УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

Јана М. Марковић

КОРПОРАТИВНА БЕЗБЕДНОСТ КАО ЕЛЕМЕНТ СИСТЕМА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ У ЗАШТИТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ РЕПУБЛИКЕ СРБИЈЕ

докторска дисертација

Београд, 2025.

UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

Jana M. Marković

CORPORATE SECURITY AS AN ELEMENT OF THE NATIONAL SECURITY SYSTEM IN THE PROTECTION OF THE CRITICAL INFRASTRUCTURE OF THE REPUBLIC OF SERBIA

Doctoral Dissertation

Belgrade, 2025

Подаци о ментору и члановима комисије

Ментор:

Проф. др Горан Ј. Мандић, ванредни професор,
Универзитет у Београду – Факултет безбедности

Чланови комисије:

Проф. др Петар Станојевић, редовни професор,
Универзитет у Београду – Факултет безбедности, председник

Проф. др Младен Милошевић, редовни професор,
Универзитет у Београду – Факултет безбедности, члан

Доц. др Ненад Радивојевић, доцент,
Универзитет у Новом Саду – Правни факултет, члан

Датум одбране: _____

КОРПОРАТИВНА БЕЗБЕДНОСТ КАО ЕЛЕМЕНТ СИСТЕМА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ У ЗАШТИТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ РЕПУБЛИКЕ СРБИЈЕ

САЖЕТАК

Транснационални карактер савремених безбедносних изазова, ризика и претњи ствара бројније и сложеније проблеме очувања и јачања националне безбедности. Иако је држава дуго времена била једини носилац функције (националне) безбедности, сада је национална безбедност одговорност како државе и владе, тако и приватних субјеката. Једна од области у којој се одговорност дели између државе и приватних субјеката јесте заштита критичне инфраструктуре. Корпоративна безбедност, са једне стране успостављена у правним лицима укључујући и правна лица критичне инфраструктуре и са друге стране, део индустрије приватне безбедности завређује све већу пажњу у научним и стручним круговима. Интензивирају се расправе које се воде у вези са концептом корпоративне безбедности, њеном организацијом и функцијом, делокругу послова који јој припадају, сарадњи са другим субјектима укључујући и субјекте са којима заједно обавља функцију безбедности, у првом реду са полицијом. У истраживању се полази од става да корпоративна безбедност припада области приватне безбедности и да је као таква формално заступљена у систему националне безбедности, те кроз своју фукцију доприноси и позитивно утиче на повећање стања националне безбедности. У истраживању су проучавани место и улога корпоративне безбедности у систему националне безбедности, као и њен допринос истом систему и то са аспекта заштите критичне инфраструктуре. Из наведеног, области које су проучаване јесу национална безбедност и систем националне безбедности, корпоративна безбедност и критична инфраструктура и њена заштита. Истраживањем које је спроведено користећи секундарну анализу података и експертски интервју добијени су налази о тренутном стању проучаваних области на подручју Републике Србије. Синтеза добијених налаза представљена је кроз сва поглавља и то на следећи начин: резултати анализе нормативних аката који уређују проучаване области представљени по поглављима који су посвећени тим областима, а резултати експертског интервјуа представљени су у посебном поглављу кроз Дискусију.

Кључне речи: национална безбедност, приватна безбедност, корпоративна безбедност, критична инфраструктура, заштита критичне инфраструктуре, Република Србија

Научна област: друштвене науке

Ужа научна област: науке о безбедности

CORPORATE SECURITY AS AN ELEMENT OF THE NATIONAL SECURITY SYSTEM IN THE PROTECTION OF THE CRITICAL INFRASTRUCTURE OF THE REPUBLIC OF SERBIA

SUMMARY

The transnational nature of contemporary security challenges, risks, and threats creates numerous and increasingly complex problems in maintaining and strengthening national security. Although the state has long been the sole bearer of the (national) security function, national security is now the responsibility of both the state and the government, as well as private entities. One of the areas where responsibility is shared between the state and private entities is the protection of critical infrastructure. Corporate security, on the one hand, established in legal entities, including those related to critical infrastructure, and on the other hand, as part of the private security industry, is receiving growing attention in academic and professional circles. Discussions are intensifying regarding the concept of corporate security, its organization and function, the scope of tasks it encompasses, and its cooperation with other entities, including those with which it shares security functions, primarily the police. The research starts from the premise that corporate security belongs to the field of private security and, as such, is formally represented in the national security system, thereby contributing to and positively influencing the enhancement of national security. The research explored the role and position of corporate security within the national security system, as well as its contribution to this system, particularly from the perspective of critical infrastructure protection. The areas studied include national security and the national security system, corporate security, and critical infrastructure and its protection. The research, conducted using secondary data analysis and expert interviews, yielded findings on the current state of the studied areas in the Republic of Serbia. The synthesis of the obtained findings is presented across all chapters as follows: the results of the analysis of normative acts regulating the studied areas are presented in chapters dedicated to these areas, and the results of the expert interview are presented in a separate chapter through the Discussion.

Key words: National security, Private security, Corporate security, Critical infrastructure, Critical infrastructure protection, Republic of Serbia

Scientific field: Social Sciences

Scientific subfield: Security Sciences

САДРЖАЈ

1. УВОДНА РАЗМАТРАЊА 1

1.1. Теоријско-појмовни оквир истраживања 4

1.1.1. Теорија система 4

1.1.1.1. Систем националне безбедности 10

1.1.1.2. Елементи система националне безбедности 11

1.1.1.3. Обележја система националне безбедности 14

1.1.2. Појмовни оквир истраживања 16

1.1.2.1. Појам безбедности 16

1.1.2.2. Појам корпорације 20

1.1.2.3. Појам корпоративне безбедности 22

1.1.2.4. Концепти критичне инфраструктуре и њене заштите 24

1.1.3. Проблем, предмет и циљ истраживања 25

1.1.3.1. Проблем истраживања 30

1.1.3.2. Предмет истраживања 34

1.1.3.3. Циљ истраживања 35

1.1.4. Истраживачка питања 35

1.1.4.1. Варијабле 36

1.1.4.2. Индикатори 38

1.2. Методолошки оквир истраживања 42

1.2.1. Тип истраживања 42

1.2.2. Тип и извори података 42

1.2.3. Методе за прикупљање података 43

1.2.3.1. Преглед литературе 43

1.2.3.2. Секундарна анализа података 44

1.2.3.3. Експертски интервју 45

1.2.4. Просторни и временски оквир истраживања 46

1.3. Структура дисертације 47

2. НАЦИОНАЛНА БЕЗБЕДНОСТ И СИСТЕМ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ 49

2.1. Теоријске основе националне безбедности 49

2.2. Општа разматрања о систему националне безбедности 53

2.3. Систем унутрашње безбедности као извршни део система националне безбедности 55

2.4. Јавна и приватна безбедност у систему националне безбедности 57

2.5. Национална безбедност и систем националне безбедности Републике Србије – начин организовања система националне безбедности 61

2.5.1. Однос система националне безбедности према корпоративној/ приватној безбедности 63

3. КОРПОРАТИВНА БЕЗБЕДНОСТ 65

3.1. Корпорација као референтни објекат корпоративне безбедности 65

3.2. Генеза корпоративне безбедности 69

3.2.1. Настанак и развој приватне безбедности 69

3.2.1.1. Приватизација послова безбедности 72

3.2.1.2. Укупни економски утицај сектора приватног обезбеђења данас 75

3.2.2. Развој корпоративне безбедности 76

3.3. Корпоративна безбедност као део индустрије приватне безбедности 78

3.3.1. Приватне безбедносне компаније 80

3.3.1.1. Приватне безбедносне компаније и корпоративна безбедност 82

3.3.2. Приватне детективске компаније 82

3.3.3. Приватне војне компаније 84

3.3.3.1. Приватне војне компаније и приватне безбедносне компаније 86

3.4. Корпоративна безбедност – дефинисање појма 87

3.4.1. Корпоративна безбедност као систем 88

3.4.2. Корпоративна безбедност као организација 89

3.4.3. Корпоративна безбедност као пословна функција 90

3.4.4. Корпоративна безбедност као својство 92

3.5. Корпоративна безбедност и њој сличне гране безбедности 94

3.6. Функције корпоративне безбедности 96

3.7. Корпоративна безбедност у служби друштвено одговорног пословања 98

3.7.1. Појам друштвено одговорног пословања 99

3.7.2. Допринос корпоративне безбедности друштвено одговорном пословању 100

3.8. Корпоративна безбедност у Републици Србији – правни оквир организације и функционисања корпоративне безбедности 103

3.8.1. Физичка и техничка заштита 104

3.8.2. Безбедност података и информација 108

3.8.3. Људски ресурси и безбедност запослених 114

3.8.3.1. Људски ресурси као организациона целина правног лица 114

3.8.3.2. Људски ресурси и безбедност запослених као функција корпоративне безбедности 115

3.8.4. Безбедност и здравље на раду 122

3.8.5. Заштита животне средине 125

3.8.6. Управљање ризиком од катастрофа и ванредним ситуацијама 127

3.8.7. Заштита од пожара ... 130
3.8.8. Остали нормативни прописи од значаја за безбедност и функционисање организације ... 131
4. КРИТИЧНА ИНФРАСТРУКТУРА И ЊЕНА ЗАШТИТА ... 135
4.1. Појмовно одређење критичне инфраструктуре и њене заштите ... 136
4.1.1. Идентификација критичне инфраструктуре ... 143
4.1.2. Отпорност, рањивост и међузависност као кључна својства критичне инфраструктуре ... 148
4.1.2.1. Отпорност критичне инфраструктуре ... 148
4.1.2.2. Индекс (мерења) отпорности критичне инфраструктуре ... 150
4.1.2.3. Рањивост критичне инфраструктуре ... 153
4.1.2.4. Међузависност критичне инфраструктуре ... 154
4.1.3. Угрожавање критичне инфраструктуре са освртом на економске последице ... 157
4.1.4. Заштита критичне инфраструктуре ... 161
4.1.4.1. Индекс мера заштите критичне инфраструктуре ... 164
4.1.4.2. Безбедност као аспект заштите критичне инфраструктуре ... 167
4.1.4.3. Заштита критичне инфраструктуре као елемент тоталне одбране ... 170
4.2. Критична инфраструктура и њена заштита у Републици Србији ... 172
4.2.1. Развој заштите критичне инфраструктуре у Републици Србији ... 172
4.2.2. Нормативни оквир заштите критичне инфраструктуре у Републици Србији – тренутно стање ... 179
5. ДИСКУСИЈА ... 189
5.1. Допринос корпоративне безбедности националној безбедности Републике Србије са аспекта заштите критичне инфраструктуре ... 189
5.1.1. Сумирани налази истраживања кроз помоћна истраживачка питања другог нивоа ... 202
5.2. Препоруке за развој доприноса корпоративне безбедности националној безбедности са акцентом на заштиту критичне инфраструктуре ... 204
5.3. Ограничења дисертације и могућности за даља истраживања ... 215
6. ЗАКЉУЧНА РАЗМАТРАЊА ... 217
7. БИБЛИОГРАФИЈА ... 221
8. ПРИЛОЗИ ... 255
8.1. Прилог 1: Правна лица (велики технички системи од значаја за одбрану (критична инфраструктура)) која су обухваћена истраживањем ... 255
8.2. Прилог 2: Иницијална питања за експертски интервју са руководиоцима на пословима безбедности у великим техничким системима од значаја за одбрану (критична инфраструктура) ... 255
9. БИОГРАФИЈА КАНДИДАТКИЊЕ ... 258

Попис коришћених табела и илустрација

Табеле:

Табела 1: Индикатори (Ауторка) 38

Табела 2: Нека одређења националне безбедности у страној литератури (Buzan, 1991, pp. 16-17) 50

Табела 3: Нека одређења националне безбедности у домаћој литератури (Ауторка) 51

Табела 4: Дефиниције система националне безбедности (Ауторка) 54

Табела 5: Приказ начина на који различити аутори схватају корпоративну безбедност (Ауторка) 93

Табела 6: Категоризација сектора критичне инфраструктуре (прилагођено према Weber, Pericàs Riera and Laumann, 2023, pp. 7-8) 146

Табела 7: Компоненте Индекса отпорности по нивоима (Fisher et al., 2010) 151

Табела 8: Компоненте Индекса мерења отпорности по нивоима (Petit, Bassett, Black et al., 2013) 152

Табела 9: Заштитне мере критичне инфраструктуре по нивоима (Petit, Bassett, Buehring et al., 2013) 164

Табела 10. Препоруке за развој корпоративне безбедности (Ауторка) 208

Табела 11: Препоруке за развој заштите критичне инфраструктуре (Ауторка) 212

Илустрације:

Илустрација 1: Графички приказ отвореног система (Ауторка) 7

Илустрација 2: Основни и изведени појмови (Ауторка) 19

Илустрација 3: Режим рада корпоративне безбедности у организацији (Ауторка) 32

Илустрација 4: Приказ односа варијабли (Ауторка) 37

Илустрација 5: Приказ индустрије приватне безбедности (Ауторка) 80

Илустрација 6: Међузависности услуга и мрежа (NARUC, 2005 према OECD, 2019) 155

Илустрација 7: Процес заштите критичне инфраструктуре (Tagarev and Pavlov, 2007, p. 42) 162

1. УВОДНА РАЗМАТРАЊА

Безбедност државе и њених конститутивних елемената – територије, становништва и суверенитета, постиже се у првом реду ефикасним системом националне безбедности. Замишљен као апарат за достизање и одржавање оптималног нивоа безбедности у држави, систем националне безбедности обухвата скуп функционално повезаних ентитета, који делујући у складу са правним поретком државе теже да заштите унутрашњу и спољну безбедност државе и њених конститутивних елемената. Успостављен превасходно да обезбеди минимум опстанка државе, систем националне безбедности развијао се паралелно са појавом нових и усложњавањем постојећих безбедносних изазова, ризика и претњи. За последицу таквих промена национална држава добила је системе националне безбедности комплексније него икада раније. Ипак, напредак у развоју државе и њеног апарата безбедности у једном тренутку развоја био је суочен са извесним потешкоћама попут преоптерећености националних буџета, као и проблема са којима су се суочавали органи унутрашње безбедности. Органи, који су били надлежни за послове унутрашње безбедности (првенствено одржавање реда и мира), неспремно су дочекали трансформацију савремених безбедносних изазова и показали се као недовољни да одговоре на њих. Под таквим околностима, дошло је до „приватизације“ послова безбедности, што је за своју последицу имало формирање приватног сектора безбедности и развој јавно-приватног партнерства у сектору безбедности, које треба да послужи као институционално окружење за усклађивање приватних и јавних интереса и одговорности у сектору безбедности.[1] Полиција, као традиционални носилац јавне безбедности, није изгубила своју улогу већ ју је модификовала. Она је добила „улогу субјекта који делује селективно, усредсређујући се на одређене („најопасније“) облике угрожавања, док је друштву укључујући и приватни сектор, остављено да се стара о оним, другим, „мање опасним“ угрожавањима“ (Стајић и Мандић, 2014, стр. 132; Стајић и Радивојевић, 2017, стр. 153). Приватизација послова безбедности била је праћена „маркетизацијом јавне управе“ (Unijat i dr., 2008, str. 26), односно такозваним *Outsourcing*-ом послова безбедности које је до тада извршавао јавни сектор, односно полиција.

