identifying the essential concepts. *WIT Transactions on the Built Environment*, 117, 117-128.
53. Braun, V. & Clarke, V. (2006). Using Thematic Analysis in Psychology, *Qualitative Research in Psychology* 3(2): 77–101.
54. Breakwell, G. M. (2007). *The psychology of risk.* Cambridge University Press. 350pp.
55. Brewin, C. R., Andrews, B., & Valentine, J. D. (2000). Metaanalysis of risk factors for posttraumatic stress disorder in trauma-exposed adults. *Journal of Consulting and Clinical Psychology*, 68(5): 748–766.
56. British Standards Institution. (2014). *BSI 65000:2014 – Guidance on Organizational Resilience*.
57. Brown, N., Rovins, J., Feldmann-Jensen, S., Orchiston, C., Johnston, J. (2017) Exploring disaster resilience within the Hotel sector: A systematic review of literature. *International Journal of Disaster Risk Reduction*.
58. Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., & von Winterfelt, D., (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities, *EERI Spectra Journal*, 19(4):733- 752.
59. Burnard, K. and Bhamra, R. (2011). Organisational resilience: Development of a conceptual framework for organisational responses. *International Journal of Production Research*, 49: 5581–5599.

60. Burns, W.J., & Slovic, P. (2009). Predicting and Modeling Public Response to a Terrorist Strike. *Non-published Research Reports, Paper 145*. CREATE Homeland Research Center.
61. Business Continuity Institute. BCI Statement on Organizational Resilience https://www.thebci.org/knowledge/bci-statement-on-organizational-resilience.html
62. Canton, L.G. (2007). *Emergency Management: Concepts and strategies for effective programs*. Hoboken, NJ: John Wiley & Sons.
63. Carlson, E. (2018). Vigilant resilience: the possibilities for renewal through preparedness. *Corporate Communications: an International Journal*. 23(2): 212–225.
64. Carpenter, S., Walker, B., Anderies, J. & Abel, N. (2001). From Metaphor to Measurement: Resilience of What to What? *Ecosystems*, 4: 765–781.
65. Carter, H.E., Drury, J., Rubin, J., Williams, R. & Amlot, R. (2014) 'Emergency Responders' Experiences of and Expectations Regarding Decontamination'.*International Journal of Emergency Services*, 3(2): 179–92.
66. Cerulo, K. A. (2008). *Never saw it coming: Cultural challenges to envisioning the worst*. Chicago, IL: University of Chicago Press
67. Chakraborty, T. and Ghosh, I. (2020). Real-time forecasts and risk assessment of novel coronavirus (COVID-19) cases: A data-driven analysis. Chaos Solitons Fractals. 135: 1-10.
68. Chaffee, M. (2009). Willingness of Health Care Personnel to Work in a Disaster: An Integrative Review of the Literature. *Disaster Medicine and Public Health Preparedness* 3(1): 42–56.
69. Chan, J.W.K. (2011). Enhancing organisational resilience: Application of viable system model and MCDA in a small Hong Kong company. *International Journal of Production Research*, 49: 5545–5563.
70. Christianson, M.K., Farkas, M.T., Sutcliffe, K.M. & Weick, K.E. (2009). Learning through rare events: Significant interruptions at the Baltimore & Ohio Railroad Museum. *Organization Science*, 20(5): 846-860.
71. Clarke, L. (1993) Drs. Pangloss and the Strangelove meet organizational theory: high reliability organizations and nuclear weapons accidents. *Sociological Forum*, 8:675–689.
72. Clement, V. & Rivera, J. (2017). From adaptation to transformation: An extended research agenda for organizational resilience to adversity in the natural environment. *Organization & Environment*, 30: 346–365
73. Cocking, C., Drury, J., & Reicher, S. (2009). The Psychology of Crowd Behaviour in Emergency Evacuations: Results from Two Interview Studies and Implications for the Fire and Rescue Services, *Irish Journal of Psychology: Special Edition: Psychology and the Fire and Rescue Services* 30(1–2): 59–73.
74. Coleman, J. S. (1990). *Foundations of social theory*. Cambridge, MA: Harvard University Press
75. Comfort, L.K. (2002). Rethinking security: organizational fragility in extreme events. *Public Administration Review*, 62(s1): 98-107.
76. Comfort, L. K. (2005). Risk, security, and disaster management. *Annual Review of Political Science*, 8: 335–356.
77. Comfort, L.K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, 67: 189-197.
78. Comfort, L. K. (2012a). Designing disaster resilience and public policy: Comparative perspectives, part I. *Journal of Comparative Policy Analysis: Research and Practice*, 14(2): 109–113.
79. Comfort, L. K. (2012b). Designing disaster resilience and public policy: Comparative perspectives, part II. *Journal of Comparative Policy Analysis: Research and Practice*, 14(2): 199–201.

80. Comfort, L., Sungu, Y., Johnson, D & Dunn, M. (2001). Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments. *Journal of Contingencies and Crisis Management.* 9. 144 - 158.
81. Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism /COM/2004/0702 final/
82. Conchie, S.M. & Burns, C. (2008). Trust and Risk Communication in High-Risk Organizations: A Test of Principles from Social Risk Research. *Risk Analysis*. 28(1): 141-149.
83. Conz, E. & Magnani, G. (2020). A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research. *European Management Journal*, 38(3): 400-412.
84. Cools, M. & Pashley, V. (2013). Pieces of a larger puzzle: the almost impossible task of protecting critical infrastructures, Cahiers inlichtingenstudies - Cahiers d'études du renseignement: BISC 3 Maklu. 3: 51-63.
85. Council Directive 2008/114/EC, On the identification and designation of european critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, 23.12.2008., L 345/75L 345/82.
86. Cyber Security of the UK´s Critical National Infrastructure. Third Report of Session 2017-2019. Joint Committee on the National Security Strategy. House of Lords, House of Commons 2018.
87. Cox, L.A., & Bier, V. (2018). *Probabilistic Risk Analysis*. In:Bier, V. (ed.) Risk in Extreme Environments, New York: Routledge, pp. 9-33.
88. Craig, R.K. (2020). Resilience Theory and Wicked Problems. *Vanderbilt Law Review*, 79: 2-39.
89. Crichton, M,. Ramsay, C., and Kelly, T. (2009) Enhancing Organisational Resilience Through Emergency Planning. Journal of Contingencies and Crisis Management,17(1): 24-37.
90. *Critical Infrastructure Resilience Strategy – Policy Statement*. (2015). Australian Government, Canberra ACT.
91. Curt, C. & Tacnet, JM. (2018). Resilience of Critical Infrastructures: Review and Analysis of Current Approaches: Resilience of Critical Infrastructures. *Risk Analysis*. 38: 1-18.
92. D'Adderio, L. (2014). The Replication Dilemma Unravelled: How Organizations Enact Multiple Goals in Routine Transfer. *Organization Science*, 25(4): 1325-1350.
93. Dalgaard-Nielsen, A. (2017). Organizational resilience in national security bureaucracies: Realistic and practicable? *Journal of Contingencies and Crisis Management*. 25(4): 341-349.
94. Dahlberg, R., Johannessen-Henry, C. T., Raju, E., & Tulsiani, S. (2015). Resilience in disaster research: Three versions. *Civil Engineering and Environmental Systems*, 32: 44–54.
95. Dahlman, O.(2011). Security and Resilience. *Resilience: Interdisciplinary Perspectives on Science and Humanitarianism*, 2:39-51.
96. Dalgaard-Nielsen, A. (2017). Organizational resilience in national security bureaucracies: realistic and practicable? Journal of Contingencies and Crisis Management, 25:341–349.
97. Danes, S.M., Lee, J., Amarapurkar, S., Stafford, K., Haynes, G. and Brewton, K.E. (2009). Determinants of family business resilience after a natural disaster by gender of business owner. *Journal of Developmental Entrepreneurship*, 14: 333–354.
98. Darkow, P.M. (2018). Beyond "Bouncing Back": Towards an Integral, Capability-Based Understanding of Organizational Resilience. *Journal of Contingencies and Crisis Management*, 00:1-12.
99. de Bruijne, MLC., Boin, A., & van Eeten, MJG. (2010). Resilience. Exploring the concept and its meaning. In L. K. Comfort, A. Boin, & C. C. Demchak (Eds.), *Designing Resilience. Preparing for extreme events.* University of Pittsburg Press. pp. 13-32.
100. Demidov, VV. (2002). Anthrax-related panic is worse than the disease. *Trends in Biotechnology*. 20(3):97.

101. Denyer, D. (2017). *Organizational Resilience: A summary of academic evidence, business insights and new thinking*. BSI and Cranfield School of Management, 54pp.
102. Department of Defense (2002). *News briefing – Secretary Rumsfeld and Gen. Myers*. Преузето 12.9.2019. са http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636
103. DesJardine, M., Bansal, P. and Yang, Y. (2017). Bouncing back: Building resilience through social and environmental practices in the context of the 2008 global financial crisis. *Journal of Management*, 45: 1434–1460.
104. Dewald, J., & Bowen, F. (2010). Storm clouds and silver linings: Responding to disruptive innovations through cognitive resilience. *Entrepreneurship Theory and Practice*, 34(1): 197–218.
105. DiGiovanni, C.J., Reynolds, B., Harwell, R., Stonecipher, E.B., & Burkle, F.M.J. (2003). Community Reaction to Bioterrorism: Prospective Study of Simulated Outbreak. Emerging Infectious Diseases, 9(6): 708-712.
106. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). . Преузето 17.07.2023. са: https://eur-lex.europa.eu/eli/dir/2022/2555
107. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Преузето 17.07.2023. са: https://eur-lex.europa.eu/eli/dir/2022/2557/oj
108. Dooley, KJ. (1997). A Complex Adaptive Systems Model of Organizational Change. *Nonlinear Dynamics, Psychology and Life Sciences,* 1, 69-97.
109. Dooley, K., Johnson, T., & Bush, D. (1995). TQM, chaos, and complexity. *Human Systems Management,* 14, 297–302.
110. Drabek, T.E. (1985). Managing the emergency response. *Public Administration Review*, 45: 85-92.
111. Drabek, T.E. & McEntire, D.A. (2003). Emergent phenomena and the sociology of disaster: Lessons, trends and opportunities from the research literature. *Disaster Prevention and Management*, 12(2): 97-112.
112. Drury, J. (2009). Managing Crowds in Emergencies: Psychology for Business Continuity.*Business Continuity Journal*, 3(3): 14–24.
113. Drury, J., Cocking, C., & Reicher, S. (2009a). Everyone for Themselves? A Comparative Study of Crowd Solidarity among Emergency Survivors'.*British Journal of Social Psychology*,48(3): 487–506.
114. Drury, J., Cocking, C., & Reicher, S. (2009b). The Nature of Collective Resilience: Survivor Reactions to the 2005 London Bombings.*International Journal of Mass Emergencies and Disasters*, 27(1): 66–95.
115. Duchek, S. (2020). Organizational Resilience: A Capability-Based Conceptualization. *Business Research*, 13: 215-246.
116. Dunaway, M.W. (2010). *Four Degrees of Proximity: Key Factors that Influence Private Sector Preparedness and Continuity Planning*. PhD Dissertation. The George Washington University, Washington D.C.
117. Dunn Cavelty, M., Kaufmann, M., & Soeby Kristensen, K. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*, 46(1):3-14.
118. Ђурић, С. (2013). *Истраживање безбедности: квалитативни приступ*. Београд: Факултет безбедности.