Приватна безбедност има дугу историју. Са једне стране, појединци и организације имале су потребу да заштите своју имовину и/или пословање у обиму који је превазилазио обавезе државних служби (полиције) које су заштиту требале да обезбеде. Под таквим околностима, појављују се ентитети који су се старали о безбедности унутар организација у којима су успостављени. Уз њих, појављују се и ентитети који су пружали услуге безбедности свима који су исте могли да плате без обзира да ли је реч о појединцима којима је требала лична или заштита имовине или о организацијама којима је требала заштита имовине и пословања. Сасвим је сигурно да су организације (корпорације) од свог настанка тежиле заштити сопствених вредности и опстанку на тржишту рада. Са друге стране, како због финансијских и разлога технолошке природе тако и због увећања и усложњавања задатака постављених у сфери националне безбедности део послова који је до тада био у искључивој надлежности државе и њених органа и служби почео је да се преноси на субјекте приватне безбедности. Део послова које је полиција (као традиционални носилац унутрашње и јавне безбедности) из свог

[1] Генерално посматрано, приватни свет не може пословати, а да не разуме и поштује политике влада и јавног сектора, док владе не могу више самостално да решавају друштвене проблеме укључујући и оне безбедносне природе.

делокруга рада пренела на друге државне и приватне актере могао би се сматрати „пренетим“ делом посла и тумачити као зона преклапања јавне и приватне безбедности. Иако корени приватне безбедности сежу далеко у људску историју, тек са настанком ових субјеката чије су активности директно или посредно увезане са безбедносном функцијом државе, односно њеним системом националне безбедности, могло се говорити о приватној безбедности (Марковић, 2023а). За тај прелаз се обично узима период деветнаестог века и оснивања првих приватних безбедносних компанија. Сумирано, поред јавне или традиционалне полиције, успостављена је приватна полиција познатија као приватна безбедност, и „радна полиција“ (Button, 2016, p. 56) као манифестација корпоративне безбедности.

Ослабљено је традиционално схватање националне безбедности, засновано на концепту суверенитета. Савремена држава остала је у једном тренутку принуђена да преиспита и редефинише концепте безбедности на националном нивоу (Pejanović, Stojanović and Komarčević, 2018, p. 241) уврстивши у субјекте националне безбедности и субјекте приватне безбедности. Уз то, мада има изузетака (Brooks, 2013; George and Kimber, 2014), корпоративну безбедност могуће је посматрати управо као део те приватне безбедности, односно приватног сектора безбедности.

Безбедност грађана и имовине престала је да буде искључива одговорност државе. Увећање броја облика и носилаца угрожавања, као и метода и средстава угрожавања довело је до процеса реорганизовања и прилагођавања постојећих система националне и јавне безбедности (Стајић и Радивојевић, 2017, стр. 169). Иако се у научним круговима препознаје ова тенденција, Карен Петерсен (*Karen Petersen*) упозорава да „још увек недостаје разумевање како приватне организације концептуализују своју улогу у националној безбедности“ (2014, p. 79). Ипак, могло би се рећи да тамо где су организација и функције корпоративне безбедности успостављене тамо постоји разумевање значаја корпоративне безбедности како за економску, тако и за националну безбедност.

Зашто постоји потреба да се говори о корпоративној безбедности у домену система националне безбедности? Према Слободану Марковићу, корпоративна безбедност препозната је као елемент савремене државе, док је корпоративни сектор препознат као субјекат који има интереса у националној безбедности (2007, str. 44). Корпоративна безбедност је саставна компонента националне безбедности (Мијалковић и Бошковић, 2010, стр. 289). Уколико се истакне циљ корпоративне безбедности, а то је заштита вредности корпорација, почињу да се попримају обриси делимичног одговора. Својим механизмима корпоративна безбедност директно утиче на заштиту сопствених интереса и унапређењу позиције и статуса, и индиректно доприноси задовољењу потреба друштва и државе (Мијалковић и Бошковић, 2010, стр. 289; Marjanović i Ćupić, 2017, str. 501). Заштитом сопствених вредности, уклањањем недостатака, улагањем у превенцију и ефикасан правовремени одговор организација опстаје на тржишту и својим (правно регулисаним) пословањем доприноси вредностима појединаца, вредностима локалне, националне и сваке друге, шире заједнице. Друштвене промене захтевају од организација стварање сигурних услова за опстанак и напредак на тржишту рада. Организације које успешно послују имају значајну улогу у економским процесима земље. Поред тога, корпоративна безбедност је „основна полуга развоја конкурентске способности компаније, а самим тим и развоја целокупног друштва“ (Николић и Синковски, 2013, стр. 127). Искуство показује да успешно пословање доприноси стабилизацији економске ситуације унутар одређене земље, ефикасном коришћењу расположивих ресурса, задовољавању интереса становништва (Shyra et al., 2021, p. 211). Једно емпиријско истраживање показало је да корпоративна безбедност има велики или средњи утицај на економску моћ државе и стабилност националне економије и то у областима као што су заштита података, корупција и „прање новца“, превенција унутрашњих сукоба у држави. У

закључцима истраживања истакнуто је да што су „компаније успешније то је држава јача, што значи мање унутрашњих сукоба и боље стање националне безбедности" (Trivan, 2013, pp. 93-94). Улажући у сопствену безбедност, организације штите свој посао, а „посао је машина за снажну економију" (Bergin, Williams and De Wilde, 2019, p. 6). Значај националне привреде за националну безбедност разлог је њене „десекуритизације" што је условило и развој концепта корпоративне безбедности (Мијалковић и Бошковић, 2010, стр. 289), па корпоративна безбедност није ништа друго него „повезаност безбедности као атрибута државе са њеном економијом, јер као што је економија неопходан чинилац безбедности, тако је и безбедност услов стабилне економије" (Savić, 2008, str. 20). Стабилна економија један је од предуслова одбрамбене способности државе. Економска безбедност притом није ништа мање но основ националне безбедности.[2] Из тог разлога, корпоративна безбедност представља „уску везу између безбедности као атрибута државе и њене економије, односно означава њихову међузависност" (Ђукић, 2018, стр. 224). Уз то, не сме се изгубити са ума чињеница да је организација која послује на одређеном тржишту уједно и битан елемент јавне политике и свакако један од субјеката политичког система који је успостављен на том тржишту или тржиштима. Циљ корпоративне безбедности у наведеном контексту је најмање двострук: 1) заштита сопствених интереса и унапређење личне позиције конкурентном привредном окружењу и 2) омогућавање друштву и држави да задовоље своје потребе (Мијалковић и Бошковић, 2010, стр. 292). Дакле, организација делује у два правца, пре унутра и према споља. Према унутра, она се стара о профиту и уједно штити себе од свих угрожавајућих фактора. Према споља, она је увек економски и политички субјекат у окружењу у којем послује.

Научни допринос овог истраживања усмерен је на откриће неких нових чињеница у вези са предметом истраживања. Научни допринос огледа се у изналажењу сазнања о доприносу које корпоративна безбедност има у систему националне безбедности, и посредно на целокупну безбедност државе, националне вредности и интересе. Досадашње студије су указале на то да је корпоративна безбедност интегрисана у националну безбедност, али не пружају систематичан увид у начине на који корпоративна безбедност својим функцијама заиста доприноси националној безбедности и очувању критичне инфраструктуре, и посредством ње – оптималном функционисању државе и друштва. Ово истраживање, посредством свеобухватног прегледа теоријских сазнања о феноменологији и етиологији корпоративне безбедности, нуди синтезу знања о настанку и развоју корпоративне безбедности, њеним карактеристикама, месту и улози коју има у систему националне безбедности и њеном доприносу националној безбедности чиме доприноси увећању научног фонда у наукама о безбедности.

Друштвена оправданост дисертације огледа се у доприносу у разумевању феномена корпоративне безбедности којем и даље у Републици Србији није посвећена пажња какву заврређује. Резултати истраживања нуде увид у тренутно стање корпоративне безбедности у Републици Србији стварајући простор за стимулисање даљих и продубљених дискусија како на државном нивоу, тако и у научним и стручним круговима. Резултати истраживања могу да се користе као основ за унапређивање правног оквира којим би се омогућило веће искоришћавање потенцијала корпоративне безбедности у заштити критичне инфраструктуре и других инфраструктурних система на којима почива функционисање државе и њеног друштва, за формулацију и имплементацију бољих политика у овој области, дефинисање препорука за даљи развој корпоративне безбедности и унапређивање њеног доприноса националној безбедности, националним вредностима и интересима Републике Србије. Поред доносилаца стратешких одлука у

[2] Треба притом имати у виду и то да „као што војна моћ није једини показатељ безбедности, тако ни развијена економија није показатељ свеукупног развоја државе, већ само економске безбедности" (Мишев, 2022, стр. 116), као једне компоненте целокупне безбедности државе.

области националне безбедности, резултате истраживања послужиће и стручњацима из области безбедности, као и научним институцијама зарад унапређењивања наставних програма и спровођења додатних истраживања.

Корпоративна безбедност, иако нова област у наукама о безбедности, ипак представља на завидном нивоу развијен систем мултидисциплинарних знања из области безбедности применљив на пословне и уопште организационе системе савременог друштва. Отуда потреба да се систематизују знања из области безбедности и области пословања и функционисања организација те као таква пренесу са теоријског на практични ниво менаџмента организација.

1.1. Теоријско-појмовни оквир истраживања

У дисертацији ће бити коришћен теоријско-појмовни оквир који је у вези са предметом истраживања. Теоријски оквир истраживања нуди увид у теоријске поставке од којих се полази у истраживању, док мрежа појмова, заснована на етаблираној групи појмова развијених у оквиру наука о безбедности, расветљава неке од средишњих концепата ове дисертације представљајући различита одређења ових појмова која се могу пронаћи у релевантној литератури.

Појмови на које је примењен теоријски оквир изабран за дисертацију приказани су од општијег – систем националне безбедности, ка посебном – систем корпоративне безбедности, с тим да је систем националне безбедности са елементима и обележјима једини појам који је обрађен у оквиру теоријског оквира с обзиром на логичку повезаност која постоји. Сви појмови су представљени редоследом који одговара њиховој тематизацији кроз дисертацију. Осим ова два наведена појма, обухваћени су и следећи: безбедност, национална безбедност, корпоративна безбедност, менаџер безбедности, критична инфраструктура, заштита критичне инфраструктуре. Појмовни оквир на овом месту представља увод у истраживање, те ће сви појмови релевантни за истраживање бити предмет прецизније и обухватније анализе која ће уследити у наредним поглављима.

1.1.1. Теорија система

> *„Елемент не постаје саставни део система на основу својих својстава, односно карактеристика, већ на основу вредности (доприноса) коју има за систем“*
> (Савић, Станковић и Јанаћковић, 2021, стр. 9).

Развој теорија система могуће је пратити кроз главне токове ове научне дисциплине који обухватају општу теорију система, теорију живих система, теорију математичких система, кибернетику, теорију друштвених система и теорију филозофских система (Adams, Hester and Bradley, 2013). За потребе овог истраживања одабрана је општа теорија система. Према општој теорији система могуће је оријентисати општу теорију друштвених система која је „општа“ због универзалног контекста, јер се „сваки друштвени контакт схвата као систем“ (Luman, 2011, str. 52). Теорија система одабрана је јер пружа структурирани приступ разумевању и управљању сложеним, међусобно повезаним елементима који конституишу систем националне безбедности, као и ниже системе попут система приватне и корпоративне безбедности. Превасходно, значајни су холистички приступ и међусобна повезаност елемената који подвлаче законитост међусобног деловања и утицаја компоненти система националне безбедности једних на друге стварајући целину која ефикасно делује.

Општа теорија система јесте наука о настанку, развоју и управљању системима. Зачетке ове теорије могуће је пронаћи у радовима америчког психолога Андраса Анђала (*Andras Angyal),* који је сматрао да за изучавање сложених појава треба увести нову категорију, коју назива „систем“ (Савић, Станковић и Јанаћковић, 2021, стр. 9-10). У истом периоду са развојем ове идеје, аустријски биолог Лудвиг фон Берталанфи (*Ludwig von Bertalanffy*) поставља теорију отворених система којом доприноси развоју ове дисциплине. Миленковић сматра ипак да претечу опште теорије система треба тражити још у радовима Талкота Парсонса (*Talcott Parsons*), на кога се касније надовезује „можда и најзначајнији представник опште теорије система“ Никлас Луман (*Niklas Luhmann*) (Milenković, 2019, str. 45).

За општу теорију система Лудвиг фон Берталанфи (*Ludwig von Bertalanffy*) наводи да представља „логичко-математичку дисциплину, која је сама по себи чисто формална, али је применљива на све науке које се баве системима“ те се стога појављује као „методолошки, важно средство за контролу и подстицање преноса принципа из једне области у другу“ тако да више не долази до дуплирања „открића истих принципа у различитим областима изолованим једна од друге“ (1950, p. 139). Слично, Кенет Болдинг (*Kenneth Boulding*) ову теорију одређује као „костур науке у смислу да служи за обезбеђивање оквира или структуре система на којима се могу окачити месо и крв одређених дисциплина и одређених тема у уређеном и кохерентном корпусу знања“ (1956, p. 208). Дакле, реч је о теоријском оквиру који омогућава мултидисциплинарни приступ у проучавању система остављајући довољно простора да се о системима и другим појавама везаним за њих говори језицима различитих области интересовања комбинујући и на тој основи развијајући корпус научног сазнања о овим појавама.

Временом, општа теорија система уобличена је у теорију система. Као разлоге за то, могуће је издвојити следеће: најпре, све се мање говори о општој или „уједињеној теорији система“ (енг. *Unified Systems Theory*) (Jackson, 1994, p. 226); друго, општа теорија система је једна од системских теорија, а било је потребно услед развоја ове дисциплине пронаћи заједнички именитељ за њих и треће, у примени ове теорије јавили су се извесни недостаци (Савић, Станковић и Јанаћковић, 2021, стр. 13).

Теорија система је више „теоријски оквир и скуп методолошких алата који се могу применити на било коју област проучавања“ него сама теорија (Buckley, 1998, p. 3). Она представља „јединствену групу специфичних пропозиција које су окупљене да помогну у разумевању система, позивајући се на побољшану моћ објашњења и тумачење са великим импликацијама за практичаре система“ (Adams et al., 2014, p. 113).

Захваљујући томе што је указала и доказала објективно постојање системских законитости, општа теорија система допринела је „развоју опште методологије проучавања сложених динамичких система и интеграцији знања јер се проблеми стварности проучавају као интеракција различитих система и подсистема“ (Šijan, Karabaševič i Rajčević, 2019, str. 92). Теорија система добила је своју примену у бројним научним дисциплинама. Њен појмовни апарат и приступ проучавању система без обзира да ли је реч о природним, биолошким или друштвеним, обезбедио јој је примену и у наукама о безбедности.

Идеја о системима потиче још из античког периода, а у модерној науци се јавља код Честера Бернарда (*Chester Barnard*) и касније Норберта Винера (*Norbert Wiener*) који је „дефинисао кључне термине – улаз, процес, излаз и повратна спрега – и начинио схему која се и данас користи у приказивању суштине система“ (Драгишић, 2011, стр. 17). Берталанфи систем дефинише као „скуп елемената који су у међусобној интеракцији“ (von Bertalanffy, 1968, pp. 33, 55). Он указује на то да поредак или организација целине или система није ништа метафизичко или филозофско, већ је то чињеница (von

Bertalanffy, 1972, p. 408). То је „интегрисана колекција компоненти или елемената дизајнираних да постигну циљ према плану“ (Garcia, 2001, p. 6), „скуп различитих елемената који функционишу као складна целина ради остварења неког циља“ (Стевановић и Субошић, 2007, стр. 15). Организација или систем јесте „општа идеја скупа предмета, елемената или делова одређене стварности, које треба схватити у њиховом међусобном споју који чини сврсисходну целину, и од којих сваки (додала ауторка: предмет, елемент или део) своје значење добија у зависности од места које заузима у тој целини“ (Кековић и Димитријевић, 2017, стр. 50).

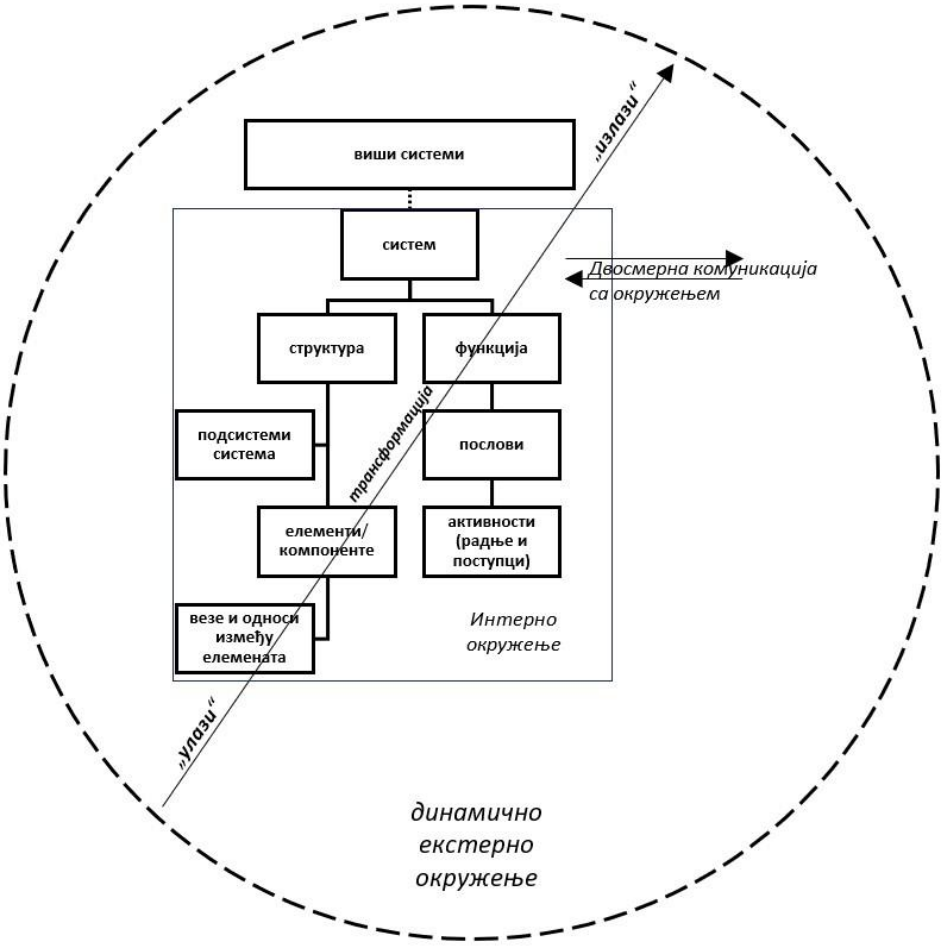
Посебан допринос у разумевању система даје Никлас Луман (*Niklas Luman*) предлажући да друштвени феномени као што су интеракције, организације или друштва буду схваћени као системи. Према њему, системи су функционална конструкција елемената која има прописане границе и окружење и не могу постојати без организације (2011). Према класификацији система коју је дао Болдинг, трећи велики светски систем је друштвени систем у који спада и организација (Boulding, 1985, p. 8). С тим у вези, свака организација јесте организациони систем или систем – у даљем тексту користиће се термин систем уважавајући теорију система.

Системи које је човек створио својим деловањем са циљем да служе свом окружењу називају се организационим системима. Због фактора људског деловања, називају се још и друштвеним системима, и означавају целину састављену од „разноврсних елемената или сазнања“, чија је сврха остварење „неког друштвеног циља“ (Стајић, 2015, стр. 40).[3] Ипак, уместо да буде реч о целини, за двојицу аутора систем се може објаснити само као тоталитет (Kast and Rosenzweig, 1972, p. 450).

Тако се системски приступ организацији заснива на општој теорији система (Dulanović i Džinović, 1995, str. 68). Системски приступ организацији појавио се услед усложњавања организација и све веће неизвесности њеног окружења (Савић, Станковић и Јанаћковић, 2021, стр. 79). Организацију је могуће посматрати као систем, односно функционални тоталитет елемената који су у међусобној интеракцији и интеракцији са окружењем. Односно реч је о отвореном систему који се може посматрати као целина коју карактеришу подцелине/подсистеми, њихова структурална повезаност, функционалне везе, унутрашња интеракција између елемената система и њихова интеракција са окружењем (Драгишић и Радојевић, 2014, стр. 40).

Свака организација као систем припада вишем систему, и уједно се састоји од мањих (под)система. Наиме, сваки систем чини структура и функција. Структуру система чине подсистеми који обухватају елементе или компоненте система који су међусобно повезани те су успостављени односи међу елементима или компонентама система. Функцију система обухватају сви послови који се састоје од различитих активности. Сваки систем има своје окружење. Оно што улази у састав система јесте његово интерно окружење, а сви актери и процеси који се налазе ван система чине његово екстерно окружење. Екстерно окружење увек је динамично и из њега, као и од других система, систем прима улазне информације, које трансформише својом структуром и функцијом у излазне информације које даље шаље у екстерно окружење. Отуда, комуникација система са екстерним окружењем увек је двосмерна (видети Илустрацију 1).

[3] О теорији система и организационим системима видети више у: Кековић, Зоран. (2011). *Системи безбедности*. Београд: Универзитет у Београду, Факултет безбедности; Стајић, Љубомир, и Гаћиновић, Радослав. 2007. *Увод у студије безбедности*. Београд: Драслар партнер; Драгишић, Зоран. (2011). *Систем националне безбедности Републике Србије*. Београд: Универзитет у Београду, Факултет безбедности.



Илустрација 1: Графички приказ отвореног система (Ауторка)

Сваку организацију као систем карактеришу следећи атрибути: технологије за решавање великог опсега проблема; агенти (људски, вештачки или обе врсте); систем активности (за решавање једног или више задатака); циљно усмерење (иако се циљеви могу променити, или не морају бити јасно артикулисани, а можда их и не деле сви чланови организације); утицаји ка или од окружења; знање, култура, сећање, историја и могућности различити од било ког појединачног агента и правни положај који се разликује од правног положаја појединих агената (Carley and Gasser, 1999, p. 300). О карактеристикама система следи детаљније у наставку текста.

Било која друштвена организација или друштвени систем јесте систем који је створио човек, физички је, сложен и динамичан.[4] Иако има аутора који сматрају да су ови системи релативно отворени или релативно затворени (Kast and Rosenzweig, 1972, p. 453), за друштвени систем се најчешће каже да је отворен.

Организацију као систем створио је човек. То је физички систем јер је састављен од стварних компоненти које постоје у простору. Услед броја компоненти и веза између њих, односно услед обима интеракција, систем карактерише и сложеност. Поред статичке сложености која је остварена постојањем мноштва елемената, односно подсистема, постоји и динамична сложеност која се огледа у интеракцији елемената (Кековић и Димитријевић, 2017, стр. 59). Систем је динамичан јер поред пасивне структуре има и активности. Отворен је, јер постоји у окружењу са којим је у сталној интеракцији. Та интеракција им омогућава да буду у стању динамичке равнотеже.

[4] Одређено према типологији: Blanchard, S. Benjamin, and Blyler, E. John. (2012). *System Engineering Management*. New Jersey: John Wiley & Sons (pp. 5-6).

Динамичка равнотежа произилази из динамичног окружења због којег и организација мора да буде динамична како би му се прилагодила (Dulanović i Džinović, 1995, str. 69). За отворени систем важи да његова „способност промене као одговор на притиске околине обезбеђује дугорочну одрживост система“ (Smith and Brooks, 2013, p. 26).

Оно што организацију одваја од окружења или околине у којој се налази јесу границе. У зависности од структуре, функција и организационе културе зависи ниво пропустљивости тих граница, које у сваком случају постоје. Такође, свака организациона целина у организацији има своје границе за које је могуће рећи да ограничавају делокруг рада организационе целине.

Сваки систем је хијерархијски устројен; као такав има вертикалну диференцијацију. Постојање хијерархије значи постојање различитих нивоа у организацији, различитих послова, улога и одговорности и обавезне координације и контроле. „Општи систем и подсистеми граде хијерархијски низ носилаца контроле понашања и делања подсистема с врховним императивом адаптације и одржања интеграције“ (Parsons, 2009, str. 22). Поред вертикалне диференцијације постоји и хоризонтална која је у првом реду функционална.

Динамичност (динамизам) јесте још једна одлика система. Динамично окружење захтева од система да буде динамичан. Када се јави промена или поремећај, да би систем опстао неопходно је да се својом динамичношћу прилагоди. Динамичност је повезана са отвореношћу и интеракцијама система.