119. Edwards, C. (2009). *Resilient nation*. London: Demos London. 104pp.
120. European Parliament and Council (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC
121. Ewertowski, T and Butlewski, M. (2021). Development of a Pandemic Residual Risk Assessment Tool for Building Organizational Resilience within Polish Enterprises. *International Journal of Environmental Research and Public Health*, vol 18, 6948.
122. Fahmy, S. & Johnson, T. (2007). Mediating the Anthrax Attacks: Media Accuracy and Agenda Setting During a Time of Moral Panic. Atlantic Journal of Communication. 15. 19-40.
123. Faraj, S., & Xiao, Y. (2006). Coordination in fast-response organizations. *Management Science*, 52(8): 1155– 1169.
124. Fink, A., Marr, B., Siebe, A. and Kuhie, J.-P. (2005). The future scorecard: Combining external and internal scenarios to create strategic foresight. *Management Decision*, 43: 360–381.
125. Fitzgerald, A., & Lupton, R. (2015). The limits to resilience? The impact of local government spending cuts in London. *Local Government Studies*, 41(4): 582–600.
126. Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalization. *Resilience*, 2(2):114-129.
127. Fleming, R.S. (2012). Ensuring organizational resilience in times of crisis. *Journal of Global Business Issues*, 6: 31–34.
128. Flynn, S. E. (2008). America the resilient-defying terrorism and mitigating natural disasters. *Foreign Affairs*, 87, 2.
129. Foster, S.P. & Dye, K. (2005). Building continuity into strategy. *Journal of Corporate Real Estate*, 7:105–119.
130. Fraccascia, L., Giannoccaro, I., & Albino, V. (2018). Resilience of complex systems: State of art and directions for further research. *Complexity*, vol 2018, 44pp.
131. Francis, R. & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*. 121: 90–103.
132. Freeman, S.F., Hirschhorn, S.J. and Maltz, M. (2004). The power of moral purpose: Sandler O'Neill & Partners in the aftermath of September 11th, 2001. *Organizational Development Journal*, 22: 69–81.
133. Fritzon, A., Ljungkvist, K., Boin, A. & Rhinard, M. (2007). Protecting Europe's critical infrastructures: Problems and prospects. Journal of Contingencies and Crisis Management. 15(1): 30-41.
134. Gallopin, G. (2006). Linkages between vulnerability, resilience, and adaptive capacity. *Global Environmental Change*, 16(3): 293-303.
135. Garrett, A.L., Park, Y.S., & Redlener, I. (2009). Mitigating Absenteeism in Hospital Workers during a Pandemic. *Disaster Medicine and Public Health Preparedness* 3(2): 141-147.
136. Gattringer, R., Damm, F., Kranewitter, P. & Wiener, M. (2021). Prospective collaborative sensemaking for identifying the potential impact of emerging technologies. *Creativity and Innovation Management*, 30: 651-673.
137. Gell-Mann, M. (1994). *The Quark and the Jaguar. Adventures in the Simple and the Complex*. New York: W.H. Freeman, 392pp.
138. Gershon, R.R. M., Magda, L.A., Qureshi, K.A., Riley, H.E.M., Scanlon, E., Carney, M.T., Richars, R.J., & Sherman, M.F. (2010). Factors Associated with the Ability and Willingness of Essential Workers to Report to Duty during a Pandemic'. *Journal of Occupational and Environmental Medicine,* 52(10): 995–1003.

139. Gibson, C.A. (2020). *Perspectives on Resilience*. Monographs in Risk and Resilience. Canberra: Australian Risk Policy Institute.
140. Gibson, C.A., & Tarrant, M. (2010). A 'Conceptual Models' Approach to Organisational Resilience. *Australian Journal of Emergency Management*. 25(2): 6-12.
141. Gilly, J.-P., Kechidi, M. and Talbot, D. (2014). Resilience of organisations and territories: The role of pivot firms. *European Management Journal*, 32: 596–602.
142. Glass, T.A. & Schoch-Spana, M. (2002). Bioterrorism and the people: how to vaccinate a city against panic. *Clinical Infectious Diseases*. 34(2):217-223.
143. Glover, J. (2012). Rural resilience through continued learning and innovation. *Local Economy*, 27: 355–372.
144. Goble, R. (2018). The Feasibility and Value of Adaptive Strategies for Extreme Risk. In: Bier, V. (ed.) *Risk in Extreme Environments*, New York: Routledge, 92-108.
145. Godschalk, D. R. (2003). Urban Hazard Mitigation: Creating Resilient Cities. *Natural Hazards Review,* 4, 136-143.
146. Goldstein, J. (1999). Emergence as a Construct: History and Issues. *Emergence*, 11: 49–72
147. Gosling, S.D., Vazire, S., Srivastava, S., & John, O.P. (2004). Should We Trust Web-Based Studies? A Comparative Analysis of Six Preconceptions about Internet Questionnaires'. *The American Psychologist,* 59(2): 93–104.
148. Grabowski, M. & Roberts, K. (2016). Reliability seeking virtual organizations: Challenges for high-reliability organizations and resilience engineering. Safety Science. 117.
149. Grint, K. (2005). Problems, problems, problems: The social construction of "leadership". *Human Relations*, 58(11), 1467-1494.
150. Grote, G. (2015). Promoting safety by increasing uncertainty – Implications for risk management. *Safety Science*. 71, 71-79.
151. Gunderson, L.H. (2000). Ecological Resilience—In Theory and Application. *Annual Review of Ecology and Systematics*, 31, 425-439.
152. Haimes, Y.Y. (2009). On the Complex Definition of Risk: A Systems-Based Approach. *Risk Analysis*, 29, 1647-1654.
153. Haldane, V., De Foo, C., Abdalla, S.M. et al. (2021). Health systems resilience in managing the COVID-19 pandemic: lessons from 28 countries. *Nature Medicine,* 27, 964–980.
154. Hamel, G. & Valikangas, L. (2003). The Quest for Resilience. *Harvard Business Review.* 81(9): 52-63.
155. Haunschild, P. R., Polidoro, F., Jr., & Chandler, D. (2015). Organizational oscillation between learning and forgetting: The dual role of serious errors. *Organization Science*, 26(6): 1682–1701.
156. Hayek, F. (1974). *The Pretence of Knowledge*. Преузето 15.09.2022. са https://www.nobelprize.org/prizes/economic-sciences/1974/hayek/lecture/
157. Hayes, B., Kane, G. & Kotwica, K. (2013). *Corporate Security – Organizational Structure, Cost of Services and Staffing Benchmark*. Research Report. Oxford: Elsevier.
158. Herbane, B. (2013). Exploring crisis management in UK small- and medium-sized entreprises. *Journal of Contingencies and Crisis Management*, 21(2): 82-95.
159. Hillmann, J. (2021). Disciplines of organizational resilience: contributions, critiques, and future research avenues. *Review of Managerial Science,* 15 (4), 879-936.
160. Hillmann, J. & Guenther, E. (2020). Organizational Resilience: A Valuable Construct for Management Research? *International Journal of Management Reviews*, 00: 1-38.
161. HM Government. (2010). Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.