Сваки систем тежи стању хаоса, распадању и нестанку, односно ентропији (Кековић и Димитријевић, 2017, стр. 62). Како не би дошло до урушавања система, сваки систем одликује адаптибилност или способност прилагођавања на различите промене или поремећаје без обзира да ли долазе из окружења или система. Некада, процеси прилагођавања могу значити трансформацију одређених квалитета (Dulanović i Džinović, 1995, str. 70). Сваки систем мора да се прилагођава што потврђује поменуту динамичку равнотежу или чак динамичку стабилност (Савић, Станковић и Јанаћковић, 2021, стр. 52).

Елементи организационих система могу да се представе као комбинација циља, снага и средстава, структуре, скупа активности и функције (Стајић, 2003, стр. 32). У организационом смислу, поред структуре (где спадају снаге и средства) и функције (где спадају активности и циљ, као нешто чијем се остварењу тежи спровођењем активности), сваки систем има своје окружење. Талкот Парсонс (*Talcott Parsons*) указао је на разлику између структурног и функционалног дела система где структуру чине компоненте система, док функционалне компоненте осигуравају опстанак система кроз динамички вид односа система и околине (2009, str. 22).

Полазећи од претпоставке да сваки систем има своје окружење, Парсонс верује да систем тежи стабилности и равнотежи, а да ће се променити једино ако у томе не успева (Parsons, 2009, str. 22). Окружење чине други системи, догађаји, појаве, простор и време, као и низ других фактора. То могу бити материја, енергија, информације. Конкретније, то су друштвена заједница, политички систем, економско стање, тржишни односи, култура, правни прописи, заинтересовани субјекти. Окружење се обично дели на: интерно и екстерно окружење. Интерно окружење чине унутрашњу конфигурацију организације и власника и управника, одбор, менаџери, запослени, а и синдикат уколико је то прописом дозвољено. Екстерно окружење, које се обично дели оперативно или конкурентско (купце, добављаче, конкуренцију, опасност од супститута и улазне баријере) и опште окружење (фактори политичке, економске, друштвене, технолошке, заштите природне средине и правне природе) (Mašić i Dželetović, 2015, str. 20). Реч је дакле о свим факторима који због отворености делују на систем и његове елементе и на који систем са елементима делује.

У зависности од правца деловања, интеракције могу бити, у првом случају од споља, у другом случају изнутра и обострано када постоји интеракција и од споља и изнутра. Интеракција је у основи размена материје, енергије или информација између система и окружења, односно између елемената система (подсистема). Када се интеракција врши од система према окружењу стварају се такозвани излази. Када окружење делује на систем, тада систем од окружења добија такозване улазе. У динамичном односу са својим окружењем, систем, односно организација прима различите улазне параметре, трансформише их и, на неки начин, извози излазе. Реч је о моделу улаз–трансформација–излаз (Kast and Rosenzweig, 1972, p. 450).

Следећа важна одлика система јесте њена функција. Функција система представља збир свих послова који се обављају ради испуњења одређеног циља. Она обухвата циљеве, послове, резултате и прописе (Кековић и Димитријевић, 2017, стр. 55). У основи, функције се састоје од послова, док се послови састоје од радњи или поступака. Са друге стране, циљеви се рашчлањују на посебне циљеве или задатке. Долази се до става да функција посредством својих послова реализује задатке ради остварења постављеног циља. Циљеви могу бити стратешки, оперативни и тактички; дугорочни и краткорочни; различити или исти за цео систем, док послови нису ништа друго него активности које спроводи структура система. Циљеви система одређују и условљавају сврху система. Сваки систем треба да има своју сврху, сврху ради које је успостављен.

Систем је састављен од подсистема и повезаних елемената. Разумевање система у целини директно је зависно од разумевања сваке његове компоненте и односа међу њима. Структура система обухвата елементе система који су интегрисани у међусобну интеракцију, а то су људи и средства (укључујући информације), односи и везе међу њима, и прописи. Људи користе средства да би вршили послове ради остварења циља, а прописи делују као регулаторни механизам тих процеса. Као основне карактеристике структуре система издвајају се уређеност и организованост (Савић, Станковић и Јанаћковић, 2021, стр. 35). Дакле, структура система јесте уређена и организована целина елемената, који су усмерени на остваривање циљева.

Систем националне безбедности, као и систем корпоративне безбедности (о ком ће бити речи у наредном поглављу) могуће је посматрати кроз призму теорије система, јер се предности коришћења теорије система огледају у разумевању карактеристика и понашања система. Сходно наведеном, системи националне и корпоративне безбедности састављени су из мноштва мањих система и њихових елемената, који испуњењем појединачних функција, обезбеђују испуњење опште функције система коме припадају. Границе ових система, као и јасну хијерархију ипак је тешко одредити. Даље, јасно је да су системи националне и корпоративне безбедности системи које је створио човек да би преко њих остварио известан циљ што је у овом случају заштитна функција државе или организације. Оба система постоје у реалном простору и времену, њихова структура је јасно одређена. Њихову структуру увек карактерише хијерархијска уређеност и организованост. Поред структуре, оба система имају и одређене активности и процесе, функције и послове безбедности. Оба система су довољно затворена како би одржали своје извесно стање, али су и довољно отворена како би имали непрекидну интеракцију са окружењем и елементима из окружења. Оба система услед промена из унутрашњег и спољашњег окружења делују у правцу одржања равнотеже адаптирајући се на те промене. У вези са изнетим, могуће је подвући да је реч о „аморфним“ системима.[5]

[5] Објашњење следи у наставку текста. Најбоље се објашњава дефиницијом националног система безбедности у ширем смислу коју даје Мијалковић (2015, стр. 242).

1.1.1.1. Систем националне безбедности

Организациони или друштвени системи који се успостављају деловањем човека, а ради остваривања одређене сврхе јесу и системи безбедности. Наиме, како је безбедност примарни структурни елемент друштвеног система јер од њега зависе сви чланови друштва, онда сваки друштвени систем настоји да организује своје појединачне сфере на начин да задовољавају потребе за безбедношћу у друштву у целини. Према томе, систем безбедности као друштвени систем обезбеђује и остваривање својих безбедносних функција. Овај принцип на којем почива систем националне безбедности проистиче из структурних веза између безбедности и људских потреба (Grizold, 1994, str. 43).

Мијалковић и Поповић дефинишу систем безбедности као„складно деловање више организација безбедности које обављају специфичне (пот)функције безбедности, што резултира извесним стањем безбедности" (2015, стр. 111). Оваква дефиниција је крајње интересантна јер обухвата елементе попут организација, функција и стања који заједно чине систем безбедности. Подсетимо, ови аутори сматрају да је одређивање националне безбедности као система најсвеобухватније, при чему праве разлику између функције и организација које чине акциони ниво безбедности и представљају субјекте, активности и снаге и стања као производа акционог дела (Мијалковић и Поповић, 2015, стр. 111).

Још једноставније одређење даје Ковачевић истичући да „функција безбедности и организација безбедности чине систем безбедности" (1980, стр. 14). Уочава се да Ковачевић својим одређењем не обухвата стање као део система безбедности. Нешто детаљније тумачење могуће је уочити у дефинисању система безбедности као „организованог друштвеног система преко којег друштво организује функцију заштите виталних вредности ради општег напретка и развитка друштва" (Стајић и Гаћиновић, 2007, стр. 91; Стајић, 2015, стр. 40), односно као „сложеној, уређеној целини низа људских делатности и специјализованих органа, усмераваних од стране политике у остваривању одређеног циља безбедности" (Иванчевић, 1993, стр. 114, према Rakić, 2008, str.250). Кековић истиче да се системи безбедности могу „одредити двојако: 1) као начин организовања друштва за заштиту од свих извора и облика угрожавања и 2) као начин заштите основних друштвених вредности", или се „посматрати и као систем теоријских знања о томе на који начин најбоље организовати једно друштво у жељене сврхе поводом заштите њених вредности" (2011, стр. 86, 89).

Из концепта система безбедности изведени су бројни други концепти и то: систем безбедности државе, који се узима као полазна тачка овог истраживања; систем безбедности регионалне или међународне заједнице; систем безбедности појединца и систем безбедности других ентитета попут организација, који се такође узима као концепт овог истраживања (систем безбедности организације схваћен као корпоративна безбедност). Одговарајући појам система безбедности на нивоу државе је систем безбедности државе или систем националне безбедности.

Систем националне безбедности попут политичког система којем припада, као подсистем у систему глобалних друштвених односа појављује се као емпиријска категорија. Попут политичког система, систем безбедности представља предмет научне дисциплине (Atanacković, 1986, str. 68). У методолошком смислу, могуће је разликовати три нивоа општости појма „систем националне безбедности".[6] Као општи појам, термин систем националне безбедности се користи да означи посебан подсистем глобалног друштва. Попут сфере права, политике, економије, културе могуће је издвојити и сферу безбедности. Уже значење се односи на класификације које се могу извршити у оквиру

[6] Видети више у: Иваниш, Жељко, Младеновић, Мирослав, и Драгишић, Зоран. (2006). *Политички систем*. Београд: Факултет цивилне одбране (стр. 27).

система безбедности, па је могуће разликовати систем безбедности јаких, слабих држава или држава у транзицији. Најуже значење се је ограничено историјски или територијално (нпр. систем безбедности Републике Србије, систем безбедности након 11. септембра).

Системи безбедности држава или системи националне безбедности јесу најразвијенији концепти безбедности (Кековић и Димитријевић, 2017, стр. 52). Хијерархијски, систем националне безбедности припада систему државне власти, односно политичком систему државе и ширем друштвеном систему државе. Даље, он припада међународном систему или међународним системима.[7] У супротном смеру, систем националне безбедности састоји се од подсистема. У основи, могуће је направити разлику између подсистема у систему националне безбедности и то су систем одбране, систем унутрашње безбедности и безбедносно-обавештајни систем. Даље, могуће је говорити и о другим подсистемима или чак микросистемима као што је систем приватне безбедности, односно систем корпоративне безбедности. Према наведеном однос система националне безбедности и система корпоративне безбедности могуће је сагледати као однос вишег и нижег појма, тако да виши појам садржи нижи. Дакле, систем корпоративне безбедности могуће је посматрати каоподсистем система приватне безбедности, (под)подсистем система унутрашње безбедности, односно (подпод)подсистем система националне безбедности.

Уколико се за пример представи национална критична инфраструктура, прецизније, организација која је идентификована као национална критична инфраструктура и њена корпоративна безбедност, теорија система као теорија организације значила би следеће: свака локална територијална јединица те организације има свој систем безбедности који припада систему безбедности регионалне организационе јединице, а сви системи регионалних организационих јединица припадају систему безбедности те организације. Даље, систем безбедности организације припада систему безбедности града или државе у којој делује. Уколико је реч у транснационалној/мултинационалној организацији, онда њен систем безбедности припада и систему безбедности региона, односно међународне заједнице.

1.1.1.2. Елементи система националне безбедности

Систем националне безбедности јесте друштвени, организациони систем. Сходно томе, елементе система националне безбедности можемо сагледати са аспекта теорије система, односно доводећи их у везу са елементима самих организационих система. Елементи организационих система јесу (Стајић, 2003, стр. 32):

- циљ због којег је систем успостављен;
- снаге и средства потребни за остварење циља;
- структуру елемената система потребних за остварење појединих активности;
- скуп активности потребних за остварење циља и
- функцију структурних елемената за остварење циља.

Систем националне безбедности, морао би имати сваки од наведених елемената, како би се могао појмити као организациони систем. Те елементе могуће је уочити из горе издвојених дефиниција. Сходно наведеном, образложење је следеће.

Циљ наведеног система је јасан – заштита и остваривање националних, али и државних, међународних и глобалних интереса и вредности. Конкретније, достизање/остваривање,

[7] О постојању једног или више међународних система видети даље у: Кековић, Зоран, и Димитријевић, Иван. (2017). *Системи безбедности са системом безбедности Републике Србије*. Београд: Универзитет у Београду, Факултет безбедности (стр. 51).

унапређивање, уживање и заштита вредности и интереса и то превенцијом, ублажавањем и елиминисањем последица остваривања угрожавања уз ревитализовање интереса и вредности након угрожавања. У крајњој линији, циљ јесте опстанак и развој друштва, квалитет живота и деловање у смеру повећања отпорности државе и друштва од различитих угрожавања.

Када је реч о вредностима и интересима, фокус је увек на националним вредностима и интересима, с тим да систем националне безбедности увек штити и оне вредности и интересе других референтних објеката као што су појединац, друштвене групе и друштво, држава, међународна заједница (Стајић, 2015, стр. 17). Мијалковић овим референтним објектима додаје човечанство и планету чије вредности и интересе назива „човечанским" (2015, стр. 11). Јасно је да било који национални интерес, а потом и основне националне вредностимогу бити угрожене. Угрожавање може потицати од природног, техничко-технолошког и друштвеног извора. Када су носиоци угрожавања људи, оно може бити свесно или несвесно. То је дакле сваки догађај, без обзира да ли настаје деловањем човека (свесно или несвесно), природе, неког техничког система или њиховом комбинацијом, који посредно и/или непосредно проузрокује или може проузроковати штетне последице по националне, државне, међународне и глобалне вредности и интересе.

Како би циљ система националне безбедности био остварен потребно је да има подршку осталих елемената, а пре свега одређене *снаге и средства*. Снаге система националне безбедности треба тумачити са опрезношћу. Најпре, снаге у смислу елемента организационог система одговарају субјектима у систему националне безбедности. Одатле, снаге као субјекти представљају „органе, тела и институције који кроз обављање својих редовних делатности директно или индиректно остварују функцију безбедности или доприносе њеној реализацији" (Стајић, Мијалковић и Станаревић, 2004, стр. 135). Као што је систем националне безбедности апарат који обезбеђује националну безбедност, тако су субјекти система ти који обезбеђују задовољење циљева система националне безбедности. Када је реч о субјектима, могуће је направити дистинкцију између конвенционалних, неконвенционалних и суплементарних (Савић, 2009, стр. 27; Стајић, 2008, стр. 304; Мијалковић, 2009, стр. 293). С обзиром на карактеристике ових трију група субјеката, приватна безбедност се заједно са припадајућом корпоративном безбедношћу може уврстити у конвенционалне субјекте. Станаревић у стандардне субјекте безбедности убраја: оружане снаге, субјекте који јавно спроводе закон (у првом реду полиција); снаге за заштиту (или јединице за заштиту); обавештајне службе; граничне стражаре и царинске органе; резервне и јединице безбедности на локалном нивоу, снаге цивилне одбране, националне страже, јединице цивилне заштите и формације за хитно деловање и пружаоце услуга комерцијалне безбедности (приватне безбедности) које је уговорила држава (2018, стр. 210). На овом месту, треба још указати на постојање разлике између субјеката, са једне стране и носиоца система националне безбедности, са друге стране, а у првом реду, државе и њених грађана (Стајић, 2015, стр. 326), али и међународне заједнице (Мијалковић, 2015, стр. 242).

Са друге стране, разлика између снага и субјеката ипак постоји. У том контексту, снаге јесу један део конвенционалних субјеката система националне безбедности и представљају „посебно организоване, обучене, опремљене и овлашћене организационе јединице субјеката безбедности које непосредно реализују одређен вид послова безбедности" (Стајић, Мијалковић и Станаревић, 2004, стр. 135). Следећи наведено, однос ова два појма – субјекти и снаге могуће је сагледати као шири и ужи појам или као општи и посебан појам.

Уколико кажемо да су субјекти у ширем смислу сви људски и материјални потенцијали који се могу ангажовати за потребе безбедности (Стајић и Гаћиновић, 2007, стр. 108-

109), обухватили бисмо и други део овог елемента организационог система – *средства*, с обзиром да материјални потенцијали управо обухватају све борбене и друге материјалне ресурсе. Са друге стране, субјекти у ужем смислу били би они субјекти чија организација, састав, опрема и оспособљеност одговарају тренутном задатку (Стајић и Гаћиновић, 2007, стр. 108-109). Из датих дефиниција система националне безбедности видимо да Мијалковић сматра да ресурсе поред наведених чине и природни, нормативно-политички и институционални ресурси.

Наиме, управљачки и извршни део система националне безбедности чине његову *структуру*, која се може сматрати целином тек када се овом институционалном делу, додају акциони и нормативни део (Драгишић, 2011, стр. 25). Структуру састављену од ових елемената Кековић назива структуром у ужем смислу или „безбедносном структуром система", док структура у ширем смислу обухвата и „институције цивилног друштва" (2011, стр. 142-143). Чињеница је да је структура без функције непотпуна, као што је неупотребљива без нормативног оквира деловања.

Без превеликог удубљивања у анализу *активности*, овде треба указати на то да је реч о најважнијем елементу система националне безбедности, јер омогућава остваривање функције система (Стајић, 2015, стр. 328), а у крајњој линији и остварење циља система. Најгрубља подела ових активности била би на оне којима се систем успоставља и организује и оне којима се делује, односно на системске и функционалне активности које заједно чине акциони део система националне безбедности (Драгишић, 2011, стр. 24). Уз то, системске активности омогућавају функционисање на унутрашњем нивоу, док функционалне омогућавају функционисање на спољном нивоу ради реализовања послова безбедности (Мијалковић, 2015, стр. 244). Ради бољег разумевања активности, неопходно је овим делом рада обухватити и послове и мере којима се остварују постављени задаци. Послови су делови функције, односно то су „потфункције националне безбедности чија је реализација у надлежности појединих субјеката и снага безбедности" (Мијалковић, 2015, стр. 244), те отуда се овај термин употребљава када се дефинишу унутрашњи послови (Стајић, 2015, стр. 336). Спроводе се у циљу остварења постављених задатака, а како би субјекти и снаге били припремљени да те задатке остваре „несметано и ефикасно" (Стајић, 2015, стр. 331), односно како би се подигли „из редовног у стање повишене готовости" (Мијалковић, 2015, стр. 244) предузимају се мере. Закључно, активности, послови и мере сматрају се акционим делом јер омогућавају деловање система националне безбедности.

Функције наведених структурних елемената јесу функција система националне безбедности. Она се може разумети као „'најопштија мисија' друштва и државе на заштити сопственог опстанка, унапређењу егзистенције и достизању, заштити и развоју личних и виталних вредности и интереса као основног и крајњег циља" (Мијалковић, 2015, стр. 243). Субјекти система националне безбедности путем активности, послова и мера остварују ову, заштитну функцију државе. С обзиром на постојање три групе субјеката, могуће је направити разлику између две потфункције система националне безбедности. Прва је функција достизања, развоја и унапређења друштвених и државних вредности и интереса, коју пре свега спроводе неконвенционални и суплементарни субјекти. Друга је функција контроле безбедносних изазова, ризика и претњи, коју пре свега спроводе конвенционални субјекти (Мијалковић, 2015, стр. 249).

Елементе система (националне) безбедности могуће је сагледати на нешто другачији начин. Тако, елементи обухватају активности, мере, послове, субјекте уз снаге и носиоце (Стајић и Гаћиновић, 2007, стр. 99; Стајић, 2015, стр. 327), те још и функције система (Стајић, Мијалковић и Станаревић, 2004, стр. 135) и безбедносну културу (Мијалковић, 2015, стр. 242). Станаревић сматра да се систем националне безбедности састоји од структура, институција и особља одговорних са једне стране за пружање безбедности и

са друге стране за управљање и надзор (2018, стр. 196). Уочава се да број елемената код аутора варира, с тим да, уколико се вратимо корак уназад, јасно је да поједини елементи који се препознају код сваког аутора, одговарају елементима организационог система уопште.

Поред изнетог приступа, елементе система националне безбедности можемо сагледати на још два начина. Најпре, правећи аналогију са системом безбедности (Мијалковић и Поповић, 2015, стр. 111), за систем националне безбедности можемо рећи да га чине организације безбедности у виду хоризонтално, вертикално и дијагонално повезаних потцелина (подсистема и микросистема), функције безбедности и стање безбедности које се остварује организацијама и функцијама. Друго, као елементе система националне безбедности могуће је одредити окружење, структуру и функцију (Кековић и Димитријевић, 2017, стр. 54). Најједноставније, систем националне безбедности, попут свих осталих организационих система, егзистира у окружењу које чине најпре други системи и догађаји. С обзиром на повезаност и њихов узајамни ефекат, било који организациони систем црпи улазне информације из окружења, обрађује исте путем своје структуре и функција са циљем да окружењу понуди излазне информације као одговор на оне добијене. У односу на окружење, систем националне безбедности свакако да није изолован од свих ентитета и догађаја који се одигравају како на националном, тако и на међународном или глобалном нивоу. Реч је о систему који је отворен и који „комуницира" са окружењем. Тако, дешавања у држави, попут избијања грађанских немира, или дешавања попут регионалних сукоба или миграција, захтевају од система националне безбедности да се адаптира новонасталој ситуацији, те да на њу адекватно одговори својом структуром и функцијама. Структуру система чине елементи, везе између истих и структурни прописи (Кековић и Димитријевић, 2017, стр. 57). Из досадашњег текста, јасно је да систем националне безбедности има своју структуру, односно носиоце, субјекте и снаге, као и средстава који заједно чине „мозак и костур" (Мијалковић, 1998, стр. 175). На крају, да би систем националне безбедности могао у окружењу деловати својом структуром, неопходан му је трећи елеменат, односно функција, као „скуп најразноврснијих послова који се обављају са истим циљем" (Кековић и Димитријевић, 2017, стр. 55).

1.1.1.3. Обележја система националне безбедности

Сви елементи система националне безбедности функционишу заједно, међусобно повезани и условљени везама услед чега систем чине не само сложеним са израженом диференцијацијом, већ и динамичним. Систем националне безбедности има своју структуру, своју функцију и окружење. С обзиром на увек динамично окружење, систему националне безбедности не остаје ништа друго него отвореност, интеракција са окружењем, динамичност, адаптабилност и регулација.

Сви елементи система, односно субјекти који чине структуру, налазе се у међусобној интеракцији, као и у интеракцији са окружењем. Без, субјекта, систем не би био у прилици да „комуницира" са окружењем. „Улази" за систем националне безбедности најчешће су информације о утицајима из окружења који су безбедносно битни а који могу бити повољни или неповољни по безбедност државе, неког њеног дела или одређене активности. „Излази" за систем националне безбедности јесу реакције система или његових појединих делова (Драгишић, 2009, стр. 168). Наиме, промене у безбедносном окружењу деловаће као „улази" за систем националне безбедности и иницираће одговор система. Са друге стране, систем ће путем „излаза" дати одговор на те промене, односно предузеће мере које су одређене као прикладне у датој ситуацији. Када један од субјеката система националне безбедности попут обавештајно-безбедносног система добије из окружења информације о планираним грађанским

немирима, обрађује их, а потом планира и спроводи одређене активности и мере (нпр. у првом реду, појачана обавештајна активност). У контексту јавно-приватног партнерства у сфери јавне безбедности, као пример интеракције наводи се стална интеракција јавних и приватних служби безбедности.[8]

Интеракција елемената захтева да они буду у некаквом међусобном односу, те је одатле, могуће говорити о њиховој хијерархијској диференцијацији. Са једне стране, уколико се посматра сам систем националне безбедности, он је сачињен од подсистема: управљачки део и извршни део система националне безбедности. Даље, сваки од ових подсистема представља целину са сопственим циљем, односно представља посебан организациони систем, па се диференцијација наставља на њих, увек правећи разлику између стратегијског, оперативног и тактичког нивоа у њиховим оквирима (Стевановић и Субошић, 2007, стр. 25). Тако, управљачки део се налази на првом хијерархијском нивоу, док се извршни део налази на другом хијерархијском нивоу. На тактичком нивоу налазе се органи и службе извршног нивоа које предузимају непосредне активности за које су надлежни. Са друге стране, и сам систем националне безбедности јесте подсистем већих система попут политичког система, друштвеног система (државе), система регионалне, међународне и глобалне безбедности. Уз то, он може бити и подсистем система заједничке безбедности (Драгишић, 2011, стр. 20). Поред овакве диференцијације, која гради хијерархије, систем националне безбедности карактерише и територијална, па и функционална диференцијација.

С обзиром на то да су послови система националне безбедности већ представљени, на овом месту довољно је осврнути се на функционалну диференцијацију. Реч је о подели послова на истом нивоу хијерархијске (вертикалне) диференцијације (Кековић и Димитријевић, 2017, стр. 65) и могуће је уочити како код система националне безбедности, тако и код њених подсистема. У том контексту, сваки подсистем има свој делокруг послова у оквирима система националне безбедности, али и у оквирима подсистема постоји подела послова на истој хијерархијској лествици. У првом случају, реч је о акционом делу система националне безбедности (Драгишић, 2011, стр. 20), док у другом случају можемо узети полицијски систем за пример и гране полиције чија разлика почива управо на функционално диференцираним пословима.

Схваћена као способност прилагођавања новим безбедносним изазовима, ризицима и претњама адаптабилност се постиже погодном организацијом, професионализацијом и демократском и цивилном контролом. За систем националне безбедности, који се налази под цивилном и демократском контролом и чији су припадници професионалци свесни своје улоге у друштву – каже се да је контролабилан, што значи да „надлежни државни органи увек имају (пуну) контролу над функционисањем система и да систем брзо и ефикасно реагује на захтеве које пред њега поставља политичко руководство државе“ (Драгишић, 2009, стр. 169). Како адаптабилност треба да омогући прилагођавање променама како би систем могао да оствари свој циљ, тако регулација треба да омогући остваривање циља узимајући у обзир резултате који се желе постићи (Драгишић, 2011, стр. 19). Узмимо за пример корупцију чије је искорењење скоро немогуће. Уколико су, на крају неког временског периода који је узет за анализу, резултати борбе против корупције испод оних жељених и очекиваних, систем националне безбедности уопште, односно његови подсистеми задужени за борбу против корупције, нису

[8] О јавно-приватном партнерству видети више у: Bures, Oldrich, and Carrapico, Helena. (2017). Private security beyond private military and security companies: exploring diversity within private-public collaborations and its consequences for security governance. *Crime Law Soc Change* 67, pp. 229–243; Радивојевић, Ненад. (2019). *Јавно-приватно партнерство у области јавне безбедности у развијеним земљама са посебним освртом на Републику Србију* (Докторска дисертација). Нови Сад: Универзитет у Новом Саду, Правни факултет у Новом Саду.

функционисали на жељени и очекивани начин, те је потребно предузети регулаторне активности и мере. Поред наведених, као карактеристике система националне безбедности могуће је издвојити и функционисање, стање, кретање и управљање или чак еквифиналитет, трајање система и понашање, или карактеристике организационих система уопштено (Драгишић, 2011, стр. 21; Кековић и Димитријевић, 2017, стр. 66).