162. Hobfoll, S. E. (2011). *Conservation of resources theory: Its implication for stress, health, and resilience*. In S. Folkman (Ed.), The Oxford handbook of stress, health, and coping. Oxford, United Kingdom: Oxford Library of Psychology, pp. 127–147.
163. Holling, C.S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4:1–23.
164. Hollnagel, E. (2012). Coping with Complexity: Past, Present and Future. *Cognition, Technology & Work*, 14(3), 199-205.
165. Hollnagel, E., Pariès, J., Woods, D.D. & Wreathall, J. (2011). *Resilience Engineering in Practice, A Guidebook*. Ashgate, Farnham.
166. Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Burlington, VT: Ashgate.
167. Homeland Security Advisory Council. (2006). *Report of the Critical Infrastructure Task Force*, January 2006.
168. Homeland Security Advisory Council. (2011). *Community resilience task force recommendations*. Washington DC, USA: Homeland Security Advisory Council.
169. Horne, J.F. (1997). *The Coming of Age of Organizational Resilience*. Business Forum, 22: 24-28.
170. Horne, J.F. & Orr, J.E. (1998). Assessing Behaviours that Create Resilient Organizations. *Employment Relations Today*, 24: 29-39.
171. Horton, R., Kiker, G.A., Trump, B.D. & Linkov, I. (2022). International airports as agents of resilience. *Journal of Contingencies and Crisis Management*. 30:217-220.
172. Hosseini, S., Barker, H. & Ramirez-Marquez, J.E. (2015). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety*. 145: 47-61.
173. Houts, P.S., Cleary, P.D., & Hu, W.T. (1988). *The Three Mile Island Crisis: Psychological, Social, and Economic Impacts on the Surrounding Population*, University Studies 49, Pennsylvania University Press.
174. Ianella, R. & Henricksen, K. (2007). Managing information in the disaster coordination centre: lessons and opportunities. In: (Van de Walle, B., P. Burghardt and C. Nieuwenhuis, eds.) *Proceedings of the 4th International ISCRAM Conference*. Delft, the Netherlands, May 2007.
175. Институт за стандардизацију Србије. (2017). *SRPS.A.L2.003:2017. Безбедност и отпорност – Процена ризика*.
176. Институт за стандардизацију Србије. (2015). *SRPS ISO 22301:2014*, *Друштвена безбедност – Системи менаџмента континуитетом пословања – Захтеви*..
177. International Standards Organization. (2016). *ISO 22316:2016, Organizational Resilience*.
178. International Standards Organization. (2015). *ISO TS 22317:2015, Societal Security – Business Continuity Management Systems – Business Impact Analysis.*
179. International Standards Organization/International Electrotechnical Commision. (2018). ISO/IEC 31010:2019*, Risk Assessment Techniques.*
180. International Standards Organization. (2009). *ISO GUIDE 73:2009, Risk Management – Vocabulary*.
181. IRGC (International Risk Governance Council). (2005). *White paper on risk governance. Towards an integrative approach*. Annexes by P. Graham, (Eds.), Geneva, Switzerland: International Risk Governance Council.
182. Jackson, S.E. & Dutton, J.E. (1988). Discerning threats and opportunities. *Administrative Science Quarterly*, 33(3): 370-387.

183. James, E.H. & Wooten, L.P. (2010). *Leading under pressure: From surviving to thriving before, during, and after a crisis*. New York, NY: Routledge Academic.
184. James, E.H., Wooten, L.P. & Dushek, K. (2011). Crisis Management: Informing a new leadership research agenda. *The Academy of Management Annals*, 5(1): 455-493.
185. Jin, A.S., Trump, B.D., Golan, M., Hynes, W., Young, M. & Linkov, I. (2021). Building resilience will require compromise on efficiency. *Nature Energy.* **6**: 997–999.
186. Johnsen, S. (2012). Resilience at interfaces: Improvement of safety and security in distributed control systems by web of influence. Informations management and computer security. 20(2): 71-87.
187. Jovanović, A., Klimek, P. & Choudhary, A. (2016). *Analysis of existing assessment resilience approaches, indicators and data sources: Usability and limitations of existing indicators for assessing, predicting and monitoring critical infastructure resilience*. Technical Report. Deliverable D1.2 of the Smart Resilience project, http://www.smartresilience.eu-vri.eu/ .
188. Kadri, F., Chatelet, E. & Chen, G. (2014). *Quantitative Assessment of Domino Effect Caused by Heat Radiation in Industrial Sites*. Proceedings of the 4th International Conference on Risk Analysis (ICRA4), Limassol, Cyprus, 1-8.
189. Kahn, W.A., Barton, M.A. & Fellows, S. (2013). Organizational crises and the disturbance of relational systems. *Academy of Management Review*, 38(3): 377-396.
190. Kahneman, D., & Tversky, A. (1973). On the Psychology of Prediction. *Psychological Review*, 80: 237-251.
191. Kahneman, D., & Tversky, A. (1979). Prospect Theory: An analysis of decision under risk. *Econometrica*, 47: 263-291.
192. Kahneman, D., Slovic, P., & Tversky, A. (Eds.). (1982). *Judgment under Uncertainty: Heuristics and Biases*. Cambridge: Cambridge University Press. 544pp.
193. Kaplan, S. & Garrick, B.J. (1981). On the Quantitative Definition of Risk. Risk Analysis, 1: 11-27.
194. Kapucu, N. (2008). Collaborative emergency management: Better community organising, better public preparedness and response. *Disasters*, 32(2): 239–262.
195. Kast, F. E., & Rosenzweig, J. E. (1972). General Systems Theory: Applications for Organization and Management. *Academy of Management Journal*, 15, 447-465.
196. Khakzad, N., Khan, F., Amyotte, P. & Cozzani, V. (2014). Risk management of domino effects considering dynamic consequence analysis. *Risk Analysis*. 34(6): 1128-1138.
197. Кековић, З. (2006). Криза као процес. У: Зоран Кековић и Желимир Кешетовић (ур.) *Кризни менаџмент – хрестоматија*. Београд: Факултет безбедности, 441-456.
198. Кековић, Z. (2020). SARS-COV-2: Од управљања ризицима ка организационој отпорности. *Зборник радова Правног факултета у Новом Саду*. 54(2): 611-633.
199. Кековић, З. (2022). Ефекти неизвесности у одлучивању о системским ризицима. Годишњак, Универзитет у Београду, Факултет безбедности, Годишњак Факултета безбедности, 15-37.
200. Keković Z, Dragišić Z, Ninković V (2014). Towards Resilient Critical Infrastructure against Terrorism Risk. In: Denis Čaleta and Vesela Radović (eds.) *Comprehensive approach as "sine qua non" for critical infrastructure protection*. NATO ARW, Amsterdam: IOS Press, pp. 45-59.
201. Кековић, З., Савић, С., Комазец, Н., Милошевић, М., Јовановић, Д. (2014). *Процена ризика у заштити лица, имовине и пословања*. Београд: Центар за анализу ризика и управљање кризама.

202. Keković, Z. & Ninković, N. (2020). Towards a conceptualisation of resilience in security studies. *Srpska politička misao*. 1:153-175.
203. Kendra, J. M. & Wachtendorf, T. (2003). Elements of Resilience after the World Trade Center Disaster: Reconstituting New York City's Emergency Operations Centre. *Disasters*, 21, 37-53.
204. Кешетовић, Ж. (2008). *Кризни менаџмент*. Београд: Факултет безбедности, Службени гласник.
205. Кешетовић, Ж. (2018). Функционисање корпорација у кризним условима. У: Кековић З., Димитријевић И.Р. и Шекарић Н. (ур.) *Корпоративна безбедност*, Београд: Факултет безбедности, 2018, 119-143.
206. Kešetović, Ž., Keković, Z., Ninković, V. (2009). Percepcija rizika. *Kultura Polisa*, V(8-9-10): 547-564.
207. Kešetović, Ž. & Toth, I. (2012). *Problemi kriznog menadžmenta – znanstvena monografija*. Veleučilište Velika Gorica / FPZ, 263pp.
208. Killian, L.M. (1952). The Significance of Multiple-Group Membership in Disaster. *American Journal of Sociology*. 57: 309-314.
209. Klein, G.A. (1993). A Recognition-Primed Decision (RPD) Model of Rapid Decision Making. In: Klein, G.A., Orasanu, J., Calderwood, R. & Zsambok, C.E. (eds.) *Decision Making in Action*. Westport, CT: Ablex, pp. 138-147.
210. Klein, K. J., Ziegert, J. C., Knight, A. P., & Xiao, Y. (2006). Dynamic delegation: Shared, hierarchical, and deindividualized leadership in extreme action teams. *Administrative Science Quarterly*, 51(4): 590–621.
211. Kolluru, R.V & Brooks, D.G. (1995). *Integrated Risk Assessment and Strategic Management,* in: R. Kolluru, S. Bartell, R. Pitblade and S. Stricoff (eds.) Risk Assessment and Management Handbook. For Environmental, Health, and Safety Professionals, New York: McGraw-Hill, 2.1–2.23.
212. Костић, А. (2006). *Когнитивна психологија*. Београд: Завод за уџбенике.
213. Kotwica, K., Correia, D. & Hayes, B. (2013). *Business Continuity – Playbook.* Oxford: Elsevier.
214. La Porte, T.R. (ed) (1975). *Organized Social Complexity: Challenge to Politics and Policy*. Princeton, N.J.: Princeton University Press.
215. La Porte, T.R. & Consolini, P.M. (1991). Working in practice but not in theory: theoretical challenges of "high-reliability organizations". *Journal of Public Administration Research and Theory*, 1:19–48.
216. Labaka, L. (2013). *Resilience Framework for Critical Infrastructures*. PhD Dissertation. Universidad de Navarra. San Sebastian.
217. Lagadec, P. (2012). *Du risque major aux mégachocs*. Bordeaux: Editions Préventique.
218. Lalonde, C. & Roux-Dufort, C. (2010). Crisis management in institutional healthcare settings: From punitive to emancipatory solutions. *Organizational Development Journal*, 28(1): 19-36.
219. Lampel, J., Bhalla, A. and Jha, P.P. (2014). Does governance confer organisational resilience? Evidence from UK employee owned businesses. *European Management Journal*, 32: 66–72.
220. Landucci, G., Argenti, F., Tugnoli, A. & Cozzani, V. (2015). Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. *Reliability Engineering and System Safety*, 143(C): 30-43.
221. Lee, A., Vargo, J. & Seville, E. (2013). Developing a Tool to Measure and Compare Organizations' Resilience. *Natural Hazards Review*. 14. 29-41.