1.1.2. Појмовни оквир истраживања

За свако истраживање, неопходно је „устројити" језик који ће се у том истраживању користити. Реч је о појмовном оквиру или мрежи која омогућава најпре одређивање предмета истраживања, а потом и целокупан процес истраживања.[9] Кроз појмовни апарат науке, научни судови и ставови се спецификују у појмове. Они се одређују као „термин који означава мисао о битним својствима неке појаве, процеса, односа" (Miljević, 2007, str. 20). Појам је мисаони и језички израз који укључује четири кључна елемента: термин, феномен, атрибуте и индикаторе, које је неопходно адекватно „уоквирити" зарад формулације адекватног појма (Gerring 1999, p. 358). Сваки појам има садржај, а логички поступак којим се утврђује садржај јесте дефиниција (Miljević, 2007, str. 21). У наставку ће бити прецизирани појам безбедности и појам корпорације, концепт корпоративне безбедности и концепти критичне инфраструктуре и њене заштите.

1.1.2.1. Појам безбедности

Основни појам од којег се полази јесте појам безбедности. Безбедност је кроз историју била једна од основних потреба, вредности и интереса појединаца. Оснивањем заједница, а потом и друштава и држава, безбедност постаје и једна од основних потреба, вредности и интереса тих колективитета. Безбедност је била и остала „двосмислен симбол" (Wolfers, 1952), а дефиниције безбедности су добро успостављена институција међународне политике (Rothschild, 1995, p. 53).[10] Постепено, безбедност постаје једна од главних преокупација различитих друштвених дисциплина попут филозофије, социологије и политичке науке, да би на крају добила своју дисциплину, савремене студије безбедности (Bajagić, 2011, str. 39-40), блиско повезану и некада преклапајућу са дисциплинама попут „међународних односа", „међународних безбедносних студија", „безбедносних студија" и „стратешких студија" (Taylor, 2012, p. 1).

Од појаве националне државе, безбедност је, уз рат и мир, била средишњи појам кључан за опстанак цивилизације (Савић, 2006, стр. 34). Од тада, као и током хладног рата, безбедност је била предмет научних истраживања држава и државних система, док су новија истраживања показала да индивидуална и колективна безбедност не зависе искључиво од националне безбедности (Стојановић и Павловић, 2014, стр. 18), иако државе и даље имају незаобилазно место у анализама, као и остваривању безбедности. Мелвин Лефлер (*Melvyn Leffler*) запажа да приступ националне безбедности приморава историчаре да проучавају геополитичка и стратешка питања у вези са политичком економијом и идеологијом, као и да се уважавају приступи и из других дисциплина. Тако, психолошки приступи ће бити корисни када се разматрају перцепције претње, теорије доношења одлука и организационог понашања и разумевање културе и

[9] О методологији формирања појмова видети више у: Копања, Михајло. (2022). *Геополитички приступ утврђивању делотворности концепта велике стратегије обуздавања: студија случаја Сједињене Америчке Државе 1979-1989* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности (стр. 12-15).

[10] Иначе, по Бери Бузану (*Barry Buzan*), вероватно најпознатији концептуални део о безбедности је представљен у књизи Арнолда Волферса, *Раздор и сарадња* (енг. *Discord and Collaboration*) (1983, p. 4).

идеологије када се дискутује о основним вредностима, или приступи корпоративног, реалистичког и светског система када се воде расправе о примени власти (1990, p. 149).

Арнолд Волферс (*Arnold Wolfers*) дефинишући безбедност указује „на одређени степен заштите претходно стечених вредности“ (1952, p. 484), односно за њега „безбедност је у објективном смислу одсуство угрожавања постигнутим вредностима и у субјективном смислу одсуство страха да ће такве вредности бити нападнуте“ (1952, p. 485). Предуслов оваквог одређења јесу дефинисане основне вредности различитих субјеката попут званичника извршне власти, владиних агенција, законодавних одбора, политичких странака, економских интересних група и етничких заједница (Leffler, 1990, p. 144).

За Дејвида Болдвина (*David Baldwin*), Волферсова карактеризација безбедности као „одсуства претњи стеченим вредностима“ треба бити преформулисана у „малу вероватноћу оштећења стечених вредности“ (1997, p. 13). Да ли заиста постоји потпуно одсуство претњи? Ако се и искључе претње које корене имају у људској природи и делању, како искључити претње попут земљотреса или урагана, цунамија?! Стога, Болдвиново се одређење намеће као исправније. На трагу Волферсовог рада, Младен Бајагић наводи да се безбедност „у објективном смислу дефинише као непостојање претњи (absence of threats) усвојеним вредностима, а у субјективном смислу као непостојање страха (absence of fear) да ће те вредности бити нападнуте, или се под њом подразумева слобода од штетних претњи“ (2011, str. 43).[11]

Безбедност такође може бити вредност чијим се остварењем обезбеђује остварење других вредности. Тако посматрана, безбедност би, сматра Чарлс Херман (*Charles Hermann*) била „инструментална“ вредност (1982, p. 19), упркос погрешном ставу појединаца и група да је реч о коначној вредности. Неведени аутор безбедност одређује као „очекивање задржавања и побољшања способности да се ужива у високо цењеним вредностима без препрека“ (Hermann, 1982, p. 19).

За потребе рада користиће се дефиниција безбедности коју је дао Љубомир Стајић. Он безбедност дефинише као „својство неког реалног друштвеног, природног или техничког субјекта (бића, творевине или ствари) испољено као успостављено, одржано и унапређено стање и(ли) вредност, а која се изражава кроз испуњеност минимума одређених (безбедносних) стандарда својствених том субјекту, а што му омогућава реалну основу за опстанак, рад, раст и развој без обзира на носиоце, облике, време и место угрожавања“ (Стајић, 2008, стр. 28). О дефинисању безбедности писали су бројни домаћи аутори (Савић, 2006; Савић, 2007; Стајић, 2008; Мијалковић, 2009; Станаревић, 2018)[12], а наведена дефиниција је изабрана јер не позива на безбедност конкретног референтног објеката.

Из другачије перспективе, безбедност је „организован механизам заштите у коме се вршењем послова безбедности на прописан начин, кроз континуиран и научно заснован процес идентификације потенцијалних опасности и управљања ризиком, долази до стања у коме је ризик редукован до прихватљивог нивоа на коме је под апсолутном контролом, тако да минимизира реалну опасност по предмет заштите, док се континуитетом процеса настоји прогресивно смањивати до могућности елиминације“ (Ostojić, 2008, str. 196). Ова дефиниција је такође у „неутралном пољу“ дефиниција, па се такође на овом месту може узети у обзир.

---

[11] Веома опсежно истраживање о разумевању концепта безбедности видети у: Bajagić, Mladen. (2011). Razumevanje bezbednosti od antičkih vremena do savremenih pristupa. *NBP. Nauka, bezbednost, policija* 16 (2), str. 39-55. Видети више и у: Ivanović, R. Aleksandar. (2017). Pojam i elementi nacionalne bezbednosti. *Pravne teme* 5 (9), str. 186-211.

[12] О безбедности може да се говори као о стању, осећању, потреби, интересу, вредности функцији, организацији и систему.

Уважавајући поставке Теорије система, безбедност није ништа друго него један „систем, хармонична целина способна да самостално функционише у извесном временском и просторном окружењу, састављен од више хоризонтално, вертикално и дијагонално повезаних потцелина (подсистема и микросистема – организација безбедности), које врше конкретне делатности (функција безбедности) чија резултанта има за циљ несметано достизање, уживање и свеобухватну заштићеност референтних вредности и интереса од угрожавања (стање безбедности)“ (Мијалковић, 2009, стр. 58).

У оквирима реалистичког теоријског правца, развио се традиционални концепт националне безбедности[13] или државоцентрични приступ безбедности под окриљем успостављања међународног система држава (енг. *state system*) Вестфалским миром 1648. године (Савић, 2006, стр. 39). Дакле, са формирањем модерне државе, као суверене и највише власти која има монопол над применом силе отпочиње развој државоцентричног схватања безбедности. Национална држава је била та која је једина могла легитимно да користи силу како би одржала унутрашњи ред и мир и очувала спољну безбедност. Безбедност, која је тада била искључиво национална безбедност, делила се на унутрашњу (јавну и државну) безбедност и на спољну (одбрамбену, војну) безбедност (Milosavljević, 2014, str. 101).

У двадесетом веку, након четири века такозваног „вестфалског модела међународних односа“ (Савић, 2006, стр. 34), државоцентрични приступ безбедности замењен је другачијим концептом безбедности. Напуштањем тог традиционалног приступа у чијем су фокусу биле искључиво војне претње дошло је до продубљивања и проширивања истраживачког поља безбедности. Првобитно, безбедност је дефинисана искључиво као слобода од објективних војних претњи по државу која постоји у анархичном међународном систему. Тек са крајем Хладног рата, када је на видело изашао читав спектар различитих изазова ризика и претњи, Копенхашка школа студија безбедности развија секторски приступ проучавању безбедности чиме проширује концепт безбедности (са војног на још четири сектора безбедности: политички, економски, социјетални и еколошки) (Buzan, Wæver and De Wilde, 1998). Са друге стране, развија се и приступ проучавању безбедности према нивоима, чиме се продубљује концепт безбедности (четири нивоа анализе: индивидуални или људски, национални или државни, регионални и глобални) (Ejdus, 2012, str. 33).

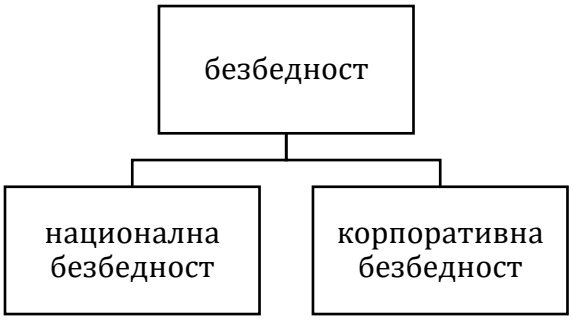
Услед усложњавања поља истраживања безбедности, из основног појма безбедности развили су се секундарни појмови. Отуда, појам безбедности као интегративни појам подразумева различите видове безбедности. Тако, можемо говорити о интегралној безбедности која обухвата унутрашњу и међународну безбедност (Стајић, 2015, стр. 32), односно различите видове квалитета живота (Стојановић и Петровић, 2014, стр. 19). Можемо говорити о безбедности државе, безбедности друштва, друштвених група или безбедности појединца. Можемо говорити о националној безбедности, регионалној и глобалној/међународној, односно заједничкој, колективној и кооперативној безбедности. Можемо говорити о војној, политичкој, економској и социјеталној безбедности, безбедности животне околине (еколошка безбедност) или људској безбедности. Уз њих, све чешће се истражују области попут здравствене безбедности, демографске безбедности, цивилне заштите, сајбер и информационе безбедности, урбане безбедности, приватне и корпоративне безбедности.[14] Постоје међутим аутори који сматрају да се не ради о новим концептима безбедности, јер је „безбедност једна,

[13] Конкретно, термин „национална безбедност“ постаје познат тек након Другог светског рата, када је 1947. године Труман потписао Закон о националној безбедности Сједињених Америчких Држава (Станаревић, 2012, стр. 146).

[14] Наведени су неки примери. Разматрање појмова изведених из појма „безбедност“ далеко је сложеније и шире. Проширење дефиниције или поља безбедности могуће је објаснити и Теоријом секуритизације.

једина и недељива“ и нема безбедности државе без других безбедности (Стајић, Радивојевић и Мирковић, 2017, стр. 1326). Немогуће је дакле говорити о било којој безбедности уколико је бар један сегмент те безбедности угрожен.

За предмет рада, значајни су појмови национална безбедност и корпоративна безбедност (видети Илустрацију 2). Ова два феномена су у основи појмовно једнаки јер је основни корпус атрибута исти. Међутим, национална безбедност и корпоративна безбедност имају сопствене секундарне атрибуте који их чине карактеристичним и по којима се разликују, те је могуће рећи да је реч о две врсте безбедности.



Илустрација 2: Основни и изведени појмови (Ауторка)

Када се користи термин национална безбедност, најпре се помисли на заштиту (државе) од претњи споља, док се за унутрашњу безбедност користи синтагма домовинска (унутрашња) безбедност (енг. *Homeland Security*). У српском језику термин национална безбедност би могао да означава безбедност једне нације, како се у друштвеним и политичким наукама изрази *националан, национална, национално* везују за нацију (Ivanović, 2017, str. 193). Ово међутим није случај. Да би се означила безбедност Републике Србије, користи се термин национална безбедност, увезен из западних језика. Све до деведесетих година прошлог века, на овим просторима, био је у употреби термин државна безбедност, да означи безбедност истог референтног субјекта. Данас, и у нашој земљи је доминантна употреба синтагме „национална безбедност“. Интересантно је да је у Сједињеним Америчким Државама, тек 2002. године под утицајем терористичког напада 11. септембра годину дана раније основано Секретаријат за унутрашњу безбедност (енг. *Department of Homeland Security*). Такво тело, у нашој земљи има традицију дугу деценијама. У склопу обавештајно-безбедносног система Министарства унутрашњих дела Краљевине Југославије постојала је Дирекција националне безбедности.

Без удубљивања у одређење националне безбедности, што ће бити предмет анализе неког од наредних делова рада, довољно је на овом месту указати на то да национална безбедност обухвата неколико елемената. Она се односи и на унутрашњу и на спољашњу средину или окружење. Обухвата безбедност од свих претњи без обзира „од кога потичу“. Усмерена је на заштиту и очување националних (државних) интереса и вредности. Националну безбедност могуће је сматрати стањем које се остварује системом националне безбедности.