222. Lengnick-Hall, C.A. & Beck, T.A. (2005). Resilience Capacity and Strategic Agility: Prerequisites for Thriving in a Dynamic Environment. In: Nemeth, C.P., Hollnagel, E., & Dekker, S. (eds.) *Resilience Engineering Perspectives, Vol.2, Preparation and Restoration*, Aldershot: Ashgate Publishing, 39-70.
223. Lengnick-Hall, C.A., Beck, T.A., & Lengnick-Hall, M.L. (2011). Developing a Capacity for Organizational Resilience through Strategic Human Resource Management. *Human Resource Management Review*, 21: 243-255.
224. Lewis, L. P. & Petit, F. (2019). *Critical infrastructure interdependency analysis: Operationalising resilience strategies*. Contributing Paper to Global Assessment Report on Disaster Risk Reduction (GAR 2019). 33pp.
225. Limnios, E.A.M., Mazzarol, T., Ghadouani, A. and Schilizzi, S.G.M. (2014). The resilience architecture framework: Four organizational archetypes. *European Management Journa*l, 32: 104–116.
226. Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kroger, W., Lambert, J.H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change*. 4:407-419.
227. Linnenluecke, M. & Griffiths, A. (2010). Beyond Adaptation: Resilience for Business in Light of Climate Change and Weather Extremes. *Business & Society*. 49(3): 477-511.
228. Linnenluecke, M.K. (2017), Resilience in Business and Management Research: A Review of Influential Publications and a Research Agenda. *International Journal of Management Reviews*, 19: 4-30.
229. Liu, Y. & Juelin, Y. (2020). Stakeholder Relationships and Organizational Resilience. Management and Organizational Review. 1-5.
230. Longstaff, P. H. (2005). *Security, resilience, and communication in unpredictable environments such as terrorism, natural disasters, and complex technology*. Boston: Center for Information Policy Research, Harvard University.
231. Longstaff, P. H. (2012). Avoiding resilience "Kum Ba Yah" recognizing the tradeoffs before they become surprises. *The CIP Report*, 11(6): 4–6.
232. Longstaff, P.H, Armstrong N.J, Perrin K, Parker W.M. & Hidek M.A. (2010). Building Resilient Communities: A Preliminary Framework for Assessment. *Homeland Security Affairs,* VI (3): 1-23.
233. Lorenz, D.F. (2010). *The diversity of resilience: Contributions from a social science perspective*. In G. Hutter, C. Kuhlicke, T. Glade & C. Felgentreff (eds.). Natural Hazards. Special Volume: Resilience in Hazards Research and Planning – A Promising Concept?, pp.1-18.
234. Luhmann , N. (1993). *Risk. A sociological theory*. Berlin: De Gruyter.
235. Macaulay, T. (2008). *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*. CRC Press.
236. Mackay, J., Munoz, A., & Pepper, M. (2020). Conceptualising redundancy and flexibility towards supply chain robustness and resilience. *Journal of Risk Research*, 23(12): 1–21.
237. Madni, A. & Jackson, S. (2011). Towards a Conceptual Framework for Resilience Engineering. *IEEE Engineering Management Review*. 39(4): 85-102.
238. Maitlis, S. & Christianson, M. (2014). Sensemaking in Organizations: Taking Stock and Moving Forward. *The Academy of Management Annals*, 8(1): 57-125.
239. Maitlis, S. & Sonneshein, S. (2010). Sensemaking in crisis and change: Inspiration and insights from Weick (1988). *Journal of Management Studies*, 47(3): 551-580.

240. Mallak, L. (1998). Putting organizational resilience to work. Industrial Management, 40: 8–13.
241. Marcus, A.A. & Nichols, M.L. (1999). On the edge: Heeding the warnings of unusual events. *Organization Science*, 10: 482–499
242. Martin, P. (2020). *The Rules of Security*. Oxford Security Press.
243. Martin-Breen, P. Anderies, JM. (2011). *Resilience: A Literature Review*. Bellagio Initiative, Brighton: IDS, 67pp.
244. Maslaric, M., Backalic, T., Nikolicic, S. & Mircetic, D. (2013). Assessing the trade-off between lean and resilience through supply chain risk management. *International Journal of Industrial Engineering and Management*. 4(4): 229-236.
245. Mason, B. & Lyons, R. (2003). Acute Psychological Effects of Suspected Bioterrorism. *Journal of epidemiology and community health*. 57.
246. Masten, A. S., Best, K. M., & Garmezy, N. (1990). Resilience and development: Contributions from the study of children who overcome adversity. *Development and Psychopathology*, 2(4), 425–444.
247. Maule, J.A. (2009). Risk Communication in Organizations. In: Hodgkinson, G.P. & Starbuck, W.H. (eds.) *The Oxford Handbook of Organizational Decision Making*. Oxford Academic Press, Oxford UK, 517-533.
248. May, R.M., 1977. Thresholds and breakpoints in ecosystems with a multiplicity of stable states. *Nature*, 269(5628), 471–477.
249. McDonald, N. (2006) Organisational Resilience and Industrial Risk. In: Hollnagel, E., Woods, D.D. and Leveson, N., Eds., *Resilience Engineering Concepts and Precepts*, Ashgate Publishing Ltd., Aldershot, 155-180.
250. McDonald, M., & Westphal, J. (2003). Getting by with the advice of their friends: CEO's advice networks and firms' strategic responses to poor performance. *Administrative Science Quarterly*, 48: 1–32.
251. McFarlane, A. C., & Norris, F. H. (2006). *Definitions and concepts in disaster research*. In F. H. Norris, S. Galea, M. J. Friedman & P. J. Watson (Eds.), Methods for disaster mental health research. New York, NY: Guilford Press, pp. 3–19.
252. McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). A Facilitated Process for Improving Organizational Resilience. *Natural Hazards Review*, 9: 81-90.
253. Meyer, A.D. (1982). Adapting to environmental jolts. *Administrative Science Quarterly*, 27(4): 515-537.
254. Mikac, R., Cesarec, I., & Larkin, R. (2018). *Kritična infrastruktura - Platforma uspješnog razvoja sigurnosti nacija*. Zagreb: Jesenski i Turk.
255. Milburn, T.W., Schuyler, R.S. & Watman, K.H. (1983). Organizational crisis, Part I: Definition and conceptualization. *Human Relations*, 36(12), 1141-1160.
256. Miller, J. & Page, S. (2007). *Complex Adaptive Systems – An Introduction to Computational Models of Social Life*. Princeton University Press.
257. Мирковић, Б. (2016). *Социо-психолошки чиниоци одговорног организационог понашања*. Докторска дисертација. Београд. Филозофски факултет.
258. Mitroff, I.I. & Pearson, C.M. (1993). *Crisis Management*. San Francisco, CA: Jossey-Bass.
259. Мићовић, М. (2020). *Специфичности критичне инфраструктуре у Републици Србији*. Београд, Криминалистичко-полицијски универзитет, 104 стр.
260. Granger Morgan, M. & Henrion, M. (1990). *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. Cambridge University Press, Cambridge, 332pp.

261. Moteff, J.D. (2012). *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*. CRS Report for Congress. 24pp.
262. Nasteckiene, V. (2021). Empirical investigation of risk management practices. *Journal of Contemporary Management Issues*, 26(2): 79-98.
263. National Infrastructure Advisory Council. (2009). *Critical Infrastructure Resilience: Final Report and Recommendations*. Washington D.C.
264. National Research Council. (2012). *Disaster Resilience: A National Imperative*, The National Academies Press.
265. *National Security Strategy – A Strong Britain in an Age of Uncertainty*. (2010). HM Government.
266. *National Security Strategy and Strategic Defence and Security Review 2015 – A Secure and Prosperous United Kingdom*, HM Government, United Kingdom 2015.
267. *National Security Strategy and Strategic Defence and Security Review 2015 – Third Annual Report*. HM Government 2018
268. *National Strategy For Homeland Security*. (2007). Department of Homeland Security, Washington D.C..
269. Neal, D.M. & Phillips, B.D. (1995). Effective emergency management: Reconsidering the bureaucratic approach. *Disasters*, 19(4): 327-337.
270. Nedeljković, M., Vukonjanski, J., Nikolić, M., Hadžić, O. & Šljukić, M. (2018). A Comparative Analysis of Serbian National Culture and National Cultures of Some European Countries by GLOBE project approach. *Journal of the Geographical Institute "Jovan Cvijić" SASA*, 68(3): 363-382.
271. Николић, Д.Ж., Ковач, М. & Митић, В.М. (2018). Безбедносна заштита објеката од посебног значаја за одбрану. *Војно дело*, 70(7): 176-188.
272. Нинковић, В. (2018). Менаџмент континуитетом пословања. У З. Кековић, И. Р. Димитријевић и Н. Шекарић (Прир.), *Корпоративна безбедност – хрестоматија*. Београд: Факултет безбедности Универзитета у Београду, pp. 209-230.
273. Ninković, V. (2021). Critical Infrastructure Resilience – National Approaches in the United States of America, the United Kingdom and Australia. *Zbornik radova Pravnog fakulteta u Novom Sadu*, 4: 1205-1225.
274. National Infrastructure Protection Plan NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. Washington D.C.: U.S. Department of Homeland Security.
275. Obama, B. (2013). Presidential Policy Directive/PPD-21. February 12, 2013. Преузето 23.12.2023. са. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-poli-cy-directive-critical-infrastructure-security-and-resil
276. *Одлука о објектима од посебног значаја за одбрану,* „Сл. Гласник РС, бр. 112/2008",
277. *Одлука о великим техничким системима од значаја за одбрану,* „Сл. Гласник РС, бр. 41/2014, 35/2015, 86/2016 и 53/2017
278. Øien, K., Bodsberg, L. & Jovanović, A. (2018). Resilience assessment of smart critical infrastructures based on indicators. In : Haugen et al (eds.). *Safety and Reliability – Safe Societies in a Changing World*. London – Taylor and Francis, 1269-1277.
279. O'Connor, P., Jimmieson, N., Bergin, A., Wiewiora, A. & McColl, L. (2021). Leader Tolerance of Ambiguity: Implications for Follower Performance Outcomes in High and Low Ambiguous Work Situations. *The Journal of Applied Behavioral Science*. 58(1): 65-96.
280. O'Sullivan, T.L., Amaratunga, C., Phillips, K., Corneil, W., O'Connor, E., Lemyre, L. &Dow, D. (2009). If Schools Are Closed, Who Will Watch Our Kids? Family Caregiving and

Other Sources of Role Conflict among Nurses during Large-Scale Outbreaks. *Prehospital and Disaster Medicine* 24(4): 321–25.
281. Parker, R. (2010). *Organizations—Their role in building societal resilience*. Fairfax, Virginia: Proceedings of the international symposium on societal resilience.
282. Parsons, D. (2010). Organizational Resilience. *The Australian Journal of Emergency Management*, 25(02): 18-20.
283. Paté-Cornell, E. (2012). On "Black Swans" and "Perfect Storms": Risk Analysis and Management When Statistics Are Not Enough. *Risk Analysis*. 32(11):1823-33.
284. Paton, D., Smith, L., & Violanti, J. (2000). Disaster Response: Risk, Vulnerability and Resilience. *Disaster Prevention and Management*. 9. 173-180.
285. Pavićević, O. (2016). Koncept otpornosti u sociologiji. *Sociologija*. 58 (3): 432-449.
286. Pearce, J.M., Rogers, M.B. Rubin, J & Wessely, S. (2011). *CIE Toolkit WP8: Risk and Crisis Communication Requirements Following a Chemical Incident or Emergency*. Unpublished Report to the European Commission'.
287. Pearce, J.M., Rubin, J., Selke, P., Amlôt, R., Mowbray, F., & Rogers, M.B. (2013). Communicating with the Public Following Radiological Terrorism: Results from a Series of Focus Groups and National Surveys in Britain and Germany'. *Prehospital and Disaster Medicine,* 28(2): 110–19.
288. Pearson, C.M. & Clair, J.A. (1998). Reframing crisis management. *Academy of Management Review*, 23(1): 59-76.
289. Pellissier, R. (2011). The implementation of resilience engineering to enhance organizational innovation in a complex environment. *International Journal of Business Management*, 6:145–164.
290. Perrow, C. (2011). *Normal accidents: living with high-risk technologies*. Princeton, NJ: Princeton University Press.
291. Pidgeon, N. (1992): *The Psychology of Risk*. in D. I. Blockley (ed.) Engineering Safety, McGraw-Hill, pp.167-186.
292. Pike, A., Dawley, S., & Tomaney, J. (2010). Resilience, Adaptation and Adaptability. *Cambridge Journal of Regions, Economy and Society*. pp.1-12.
293. Pitt, M. (2007). *Learning Lessons from the 2007 Floods. An Independent Review by Sir Michael Pitt, Interim Report (The Pitt Review).* U.K. Government, London.
294. Polua, G. (1957). *How to Solve It – A New Aspect of Mathematical Method*. Double Day Anchor Books, New York, USA 253 pp.
295. Ponomarov, S.Y. & Holcomb, M.C. (2009). Understanding the Concept of Supply Chain Resilience. *The International Journal of Logistics Management*, 20(1):124-143.
296. *Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura*, Narodne Novine Republike Hrvatske, br.47/2016
297. Prigogine, I. & Stengers, I. (1984). Order Out of Chaos: Man's New Dialogue with Nature, Verso Books. 384pp.
298. *Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*. /* COM/2006/0787 final - CNS 2006/0276 */
299. Pursiainen, C. (2009). The Challenges for European Critical Infrastructure Protection, *European Integration*, vol. 31, no. 6.
300. Quarantelli, E.L. (1988). Disaster crisis management: a summary of research findings. *Journal of Management Studies*, 25(4): 373-385.
301. Quarantelli E.L. (2005). A social science research agenda for the disasters of the 21st century: Theoretical, methodological and empirical issues and their professional

implementation. In: Perry, R.W.& E.L. Quarantelli (eds.). *What is a disaster? New answers to old questions*: 325-396. Philadelphia, PA: Xlibris.
302. Quarantelli, E. L., & Dynes, R. R. (1977). Response to social crisis and disaster. *Annual Review of Sociology*, 3: 23–49.
303. Qureshi, K., Gershon, R.R.M., Sherman, M.F., Straub, T., Gebbie, E., McCollum, M., Erwin, M.J.,& Morse, S.S. (2005). Health Care Workers' Ability and Willingness to Report to Duty DuringCatastrophic Disasters. *Journal of Urban Health: Bulletin of the New York Academy of Medicine*, 82(3): 378–88.
304. Rabbani M., Yazdanparast R. & Mobini M. (2019). An algorithm for performance evaluation of resilience engineering culture based on graph theory and matrix approach. International Journal of System Assurance Engineering and Management, 10(2): 228–241.
305. Radvanovsky, R. & McDougall, A. (2010). *Critical Infrastructure: Homeland Security and Emergency Preparedness*. NY, CRC Press.
306. Rahmandad, H., & Repenning, N. (2016). Capability erosion dynamics. *Strategic Management Journal*, 37(4): 649–672.
307. Ракић, М. (2015). *Кризни менаџмент у функцији заштите критичне инфраструктуре у земљама у транзицији*. Докторска дисертација. Београд, Факултет безбедности.
308. Ramirez, R., Selsky, J.W. and van der Heijden, K. (eds) (2010). *Business Planning for Turbulent Times: New Methods for Applying Scenarios*. London: Earthscan Ltd.
309. Rankin, A., Lundberg, J., Woltjer, R., Rollenhagen, C. & Hollnagel, E. (2014). Resilience in Everyday Operations. *Journal of Cognitive Engineering and Decision Making*, 8(1): 78-97.
310. Ray, J.L., Baker, L.T. and Plowman, D.A. (2011). Organizational mindfulness in business schools. *Academy of Management Learning & Education*, 10: 188– 203.
311. Reid, L. (2005). Diminishing Returns? Risk and the Duty to Care in the SARS Epidemic', *Bioethics,* 19(4): 348–361.
312. Renn, O. (1992). *Concepts of risk: A classification*. In: Krimsky, S. & Golding, D. (eds), Social Theories of Risk, Praeger Publishers, Westport, CT.
313. Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. London: Earthscan. 456op.
314. Renn, O. (2015). Stakeholder and Public Involvement in Risk Governance, *International Journal of Disaster Risk Science*, 6: 8-20.
315. Renn, O., & Klinke, A. (2015). *Complexity, Uncertainty and Ambiguity in Inclusive Risk Governance*. In T. J. Andersen (Ed.), The Routledge companion to strategic risk management (pp. 13-30). London: Routledge.
316. Report of the Royal Society Study Group, (1992). *Risk: Analysis, Perception, Management*. London, Royal Society.
317. Rerup, C. (2001). Houston, We Have a Problem: Anticipation and Improvisation as Sources of Organizational Resilience. *Comportamento Organizacional e Gestao*, 7: 27-44.
318. Rerup, C. (2009). Attentional triangulation: Learning from unexpected rare crises. *Organization Science*. 20(5): 876-893.
319. *Resilience Study Scoping Report*, National Infrastructure Commission, UK September 2019.
320. Riddle, L. (2015). *Variations in Organizational and Employee Responses to High-Impact, Low-Probability Events*. PhD Dissertation, Department of War Studies, Kings College, London.

321. Ridley, G. (2017). Resilience and National Security. In: Dover. R, Dylan H & Goodman M. (eds.). *The Palgrave Handbook of Security, Risk and Intelligence*. Palgrave Macmillan UK, London, pp.79-98.
322. Riggio, R.E. & Newstead, T. (2023). Crisis Leadership. *Annual Review of Organizational Psychology and Organizational Behavior*. 10:201-204.
323. Righi, A.W., Saurin, T.A. & Wachs, P. (2015) A Systematic Literature Review of Resilience Engineering: Research Areas and a Research Agenda Proposal. *Reliability Engineering & System Safety*, 141: 142-152.
324. Rijpma, J.A. (1997). Complexity, tight-coupling and reliability: connecting normal accidents theory and high reliability theory. Journal of Contingencies and Crisis Management, 5:15–23.
325. Rinaldi, S., Peerenboom, J., Kelly, T. (2001). Critical Infrastructure Inter-dependencies. *IEEE Control Systems Magazine*. 21(6):11-25.
326. Rittel. H.W.J. & Webber, M.M. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences*, 4, 155-169.
327. Robbins, S. P. (1992). *Bitni elementi organizacijskog ponašanja*. Zagreb: Mate.
328. Robert, B. (2010). *Organizational Resilience – Concepts and Evaluation Method*. Montreal: Presse de l'Ecole Polytechnique de Montreal.
329. Roberts, K.H. (1993). *New challenges to understanding organizations*. Macmillan Publishing, New York.
330. Roberts, K. H., Stout, S. K., & Halpern, J. J. (1994). Decision dynamics in two high reliability military organizations. *Management Science*, 40(5): 614–624.
331. Rodehorst, B., Dix, B., Hurley, B., Keller, J., Hyman, R., Beucler, B., Mohamed, K., & Kafalenos, R. (2018). Planning to Build Resilience into Transportation Assets: Lessons Learned. *Transportation Research Record*, 2672(3), 118–129.
332. Rogers, M.B., & Pearce,J.M. (2013). Risk Communication, Risk Perception and Behavior as Foundations of Effective National Security Practices. In *Strategic Intelligent Management*, 1st ed.: 66–74. Elsevier Butterworth-Heinemann.
333. Rogers, M.B., Amlot, R., & Rubin, J. (2013). The Impact of Communication Materials on Public Responses to a Radiological Dispersal Device (RDD) Attack. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science,* 11(1): 49–58.
334. Roux-Dufort, C. (2007). Is crisis management (only) a management of exceptions? *Journal of Contingencies and Crisis Management*, 15 (2): 105-114.
335. Roux-Dufort, C. (2016). Delving into the roots of crises: The genealogy of surprise. In: A. Schwarz, M.W.Seeger & C.Auer (Eds.) *The handbook of international crisis communication research*: 24-33. West Sussex, UK: Wiley.
336. Roux-Dufort, C. & Vidaillet, B. (2003). The difficulties of improvising in a crisis situation – a case study. *International Studies of Management & Organization*. 33(1): 86-115
337. Rosenthal, U., Charles, M. & 't Hart, P. (1989). "The world of crises and crises management" in Rosenthal U., Charles M.T. & 't Hart P (eds.): *Coping with Crises: the Management of Disasters, Riots and Terrorism*.. Springfield, Il: Charles T. Thomas.
338. Rubens, D. (2020). COVID-19: Lessons from a "Near-Miss" in Keković, Z., Đorić, M. & Polović, J. *Security Crises in the 21st Century and How to Manage Them*, Proceedings of the international academic conference held online on 13-14 October 2020. Beograd – CARUK, vol 1. pp.225-228.
339. Rubens, D. (2023). *Strategic Risk and Crisis Managemen*t. London, UK: Kogan Page LTD.