Да би се говорило о националној безбедности и систему националне безбедности, било је потребно осврнути се на општи појам безбедности, а потом појмовно одређење националне безбедности као стања безбедности када је држава главни (али не и једини) референтни објекат заштите.[15] Држава је била и остала, бар за сада, најодговорнија за постојање безбедности, па је њена безбедносна функција уједно и услужна функција (Гаћиновић, 2017, стр. 88).

Први теоријски део у којем се обрађује национална безбедност и систем националне безбедности заснива се претежно на домаћој литератури с обзиром на то да је просторни фокус истраживања на Републици Србији. Са друге стране, други и трећи теоријски део

[15] Поред државе, референтни објекти могу да буду појединци, друштвене групе и друштво.

у којем се обрађује феномени корпоративне безбедности и критичне инфраструктуре заснива се на анализи мешовите литературе где доминира инострана библиографија имајући у виду недовољност домаће литературе из ових области. Значајно је указати на то да количина досад објављених радова који су се бавили проблематиком корпоративне безбедности указује да постоји академска тематизација овог феномена.

1.1.2.2. Појам корпорације

Корпорација се дефинише као најважнија иновација двадесетог века. Татјана Гергинова (*Tatjana Gerginova*) исту одређује као „нови организациони облик правног лица или као најразвијенији савремени начин рада пословних система у развијеним земљама са тржишном економијом или капиталом предузећа, ... које је законом признато као правно лице, које има слична права као и физичко лице у циљу спајања и груписања пословних интереса, и као такво је најчешћи облик пословног удруживања“ (2017, p. 363). Слободан Марковић истиче да је то „законски одређена `особа` замишљена да вреднује сопствене интересе“ (2007, str. 149). Модерни облици организација настају трансформацијом, односно реструктурирањем ранијих сложених организација. Ти модерни облици који се формирају јесу пословни системи који делују као јединствене целине и имају форму корпорације и холдинга. Разлика која постоји између њих огледа се у томе што прву форму карактерише и пословна и власничка јединственост, док другу форму карактерише само власничка јединственост.[16]

Корпорација је „велика привредна компанија“ или „организација или група организација која је законом призната као јединствена јединица“ (Oxford Advanced Learner's Dictionary, 2010, p. 327). То је организација ресурса (људских, физичких, финансијских и информационих) који су интегрисани ради задовољења циљева. Један од кључних задатака за профитабилност и одрживост организација (јавних, приватних, профитних или непрофитних) јесте заштита тих ресурса, односно материјалне и нематеријалне имовине укључујући и заштиту имица и угледа организације и свих заинтересованих страна.

Препозната је као „најдоминантнији облик институционалног организовања друштва капитала у тржишној привреди, којег као привредног субјекта оснива једно или више правних, односно физичких лица, и представља одраз ... успостављања тржишта капитала“ (Dželetović, 2020, str. 4). Корпорације представљају највишу форму организовања економске делатности у друштву, основни организациони облик друштва. Према томе, „корпорације су нека врста основних ћелија друштва чији степен развоја дефинише и степен развоја друштва. Овако схваћене корпорације (организације) су саставни елементи тзв. критичне инфраструктуре“ (Николић и Синковски, 2013, стр. 126). Коначно, корпорација је, као нека форма правне фикције, најважнији субјекат привређивања у земљама тржишне привреде и уједно најразвијенији облик привредног организовања.

Све чешће, корпорације имају транснационални/мултинационални карактер. Као такве, корпорације имају „директне пословне активности у најмање две државе“, односно „послују директно у страној земљи путем оснивања филијала, а тиме и кроз власништво над имовином која се налази у иностранству“ (Ietto-Gillies, 2005, pp. 11-12). Карактеристике ових корпорација које је могуће издвојити односе се на поседовање својих огранака или филијала у најмање две државе, остваривање активности у најмање две државе, остваривање контроле над својим организацијама и активностима у иностранству, утицај на привреду како матичне државе, тако и привреду других држава у којима послују.

[16] О разлици између корпорације и холдинга видети више у: Marković, Slobodan. (2007). *Osnovi korporativne i industrijske bezbednosti*. Novi Sad: Fakultet za poslovne i pravne studije.

Корпорација је један од институционалних сектора са сопственом институционалном логиком у друштвеном систему. Као таква, корпорација представља као „друштвено конструисане, историјске обрасце културних симбола и материјалне праксе, укључујући претпоставке, вредности и веровања, којима појединци и организације обезбеђују значење друге њихове свакодневне активности, организују време и простор и репродукују своје животе и искуства“ (Thornton, Ocasio and Lounsbury, 2012, p. 2). У чисто дескриптивном смислу, корпорација је „структура успостављена законом како би се омогућило различитим странама да доприносе капиталу, стручности и раду за максималну корист свих њих“ (Monks and Minow, 2011, p. 6). Корпорацију је у основу могуће одредити као правно лице, које има карактеристике привредног друштва, без обзира чиме се бави, има основни капитал и акције и сопствену одговорност према трећим лицима.

„Израз корпорација представља генерички, пореклом англоамерички појам, којим се означавају све организације са признатом правном способношћу, без обзира да ли спадају у јавни или приватни, профитни или непрофитни сектор“ (Милошевић и Младеновић, 2017, стр. 290). У домаћој правној терминологији, термин правно лице је потпуни еквивалент термину корпорација. Правно лице јесте привредно друштво које је ово својство добило регистрацијом у Регистар привредних субјеката, а које обавља делатност у циљу стицања добити (Закон о привредним друштвима, 2011, чланови 2-3). Правно лице јесте „сваки домаћи или страни правни субјект који се по позитивним прописима Републике сматра правним лицем“ (Закон о одговорности правних лица за кривична дела, 2008, члан 5). Стога, правно лице јесте „организовани друштвени колективитет који чине лица, са имовином и одређеним (законитим) циљем, који је признат као правно лице са правном способношћу и који представља вештачку личност различиту од других правних (без такве способности) или физичких лица“ (прилагођено према Марковић, 2021, стр. 3).

На основу приложених одређења појма корпорације, уочава се да не постоји једна општеприхваћена дефиниција која објашњава и одређује овај појам. То се је у основи могуће приписати различитој припадности аутора различитим теоријско-методолошким правцима и то у различитим научним областима. Дакле, свака дефиниција корпорације одражава перспективу онога ко исту пише. Једино, законска основа увек одређује услове за стицање овог статуса и права и обавезе које проистичу из тог статуса.

Термин корпоративна безбедност скован је од термина „корпорација“ и „безбедност“. Како корпоративно није нужно приватно (Lippert, Walby and Steckle, 2013, p. 211), тако корпоративна безбедност пружа услуге унутрашње безбедности и за јавну и за приватну организацију (Brooks, 2013, p. 91). Дакле, корпоративна безбедност није својство корпорација схваћених као велике привредне компаније. Реч је о својству далеко ширег обима јединица, па је корпорације оправдано пре схватити као легалне организације (било да је једна организација или скуп организација) које су целина за себе. То су приватни ентитети, као и јавни ентитети који су у власништву државе. На овај начин, обухваћене су како организације приватног сектора тако и организације јавног сектора без обзира на делатност коју имају, без обзира да ли остварују профит или не.[17]

[17] У дисертацији, термини организација и корпорација ће се равномерно користити. Могуће је да се појави и неки сличан термин уколико строги превод текста других аутора тако налаже. Термин предузеће појављиваће се у тексту због навођења одредаба нормативних аката у којима се овај термин користи приликом анализе. Уз то, корпорације као организације ограничене су на оне које имају правни легитимитет, односно које су законски признате. Са друге стране, корпоративна безбедност у пракси може бити успостављена и у организацијама које немају правни статус, али се тада не би могло говорити о правно утемељеној корпоративној безбедности, те као таква не спада у праску и теорију безбедности, па ни у домен овог истраживања.

Организација је увек у основи збир људи који заједнички делују и раде у групама користећи технолошка знања и технике ради остваривања циљева (прилагођено према Dulanović i Džinović, 1995, str. 9). То је „група људи који заједно формирају бизнис, клуб, ... како би постигли одређени циљ“ (Oxford Advanced Learner's Dictionary, 2010, p. 1037). Организација је друштвени систем (Boulding, 1985, p. 8). Дакле, за организациони систем и организацију као систем могуће је рећи да су то 1) „формални (предузеће, фудбалски тим, полиција, војска, држава и сл.), а не неформални (путници на железничкој станици, публика на стадиону и сл.), и организовани (уређени) скупови људи и средстава 2) који су свесно удружени у те системе ради задовољења одређене сврхе (циља) и 3) који функционишу по одређеним принципима“ (Форца, 2019, стр. 43).

Организација може бити компанија, корпорација, фирма, предузеће, орган или институција, лице или лица или њихов део или комбинација, без обзира да ли су инкорпорирани или не, јавни или приватни, а који имају своје функције и администрацију (ISO, n.d.). Постизање безбедности у организацији доприноси њеном ефикасном пословању. Стога, корпоративна безбедност јесте „концепт који обезбеђује постизање циљева и кључних вредности корпорације“ (Gerginova, 2017, p. 367).

1.1.2.3. Појам корпоративне безбедности

Термин корпоративна безбедност преузет је из западне литературе. За овај термин је као и за мноштво других (на пример, корпоративно управљање, корпоративна култура, корпоративна етика) као основна одредница послужила корпорација. Данас, корпоративна безбедност представља и праксу и теорију која се развија. То је „јединствен део општег безбедносног домена; међутим, то није јавна полиција, приватно војно обезбеђење или физичко обезбеђење. Корпоративна безбедност је функција подршке која је у погледу ефикасности усклађена са корпорацијом и помаже њеном успеху“ (Cubbage and Brooks, 2012, p. xiii). Корпоративна безбедност или „безбедност у новом корпоративном окружењу“ добила је на значају глобализацијом економије (Savić, 2008, str. 20).

Вероватно најједноставније одређење појма корпоративне безбедности јесте њено одређивање као „осигурања безбедности којим се желе постићи корпоративни организациони циљеви“ (Walby and Lippert, 2014, p. 2) или као „интерни приступ безбедности у корпорацијама повезан са спречавањем губитака и заштитом имовине“ (Walby, Luscombe and Lippert, 2014, p. 121). Истина је да, иако ниједно одређење није погрешно, ипак је доста широко, те не даје до краја довољно јасну спознају о концепту корпоративне безбедности.

Довољно обухватна, а опет не преобимна дефиниција одређује корпоративну безбедност као својство „испољено као стање, процес и/или инструмент заштићености лица, имовине и пословања (објекти заштите) који се штите од свих извора, носиоца и облика угрожавања, а која се постиже људским, материјалним и организационим капацитетима тог лица“ (Мандић, 2020, стр. 169). Када се корпоративна безбедност посматра као својство, она је уједно и организација. Уколико се користи принцип хијерархије у организовању виших и нижих ентитета, у овом случају организација, онда следи да је корпоративна безбедност организација која припада вишој организацији, на пример, пословној организацији. Тада, за корпоративну безбедност се каже да је организациона целина која има свој систем са подсистемима и функцију са потфункцијама. Свака организациона целина се успоставља са неким циљем, па је у овом случају реч о функцији заштите свих вредности организације од било ког угрожавања.

У литератури корпоративна безбедност се схвата као систем, организација (организациона целина), функција или као својство организације. У сваком од наведених

случајева, корпоративна безбедност је једна од кључних елемената опстанка организације у динамичном и често ризичном окружењу које карактерише савремено доба. Из бројних одређења корпоративне безбедности, произилази да она у себи обједињује својство, организацију, систем и функцију.

Корпоративна безбедност јесте процес заштите пословне организације. То значи заштиту имовине корпорације и њеног пословања, односно заштиту људи, ствари и информација које су или у власништву организације или су јој поверене. У крајњој линији корпоративна безбедност треба да допринесе спречавању губитака и увећању вредности (Kovacich and Halibozek, 2003, p. 48). То је стратешка функција и уједно интегрална безбедност која у себи обухвата све аспекте безбедности и заштите (Милошевић, 2017, p. 31). Сви послови безбедности унутар организације налазе се под функцијом корпоративне безбедности која исте координише и контролише. На тај начин, корпоративна безбедност не само да омогућава заштиту целокупне организације већ обезбеђује највишем менаџменту основ за доношење свих одлука. Постизање оптималне безбедности организација, не значи безбедност само за њу, њене запослене и друге заинтересоване субјекте, већ значи безбедност и за локалну и државну заједницу у којој послује. Таква безбедна заједница јесте заједница која има могућности да допринесе целокупној регионалној, међународној, па и глобалној безбедности. Корпоративна безбедност се мора третирати у оквиру националне безбедности (Savić, 2008, str. 20; Lee, 2015, p. 10). Она је компонента (система) националне безбедности (Marković, 2007; Даничић и Стајић, 2008; Кешетовић и Симоновић, 2009; Мијалковић и Милошевић, 2010; Mijalković i Milošević, 2011; Bošković i Bošković, 2011; Marjanović i Ćupić, 2017; Kozarev, 2017; Trifunović, 2019; Gjurovski and Alceski, 2021).[18]

Допринос корпоративне безбедности националној безбедности могуће је сагледати из два аспекта. Најпре, приватни и јавни ентитети имају одговорност у организовању сопствене заштите. Заштита посебно долази до изражаја код критичне инфраструктуре која сама по себи представља један од услова опстанка и функционисања државе и друштва. Уз њу, потребно је обезбедити заштиту и за инфраструктуру која није идентификована као критична али пружа осталу робу и услуге. Друго, корпоративна безбедност је значајан „играч“ у борби против безбедносних изазова, ризика и претњи, без обзира да ли је успостављена у јавном или приватном сектору. Самостално или кроз сарадњу са јавним сектором безбедности, приватни сектор може да допринесе безбедносним напорима и националној безбедности. Само један аспект ове сарадње, а уједно можда најзначајнији, јесте дељење информација којима приватни сектор располаже, а које су кључне у борби против криминала и заштити друштвених вредности. Опет, није прихватљиво занемарити дељење информација између корпоративне безбедности успостављене у јавном сектору и јавног сектора безбедности.