340. Ruderman, C., Tracy, C.S., Bensimon, C.M., Bernstein, M., Hawryluck, L., Shaul, R.Z., & Upshur, R.E.G. (2006). On Pandemics and the Duty to Care: Whose Duty? Who Cares?.*BMC Medical Ethics* 7(5).
341. Rudolph, J.W. & Repenning, N.P. (2002). Disaster dynamics: Understanding the role of quantity in organizational collapse. *Administrative Science Quarterly*, 47(1): 1-30.
342. Sagan, S. D. (2004). Learning from Normal Accidents. *Organization & Environment*, 17(1): 15–19.
343. Salanova, M., Llorens, S., Cifre, E. & Martínez, I.M. (2012). We need a hero! Toward a validation of the healthy and resilient organization (HERO) model. *Group & Organization Management*, 37: 785–822.
344. Sandaker, I. (2009). A Selectionist Perspective on Systemic and Behavioral Change in Organizations. *Journal of Organizational Behavior Management*, 29(3-4): 276-293.
345. Sawalha, I.H. (2013). Organisational performance and business continuity management: a theoretical perspective and a case study. *Journal of Business Continuity and Emergency Planning*, 6:360–373.
346. Sawalha, I.H. (2015). Managing adversity: understanding some dimensions of organizational resilience". *Management Research Review*, 38(4), 1-21.
347. Scheffer, M., Carpenter, S., Foley, J., Folke, C., & Walker, B. (2001). Catastrophic shifts in ecosystems. *Nature,* 413: 591–596.
348. Schneider, S.K. (1992). Governmental response to disasters: The conflict between bureaucratic procedures and emergent norms. *Public Administration Review*, 52(2): 135-145.
349. Schulman, P., Roe, E., van Eeten, M., & De Bruijne, M. (2004). High reliability and the management of critical infrastructures. *Journal of Contingencies and Crisis Management*, 12(1): 14–28.
350. Shaghaghi, A., Bhopal, R.S., & Sheikh, A. (2011). Approaches to Recruiting "Hard-To-Reach" Populations into Research: A Review of the Literature'. *Health Promotion Perspectives,* 1(2): 86–94.
351. Shaw, K.A., Chilcott, A., Hansen, E., & Winzenberg, T. (2006). The GP's Response to Pandemic Influenza: A Qualitative Study'. *Family Practice* 23(3): 267–272.
352. Shaw, K. & Maythorne, L. (2013). Managing for Local Resilience: Towards a Strategic Approach. *Public Policy and Administration,* 28(1):43-65.
353. Shaw, K. & Theobald, K. (2011). Resilient Local Government and Climate Change Interventions in the UK. *Local Environment*, 16(1): 1-15.
354. Shepherd, D. A., & Williams, T. A. (2014). Local venturing as compassion organizing in the aftermath of a natural disaster: The role of localness and community in reducing suffering. *Journal of Management Studies*, 51(6): 952–994.
355. Sheppard B., Rubin, J., Wardman, J.K., & Wessely, S. (2006). Terrorism and Dispelling the Myth of a Panic Prone Public. *Journal of Public Health Policy*, 27(3): 219–45.
356. Sheu, S.J., Wei, I.L., Chen, C.H., Yu, S., & Tang, F.I. (2009). Using Snowball Sampling Method with Nurses to Understand Medication Administration Errors'. *Journal of Clinical Nursing,* 18(4): 559–69.
357. Shrivastava, P. (1992). *Bhopal: Anatomy of a crisis*. London, UK: Paul Chapman
358. Simola, S.K. (2005). Organizational Crisis Management: Overview and Opportunities. Consulting Psychology Journal: Practice and Research, 57(3): 180–192.
359. Simonovic, S.P. (2016). From risk management to quantitative disaster resilience: a paradigm shift. *International Journal of Safety and Security Engineering*, 6(2):85-95.
360. Simonović, S.P. (2020). Systems Approach to Management of Water Resources—Toward Performance Based Water Resources Engineering. *Water*, 12(4): 1208.

361. Simonovic, S.P. & A. Peck, (2013). Dynamic Resilience to Climate Change Caused Natural Disasters in Coastal Megacities - Quantification Framework. *British Journal of Environment and Climate Change*, 3(3): 378-401.
362. Singer, P.A., Benatar, S.R., Bernstein, M., Daar, A.S., Dickens, B.M., MacRae, S.K., Upshur, R.E.G. & Shaul, R.Z. (2003). Ethics and SARS: Lessons from Toronto'. *BMJ* 327(7427): 1342–44.
363. Singh, P. (2021). *Development of Theory and Methodologies to Assess Adaptive Resilience in Infrastructure Systems*. Georgia Institute of Technology. PhD Thesis.
364. Skjerve, A.B., Kaarstad, M., Storseth, F., Waero, I. & Grotan, T.O. (2012). Planning for resilient collaboration at a new petroleum installation – A case study of a coaching approach. *Safety Science*, 50: 1952-1959.
365. Skyttner, L. (2005). *General Systems Theory: Problems, Perspectives, Practice*. Singapore: World Scientific Publishing, 536pp.
366. Slovic, P. (1987). Perception of Risk. *Science,* **236**: 280-285.
367. Slovic, P., Fischhoff, B., Lichtenstein, S. & Roe, F.J.C. (1981). *Perceived Risk: Psychological Factors and Social Implications*. Proceedings of The Royal Society A: Mathematical, Physical and Engineering Sciences 376: 17-34.
368. Smart C. & Vertinsky I. (1977). Designs for crisis decision units. *Administrative Science Quarterly*, 22(4): 640-657.
369. Smith, E., Morgans, A., Qureshi, K., Burkle, F., & Archer, F. (2009). Paramedics' Perceptions of Risk and Willingness to Work during Disasters. *The Australian Journal of Emergency Management*, 24(3): 25.
370. Somers, S. (2009). Measuring Resilience Potential: An Adaptive Strategy for Organizational Crisis Planning. *Journal of Contingencies and Crisis Management*. 17: 12-23.
371. Sornette, D. (2009). Dragon-Kings, Black Swans and the Prediction of Crises. *International Journal of Terraspace Science and Engineering*. 2 (1): 1-18.
372. Stacey, R. D. (1995). The science of complexity: An alternative perspective for strategic change processes. *Strategic Management Journa*l, 16(6): 477–495.
373. Stark, A. (2014). Bureaucratic values and resilience: An exploration of crisis management adaptation. *Public Administration*, 92: 692–706.
374. Starr, C. (1969). Social benefit versus technological risk. *Science*. 165:1232-1238.
375. Starr, R., Newfrock, J. & Delurey, M. (2003). Enterprise resilience: Managing risk in the networked economy. *Strategy and Business*, 30: 1–10.
376. Stephenson, A. (2010). *Benchmarking the resilience of organisations*. PhD dissertation, University of Canterbury, NZ.
377. Stergachis, A., Garberson, L., Lien, O., D'Ambrosio, L., Sangare, L. & Dold, C. (2011). Health Care Workers' Ability and Willingness to Report to Work During Public Health Emergencies. *Disaster Medicine and Public Health Preparedness*, 5(4): 300–308.
378. Straus, S.E., Wilson, K., Rambaldini, G., Rath, D., Lin, Y., Gold, W.L., & Kapral, M.K. (2004). Severe Acute Respiratory Syndrome and its Impact on Professionalism: Qualitative Study of Physicians' Behaviour during an Emerging Healthcare Crisis'. *BMJ* 329(7457):83.
379. *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, Cabinet Office, March 2010.
380. Sung, S.Y., Antefelt, A. & Jin, N.C. (2017). Duel Effects of Job Complexity on Proactive and Responsive Creativity: Moderating Role of Employee Ambiguity Tolerance. *Group & Organization Management*, 42(3): 388-418.

381. *Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects*. (2020). CISA. Преузето 07.12.2023. са https://www.cisa.gov/resources-tools/resources/incorporating-resilience-critical-infrastructure-projects
382. Sutcliffe, K.M. & Vogus, T.J. (2003). Organizing for resilience. In: K.S. Cameron, J.E.Dutton & R.E.Quinn (eds.), *Positive organizational scholarship: foundations of a new discipline*: 94-110. San Francisco, CA: Berret-Koehler.
383. Sydow, J., Muller-Seitz, G. & Provan, K.G. (2013). *Managing Uncertainty in Alliances and Networks - From Governance to Practice*. In T.K.Das (Ed.) Managing Knowledge in Strategic Alliances, Charlotte, NC: Information Age Publishing, pp.94-110.
384. Taleb, N.N. (2019). *Antikrhkost – stvari kojima prija nered*. Smederevo: Heliks.
385. Taleb, N.N. (2015). *Crni labud – uticaj krajnje neverovatnih zbivanja*. Smederevo: Heliks.
386. Tarrant, M. (2010). The Organisation: Risk, Resilience and Governance. *The Australian Journal of Emergency Management*. 25(2): 15-19.
387. Termeer, C. J. A. M., & van den Brink, M. A. (2013). Organizational conditions for dealing with the unknown: Illustrated by how a Dutch water management authority is preparing for climate change. *Public Management Review*, 15(1): 43–46.
388. The White House. (2010). *National Security Strategy*.
389. Therrien, M.C., Tanguay, G.A. & Beauregard- Guérin, I. (2015). Fundamental determinants of urban resilience: A search for indicators applied to public health crisis. *Resilience: International Policies, Practices and Discourses*,3(1): 18-39.
390. Thorogood, J. (2013). Is there a place for high-reliability organizations in drilling? *SPE Drilling and Completion*, 28(03): 263–269.
391. Thorogood, J. & Crichton, M.T. (2014). Threat-and-error management: the connection between process safety and practical action at the worksite. SPE Drilling and Completion, 29(04): 465–472.
392. Tilman, D. & Downing, J. (1994). Biodiversity and Stability in Grasslands. *Nature*. 367. 363-365.
393. Tjosvold, D. (1984). Effects of crisis orientation on managers' approach to controversy in decision making. *Academy of Management Journal*, 27(1): 130-138.
394. Turner, B.A. (1976). Organizational and interorganizational development of disasters. *Administrative Science Quarterly*, 21(3): 378-397.
395. Tveiten, C., Albrechtsen, E., Wærø, I. & Wahl, A. (2012). Building resilience into emergency management. Safety Science. 50: 1960–1966.
396. Tversky, A., & Kahneman, D. (1981). The framing of decisions and psychology of choice. *Science*, 211: 453-458.
397. Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*. 5: 297–323.
398. United Kingdom. Government Office for Science. (2012).*Blackett Review of High Impact LowProbability Risks*, Преузето 11.09.2020. са https://www.gov.uk/government/publications/highimpact-low-probability-risks-blackett-review
399. *Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије*, „Сл. Гласник РС, бр. 69/2022".
400. *Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије,* „Сл. Гласник РС, бр. 18/92"
401. U.S. Department of Defense. (2010). *Quadrennial Defense Review Report*.

402. U.S. Department of Homeland Security Risk Steering Committee. (2010). *DHS Risk Lexicon*. Преузето 9.10.2019 са http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.
403. U.S. Department of Homeland Security "What is Critical Infrastructure". Преузето 11.08.2019. са https://www.dhs.gov/what-critical-infrastructure
404. U.S. Nuclear Regulatory Commission. (1975*). Reactor Safety Study. An assessment of Accident Risk in U.S. Commercial Nuclear Power Plants* (Washington, NUREG-75/014).
405. US President Executive Order 13010 of July 15, 1996. (1996). *Critical Infrastructure Protection*, Federal Register, 61, 37347.
406. Välikangas, L. and Romme, A.G.L. (2012). Building resilience capabilities at "Big Brown Box, Inc.". *Strategy & Leadership*, 40: 43–45.
407. Van Der Vegt, G.S., Essens, P., Wahlström, M. & George, G. (2015). Managing risk and resilience. *Academy of Management Journal*. 58(4): 971-980.
408. Van Maaren,, I. (2022). A reference model for auditing organisational resilience. *Maandblad voor Accountancy en Bedrijfseconomie,* 96(7/8): 201-211.
409. Vidanović, I. (2006). *Rečnik socijalnog rada*. Udruženje stručnih radnika socijalnog rada Srbije.
410. Vinchon, C., Carreño, M.L., Contreras-Mojica, D.M., Kienberger, S. , Schneiderbauer, S. , Alexander, D., . . . Welle, T. (2011). *MOVE Project - Assessing vulnerability to natural hazards in Europe:From Principles to Practice - A manual on concept, methodology and tools*.
411. Vujošević, M. (1996). Primena teorije pouzdanosti u analizi rizika. u: Zbornik radova "*Tehnički sistema i sredstva zaštite od požara, eksplozija, havarija i provala*". Dunav preving, Beograd, 21-27.
412. Вукићевић, С., Видовић, М. (1995). Могућности оптимизације улагања у превентиву и интерес осигуравајућих компанија за та улагања. *Превентивно инжењерство*, III(1), 5-14.
413. Vukonjanski, J., Nikolić, M., Hadezic, O., Terek, E. & Nedeljkovic, M. (2012). Relationship between GLOBE organizational culture dimensions, job satisfaction and leader-member exchange in Serbian organizations. *Journal for East European Management Studies*, 17(3): 333-368.
414. Vogus, T. & Sutcliffe, K. (2007). Organizational Resilience: Towards a Theory and Research Agenda. *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*. 3418-3422.
415. Von Winterfeldt, D., John, R. S., & Borcherding, K. (1981). Cognitive Components of Risk Ratings. *Risk Analysis*, 1(4), 277–287.
416. Walker, S.J. (2004). *Three Mile Island: A Nuclear Crisis in Historical Perspective.* Berkeley: University of California Press.
417. Walker, B., Carpenter, J. Anderies, N. Abel, G. S. Cumming, M. Janssen, L. Lebel, J. Norberg, G. D. Peterson, & R. Pritchard. (2002). Resilience management in social-ecological systems: a working hypothesis for a participatory approach. *Conservation Ecology* 6(1): 14.
418. Walker, B, Holling, C.S., Carpenter, S. & Kinzig, A. (2003). Resilience, Adaptability and Transformability in Social-Ecological Systems. *Ecology and Society*. 9(2):5.
419. Walker, B. H., L. H. Gunderson, A. P. Kinzig, C. Folke, S. R. Carpenter, & L. Schultz. (2006). A handful of heuristics and some propositions for understanding resilience in social-ecological systems. *Ecology and Society* 11(1): 13.
420. Walker, B., & Salt, D. (Eds.) (2006). *Resilience thinking: Sustaining ecosystems and people in a changing world*. Washington DC: Island Press.
421. Walker, J. & Cooper, M. (2011). Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation. *Security Dialogue*. 42:143-160.

422. Walker, W.W., Marchau, V.A.V.J & Kwakkel, J. H. (2019). Dynamic Adaptive Planning. In: Marchau, V., Walker, W., Bloemen, P., Popper, S. (eds.) *Decision Making under Deep Uncertainty*. Springer, Cham. pp 53-69.
423. Waller M.J., Lei Z. & Pratten R. (2014). Focusing on teams in crisis management education: An integration and simulation-based approach. *Academy of Management Learning & Education*, 13(2): 208-221.
424. Wan, W.P. & Yiu, D.W. (2009). From crisis to opportunity: environmental jolt, corporate acquisitions, and firm performance. *Strategic Management Journal*, 30(7): 791-801.
425. Wan, C., Yang, Z., Zhang, D., Yan, X. & Fan, S. (2017). Resilience in transportation systems: a systematic review and future directions. *Transport Reviews*. 1-20.
426. Weick, K.E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studie*s, 25(4): 305-317.
427. Weick, K.E. (1993). The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. *Administrative Science Quarterly*, 38(4), 628-652.
428. Weick, K.E. & Roberts K.H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly*, 38(3): 357-381.
429. Weick, K. E., Sutcliffe, K. M. & Obstfeld, D. (1999). *Organizing for high reliability: Processes of collective mindfulness*. In: B. M. Staw & R. I. Sutton (Eds.), Research in organizational behavior, Greenwich, CT: JAI Press, pp. 81–123.
430. Weick, K.E. & Sutcliffe, K.M. (2006). Mindfulness and the Quality of Organizational Attention. *Organization Science*, 17(4): 514-524.
431. Weick, K.E. & Sutcliffe, K.M. (2007). *Managing the unexpected: assuring high performance in an age of complexity*, 1st edn. Jossey-Bass, San Francisco.
432. Wenger, D.E. (1992). *Emergent and volunteer behavior during disaster: Research findings and planning implications*. College Station, TX: Texas A&M University Hazard Reduction Recovery Center.
433. Wenger, D.E., Quarantelli, E.L. & Dynes R.R. (1990). Is the Incident Command System a plan for all seasons and emergency situations? *Hazard Monthly*, 10(12): 8-9.
434. White, R. P., & Shullman, S. L. (2010). Acceptance of uncertainty as an indicator of effective leadership. *Consulting Psychology Journal: Practice and Research*, 62(2), 94–104.
435. Whiteman, G. & Cooper, W.H. (2011). Ecological sensemaking. *Academy of Management Journal*, 54(5): 889-911.
436. Wildavsky, A. (1991). *Searching for Safety*, Transaction publishers, New Brunswick/Oxford, 253pp.
437. Wilkin L.& Sutton, A. (eds.) (1986) *The Management of Uncertainty: Approaches, Methods and Applications*. NATO ASI Series (D: Behavioural and Social Sciences), vol 32. Springer, Dordrecht.
438. Williams, T.A. & Shepherd, D.A. (2016). Building resilience or providing sustenance: Different paths of emerging ventures in the aftermath of the Haiti earthquake. *Academy of Management Journal*, 59: 2069-2102.
439. Williams, T.A., Gruber, D.A., Sutcliffe, K.M., Shepherd, D.A. & Zhao, E.Y. (2017). Organizational response to adversity: fusing crisis management and resilience research streams. *Academy of Management Annals*, 11(2), 733-769.
440. Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model, *Communication Monograph,* 59(4): 329–49.
441. Witte, K., & Allen, M. (2000). 'A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns', *Health Education & Behavior,* 27(5): 591–615.

442. Wucker, M. (2016). *The Gray Rhino: How to Recognize and Act on the Obvious Dangers We Ignore*. St. Martin's Press.
443. Wulandhari, N.B.I., Budhwar, P., Mishra, N., Akbar, S., Do, Q. and Milligan, G. (2022). Organizational Resilience to Supply Chain Risks During the COVID-19 Pandemic. *British Journal of Management*, Vol. 0, 1–34.
444. *Закон о критичној инфраструктури* (Сл. гласник РС бр. 87/2018).
445. *Закон о одбрани* „Сл. Гласник РС, бр. 116/2007, 88/2009, 88/2009 – др. закон, 104/2009 – др. закон, 10/2015 и 36/2018“,
446. Zimmerman, R., Restrepo, C.E. Culpen, A., Remington, W.E., Kling. A., Portelli, I., & Foltin, G.L. (2010). Risk Communication for Catastrophic Events: Results from Focus Groups, *Journal of Risk Research,* 13(7): 913–35.
447. Zobel, C. (2010). *Representing the Multi-Dimensional Nature of Disaster Resilience*. Proceedings of the 8th International ISCRAM Conference, Lisbon, Portugal.
448. Zuger, A. & Miles, S.H. (1987). Physicians, AIDS, and Occupational Risk. *JAMA: The Journal of the American Medical Association*, 258(14): 1924–28.

ПРИЛОЗИ

Прилог 1. Сектори и подсектори критичне инфраструктуре према директиви 2022/2557 ЕК

Енергетика	Електрична енергија	Продаја
Енергетика	Електрична енергија	Дистрибуција
Енергетика	Електрична енергија	Транспорт
Енергетика	Електрична енергија	Производња
Енергетика	Електрична енергија	Тржишни оператери
Енергетика	Електрична енергија	Складиштење
Енергетика	Грејање	Оператори грејања (топлане)
Енергетика	Нафта	Оператори нафтовода
Енергетика	Нафта	Производња, рафинерије, прерада, складиштење и трансмисија
Енергетика	Нафта	Централно тело за залихе
Енергетика	Гас	Продаја/снабдевање крајњих корисника
Енергетика	Гас	Дистрибуција
Енергетика	Гас	Трансмисија
Енергетика	Гас	Складиштење
Енергетика	Гас	Оператори течног природног гаса LNG
Енергетика	Гас	Производња
Енергетика	Гас	Прерада и рафинисање
Енергетика	Водоник	Производња, складиштење и трансмисија
Саобраћај	Ваздушни	Авио компаније
Саобраћај	Ваздушни	Аеродроми
Саобраћај	Ваздушни	Контрола лета
Саобраћај	Железнички	Оператори инфраструктуре
Саобраћај	Железнички	Комерцијална предузећа и оператори сервисних објеката
Саобраћај	Водни	Компаније за речни и поморски, путнички и карго саобраћај (не укључује индивидуална пловила)
Саобраћај	Водни	Луке
Саобраћај	Водни	Организације задужене за безбедност и ефикасност пловног саобраћаја
Саобраћај	Друмски	Организације/институције надлежне за управљање саобраћајем,

Саобраћај	Друмски	Оператори „интелигентног“ друмског саобраћаја
Саобраћај	Јавни превоз	Оператори јавног превоза
Банкарство	/	Кредитне институције
Тржиште финансијских инструмената		Локације трговине (Мултилатералне трговинске платформе – МТП и Организоване трговинске платформе ОТП)
Тржиште финансијских инструмената		Средишње друге уговорне стране (посредници)
Здравство		Организације здравствене заштите
Здравство		ЕУ референтне лабораторије
Здравство		Организације за истраживачке и развојне делатности у области медицинских производа
Здравство		Фармацеутске фирме
Здравство		Организације које производе медицинска средства критична у току ванредних ситуација у сектору јавног здравља
Здравство		Овлашћени дистрибутери медицинских и фармацеутских производа
Вода		Снабдевачи и дистрибутери пијаће воде
Отпадне воде		Прикупљање и одлагање или прерада отпадних вода
Дигитална инфраструктура		Центри за размену интернет саобраћаја
Дигитална инфраструктура		Пружаоци ДНС услуга (интернет домена)
Дигитална инфраструктура		Регистар назива домена РНИДС
Дигитална инфраструктура		Провајдери рачунарских услуга у „клауду“
Дигитална инфраструктура		Провајдери услуга дата центара
Дигитална инфраструктура		Провајдери мрежа за испоруку садржаја
Дигитална инфраструктура		Пружаоци услуга поверења
Дигитална инфраструктура		Пружаоци услуга јавних мрежа за електронску

		комуникацију
Дигитална инфраструктура		Пружаоци услуга мрежа за електронску комуникацију
Јавна управа		Субјекти јавне управе централне владе дефинисаних у складу са националним законима
Свемир		Оператори инфраструктуре на земљи који подржавају услуге у свемиру
Производња, прерада и дистрибуција хране		Организације које су укључене у логистику и дистрибуцију на велико, индустријска производња и прерада хране

Прилог 2. Водич за полуструктурисани интервју

Увод

Хвала Вам што сте пристали да учествујете у овом интервјуу. Наше истраживање се бави организационом отпорношћу на ризике ниске вероватноће а високог утицаја, попут пандемија, терористичких напада и природних катастрофа. Не очекујемо од вас да будете експерти за ову врсту инцидената. Нас занимају ваши погледи, пракса планирања и доношења одлука у вашој организацији и могуће реакције на овакве врсте догађаја. У овом интервјуу не постоје тачни одговори на питања.

Питања

1. Која је Ваша позиција и улога у организацији?

2. Да ли постоје формални процеси процене и управљања ризиком, кризама и континуитетом пословања? Да ли је исти сектор или особа одговорна за све ове процесе? Да ли се ти процеси обављају у складу са међународним стандардима или су у питању интерне процедуре?

3. Како се ваша организација припрема за будуће реметилачке догађаје (да ли је фокус на претње – сценарије, или на штићене вредности – утицаје)?

4. На који начин се идентификују ризици за сценарија, у смислу да ли су сценарији са највећом вероватноћом, најтежим последицама или је неки други фактор пресудан? Можете ли поменути неке од сценарија које сте идентификовали/увежбавали?

5. Колико је планирање одговора на ризик, кризу и континуитет пословања партиципативно? Да ли су сви сектори укључени или само поједини?
    a. Да ли различити сектори дају представнике за тимове континуитета пословања или кризног тима?
    b. Колико су у планирање континуитета пословања укључени запослени (просечан запослени, не члан тима за КП или кризног тима)
    c. Колико се пажње поклања сарадњи са екстерним институцијама и организацијама (МУП, БИА, здравствене институције итд) приликом планирања кризног одговора и одговора на инцидент? Да ли су оне укључене у планирање?

6. Да ли су планови управљања ризиком, кризама и континуитетом пословања адаптабилни – тј. Да ли се редовно мењају и ажурирају у случају промене у окружењу и организацији, нових научних и стручних налаза итд. Објасните укратко процес.

7. Да ли је фокус у планирању одговора усмерен на ниво организације, тимова или индивидуалном одговору запослених?

8. Да ли сматрате да су запослени довољно освешћени, обучени и спремни за одговор на кризе и које су то активности (тренинзи, обуке, процедуре) које би их додатно оснажиле?

a. Запослени у сектору безбедносних послова / корпоративне безбедности
b. Остали запослени

9. Да ли се људски, финансијски и материјални ресурси алоцирају на конкретне претње или постоје слободни ресурси за активирање у случају избијања непредвиђеног догађаја?

10. На који начин се руководило организацијом у претходним кризама – да ли се придржавало планова и процедура или се импровизовало? Да ли је то по вашем мишљењу било ефикасно или сматрате да би другачији приступ био адекватнији?

11. Како се запосленима комуницирају идентификовани ризици и планирани одговор? Да ли је комуникација двосмерна, тј. да ли се уважава повратна информација при планирању сценарија-одговора?

12. Како сте комуницирали са запосленима у току озбиљних инцидената и криза? Да ли је комуникација била двосмерна и колико је повратна информација запослених утицала на измену и унапређивање одговора?

13. По Вашем мишљењу, на који начин можете унапредити организациони одговор на непредвиђени негативни догађај или кризу?

14. Можете ли нам објаснити процес припреме, одговора и опоравка на пандемију COVID-19:
    a. Да ли се пандемија налазила у регистру ризика и да ли је по вашем мишљењу организација била приправна за одговор?
    b. У ком тренутку је било јасно да ће COVID-19 прерасти у пандемију и имати велики утицај на пословање.
    c. Да ли су се планови одговора на кризу и континуитет пословања мењали и ревидирали у току пандемије? Који су били разлози за то?
    d. Да ли је било случајева учесталог изостанка са радног места већег броја запослених током пандемије COVID-19? Који су били узроци и образложења. На који начин се реаговало? Да ли је одговор био адекватан?
    e. Које су научене лекције из пандемије у смислу приправности и одговора на будућу пандемијску кризу?

15. Да ли бисте додали нешто што сматрате да би било релевантно а није покривено претходним питањима?

16. Да ли имате нека питања за мене?

БИОГРАФИЈА АУТОРА

Владимир Нинковић је рођен 9. новембра 1981. године у Београду. XIV београдску гимназију завршио је 2000. године. Основне академске студије завршио је на Филолошком факултету Универзитета у Београду са просечном оценом 7,87. Специјалистичке струковне студије кризног менаџмента завршио је 2006. године на Факултету безбедности – са просечном оценом 9.24. Дипломске академске студије – мастер из области социолингвистике завршио је на Филолошком факултету, са просечном оценом 9.60.

Током 2015-2016. године био је ангажован као истраживач на пројекту: Отпорност заштите критичне инфраструктуре у Европи (RECIPE) који је финансирао Генерални директорат за хуманитарну помоћ и цивилну заштиту Европске Уније (ECHO). Такође, 2018. и 2019. године био је ангажован као истраживач на европском Horizon 2020 пројекту PopRebel (Populism in Central and Eastern Europe). Запослен је као регионални менаџер безбедности задужен за регион Африке у компанији DAI LLC. Такође, волонтерски обавља функцију генералног секретара Крикет федерације Србије.

Као аутор или коаутор објавио је двадесетак научних радова и две научне монографије из области студија безбедности, са посебним нагласком на теме везане за менаџмент ризиком, менаџмент континуитетом пословања и заштиту критичне инфраструктуре.

Изјава о ауторству

Име и презиме аутора: Владимир Нинковић

Број индекса: 10/14

Изјављујем

да је докторска дисертација под насловом

„Отпорност критичне инфраструктуре на нерутинске ризике“

• резултат сопственог истраживачког рада;

• да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;

• да су резултати коректно наведени и

• да нисам кршио ауторска права и користио интелектуалну својину других лица.

У Београду, 28.10.2024. **Потпис аутора**

_____

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора: Владимир Нинковић

Број индекса: 10/14

Студијски програм: Студије наука безбедности

Наслов рада: Отпорност критичне инфраструктуре на нерутинске ризике

Ментор: Проф. Др Зоран Кековић

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао ради похрањивања у Дигиталном репозиторијуму Универзитета у Београду.

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, 28.10.2024.

_____

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом: „Отпорност критичне инфраструктуре на нерутинске ризике“ која је моје ауторско дело.

Дисертацију са свим прилозима предао сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио.

1. Ауторство (CC BY)

2. Ауторство – некомерцијално (CC BY-NC)

3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)

4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)

5. Ауторство – без прерада (CC BY-ND)

6. Ауторство – делити под истим условима (CC BY-SA)

Потпис аутора

У Београду, 28.10.2024.

_____

1. Ауторство. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. Ауторство – некомерцијално. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. Ауторство – некомерцијално – без прерада. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. Ауторство – некомерцијално – делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. Ауторство – без прерада. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. Ауторство – делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.