Професионалац за безбедност у великој корпорацији који је одговоран за успостављање и управљање програмом заштите корпоративне имовине јесте менаџер корпоративне безбедности (Kovacich and Halibozek, 2003, p. 73). Односно он је тај који треба да „управља интеграцијом безбедносних технологија, особља, политика и процедура у сложене безбедносне системе“ (Brooks and Smith, 2014, p. 130). Менаџери корпоративне безбедности треба да од постојећих структура и ресурса организације створе функционалну целину и јединство у остваривању циља, уважавајући тренутно стање у којем се организација налази, али и визију будућих праваца развоја како система (корпоративне) безбедности, тако и организације (Мандић и Станојевић, 2020, стр. 28).

[18] Аутори говоре још и о интеграцији корпоративне безбедности и националне безбедности (Petersen, 2014; Walby and Lippert, 2015a).

Менаџер безбедности требало би да буде „пословни лидер који се залаже за безбедносни циљ за већу добробит организације“ (Smith and Brooks, 2013, p. 25) играјући већу улогу у управљању организацијом (Borodzicz, 2005, p. 69). Функција менаџера безбедности или водећег консултанта за безбедност (Ludbey, Brooks and Coole, 2017) треба да интегрише функцију менаџмента (планирање, организовање, управљање, координација и контрола) и функцију корпоративне безбедности.

У литератури, као и пракси, постоје и друге позиције на којима се врше послови безбедности. Са једне стране, испод позиције менаџера безбедности налазе се сви запослени који обављају послове безбедности (службеници обезбеђења и други запослени на пословима корпоративне безбедности) и за њих одговарају менаџеру безбедности. Са друге стране, менаџер безбедности увек одговара некоме на вишој позицији и то је најчешће генерални директор и власник капитала. Менаџер безбедности у организацији може уједно да буде надзорник за безбедност или координатор безбедности. Поред ових функција, (одређене) послове корпоративне безбедности могу вршити консултант за безбедност или специјалиста за безбедност, с тим да консултант подразумева специјализацију у овој области, па је консултант увек и специјалиста.

1.1.2.4. Концепти критичне инфраструктуре и њене заштите

Критична инфраструктура у свом најширем смислу није нов феномен. Сетимо се аквадукта и путева које су античке цивилизације градиле како би снадбевале становништво водом или користили путеве за кретање војске и трговаца. Касније, електране са далеководима, луке, мостови или железница истовремено бивају круцијални елементи за снадбевање струјом, кретање становништва, али и мете непријатеља. Иако се тада ови елементи нису називали критичном инфраструктуром, они нису били ништа друго него управо то – елементи неопходни за добробит становништва, привреде, а на крају и безбедности. Појам критичне инфраструктуре у безбедносном смислу појављује се као последица развоја држава у деветнаестом и двадесетом веку (Стајић, 2018, стр. 121), док у последње две деценије заштита и отпорност критичне инфраструктуре долазе до изражаја, јер се ризик по критичну инфраструктуру интензивирао услед новопојавних облика угрожавања и нових ризика, као и међусобне повезаности, сложености и зависности ових инфраструктура.

Уопштено, инфраструктура представља „мрежу независних, углавном у приватном власништву, система које је направио човек и процеса, који функционишу заједно и синергијски како би произвели и дистрибуирали континуирани ток основних добара и услуга (US President's Commission on Critical Infrastructure Protection, 1997). Реч је о техничким системима великих размера, масивним инфраструктурним мрежама „који су дошли да организују свакодневни живот“. Бројни аутори тврде да инфраструктуре обично почињу као низ малих, независних технологија које постају инфраструктуре „када један технолошки систем доминира над другима или када се независни системи развију у мрежу“ (Larkin, 2013, p. 330).[19] Компоненте инфраструктуре могуће је класификовати на: техничке структуре и средства (чворови, линеарне или мрежне структуре), људско особље (у планирању, управљању, одржавању и поправци/реконструкцији), функције (организација, процеси, квалитет, прописи) и животну средину (услуге заштите животне средине, природни ресурси, просторни положај) (Fekete, 2011, p. 17).

[19] У вези са наведеним одређењем, као основ за разматрање (система) заштите критичне инфраструктуре могуће је користити и Теорију система. Видети више у: Simić, Slobodan. (2022). „Kompleksnost sistema zaštite kritične infrastrukture“. U: L. Gostimirović i G. Maksimović (Ur.). *Diskurs o kritičnoj infrastrukturi* (str. 1-9). Doboj: Visoka poslovno tehnička škola; Banja Luka: Bezbjednosni istraživački centar.

Оно по чему се критична инфраструктура издваја од све остале инфраструктуре јесте атрибут критичности. Иако се критичност може тумачити различито, када се за један систем каже да је критичан у односу на други, то по правилу значи да је „први неопходан да би се наставило са радом другог". Инфраструктуру називамо критичном уколико би „нарушавање функционисања, недостатак или уништење физичких и виртуелних система, установа, опреме и других услуга могло да изазове нарушавање друштвене стабилности и безбедности државе, створи кризно стање или озбиљно утиче на функционисање државне управе и аутономију у кризним ситуацијама" (Hofreiter and Zvaková, 2017, p. 139). То је „жила куцавица" једног друштва или „линија за спасавање". Последње се користи да означи „сваки систем који одржава функцију заштите људског живота обезбеђивањем неопходне инфраструктуре у насељеним градовима" (Hamada, 2014, p. 3).

Након што је укључен у стратегију цивилне одбране Сједињених Америчких Држава, појам критичности добија интензивнију употребу „ради означавања и идентификације организација и институција које су на било који начин важне, релевантне или неопходне за континуитет снабдевања становништва и привреде добрима и услугама" (Милосављевић и Вучинић, 2021, стр. 43-44). Група аутора сматра да су бројни друштвени, економски, политички и технолошки разлози довели до промена у организационим, оперативним и техничким аспектима инфраструктуре. Некада, ове инфраструктуре су пре личиле на аутономне вертикалне интегрисане системе са врло мало додирних тачака у односу на друге инфраструктуре, док данас оне представљају чврсто повезане системе са великим бројем зависности (Setola et al., 2016, p. 3).

Критична инфраструктура је ослонац читавог друштва јер захваљујући њој друштво правилно и ефикасно функционише. Значај критичне инфраструктуре је схваћен широко. Националне владе препознале су потребу за улагањем у њихово стварање и одржавање. Међународне заједнице улажу напоре у развој ефикасне заштите критичних инфраструктура од којих зависе њихове чланице. У основи, заштита критичне инфраструктуре представља „стратегије, политике и спремност потребне за заштиту, спречавање и, када је потребно, одговор на нападе..." (Lewis, 2006, p. 4). Циљ заштите критичне инфраструктуре јесте обезбеђивање њене континуиране функционалности за потребе функционисања државе и пружања добрих услова за живот становништва. Централно место заштите критичне инфраструктуре заузима отпорност као индикатор њене способности да обезбеди рад у условима утицаја спољашњих и унутрашњих фактора, без обзира да ли ће користити апсорпцију, адаптацију или обнову, или сва три елемента заједно.

1.1.3. Проблем, предмет и циљ истраживања

Кроз целу историју људског рода, а нарочито данас, у ери најразличитијих безбедносних изазова, ризика и претњи који озбиљно прете да угрозе животе и здравље људи и њихова права, безбедност је горућа тема о којој се непрекидно разговара на националном и глобалном плану. Поред тога, у „друштву ризика"[20] грађани постају све више забринути за своју безбедност. Преузимајући одговорност за своју безбедност, ангажују приватни сектор безбедности који им пружа услуге заштите и безбедности уз надокнаду која је претходно утврђена. Све чешће се за постизање безбедносних циљева ангажују субјекти приватне безбедности да делују самостално или са државним субјектима. Добро је

[20] Транзиција из модерног индустријског друштва у ново доба учинило је друштво рањивим на технолошке опасности, поред већ присутних природних опасности. Безбедност је угрожена више, а вера у институције које треба да обезбеде ту безбедност пољуљана. О „друштву ризика" видети више у: Bek, Ulrih. (2001). *Rizično društvo: u susret novoj moderni*. Beograd: Filip Višnjić; Bek, Ulrih. (2011). *Svetsko rizično društvo: u potrazi za izgubljenom sigurnošću*. Novi Sad: Akademska knjiga.

познато ангажовање приватних војних и безбедносних компанија у бројним сукобима широм света. Такође, добро је познато и ангажовање великог броја људи (службеника обезбеђења) на различитим пословима обезбеђења лица, имовине, као и људи (приватних детектива) који се баве истражитељском делатношћу. Оправдано је говорити о „индустрији приватне безбедности" коју данас карактерише разноликост у услугама безбедности које пружа, њеној специјализацији и професионализацији, чак и неопходности у ангажовању на свим оним местима на којима држава са својим безбедносним снагама није у стању самостално да делује. Сумирано, индустрију приватне безбедности чине приватне војне компаније, приватне безбедносне компаније, приватне војно-безбедносне компаније, приватне детективске компаније и корпоративна безбедност. Један део те индустрије – корпоративна безбедност, разматраће се опсежно у овом раду.

Једно од основа функционисања сваког друштва и државе јесте критична инфраструктура. Системи и мреже које пружају основна добра и услуге нужан су услов живота и функционисања људи. Не само да се данас живот не може замислити без тих критичних инфраструктура већ су оне предуслов пружања услуга од стране државе и извршавања обавеза које има према свом становништву. Национална безбедност, економски просперитет и благостање зависни су од националне критичне инфраструктуре. Док са једне стране, нема националне безбедности без националне критичне инфраструктуре, тако са друге стране, нема националне критичне инфраструктуре без националне безбедности. Да би национална безбедност и систем који се ради ње успоставља вршио своју функцију неопходно је, као њихову потпору, учинити доступном и заштићеном сву критичну инфраструктуру која им је потребна. Једноставно, национална безбедност и њен систем само су један од „корисника" критичне инфраструктуре. Није могуће замислити било који систем укључујући и овај који може да функционише без основних елемената као што су електрична енергија, нафта и природни гас, телекомуникационе и информационе мреже, транспортне мреже, финансије. Како систем националне безбедности „треба" критичну инфраструктуру, тако критична инфраструктура „треба" систем националне безбедности. Не постоји ниједан други начин да инфраструктурни системи и мреже који су критични за једну државу и њено друштво остану заштићени осим преко система националне безбедности. Ту на сцену ступају поред државних ентитета (у првом реду војске, полиције, обавештајно-безбедносних служби) и приватни ентитети (приватна безбедност).[21] Због значаја који има, критична инфраструктура увек је мета напада током оружаних сукоба. Најчешће се као мете јављају постројења електричне енергије, цевоводи, складишта и станице за дистрибуцију нафте и гаса, телекомуникације, системи воде, складишта хране, па чак медицински објекти. Стављање „мете" на критичну инфраструктуру начин је да се непријатељ ослаби, јер оставља негативне последице по најважније потребе становништва, а када је становништво ослабљено држава и њена одбрана трпе. У овом раду, неће се разматрати угрожавање и заштита критичне инфраструктуре током оружаних сукоба, већ искључиво у мирнодопским условима.

[21] Поред ових субјеката (система националне безбедности), значајни субјекти који би могли да допринесу развоју заштите јесу академска заједница/истраживачки субјекти/стручњаци, приватни субјекти попут оператора критичне инфраструктуре и пословних субјеката, међународне организације, невладине организације, као и други релевантни друштвени субјекти. Потенцијални значај ових субјеката потврђен је и документом *Радни документ комисије - Процена утицаја - Пратећи документ - Предлог директиве Европског парламента и Савета на отпорности критичних ентитета* где су означени као заинтересовани субјекти који су консултовани приликом израде истог. Видети више у: European Commission. (2020). *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities* (SWD/2020/358 final).

Један од приоритетних циљева и задатака националне безбедности јесте заштита критичне инфраструктуре. Угрожавање из различитих извора, претње различитог природног, техничко-технолошког или антропогеног карактера или последице које би могле да наступе на критичној инфраструктури превише су озбиљни да би били занемарени. Да би се она заштитила потребно је одредити је и идентификовати. Одређење критичне инфраструктуре могуће је вршити према критеријумима који се могу груписати у три целине: „људски губици (процењује се број погинулих или повређених због прекида функционисања поједине критичне инфраструктуре), економски губици (процењује се према важности економског губитка или смањења квалитета производа или услуга, укључујући могући утицај на животну средину), утицај на јавност (процењује се према утицају на поверење јавности, физичке патње и нарушавање свакодневног живота, укључујући губитак основних услуга)“ (Pavić i Jokanović, 2021, str. 23; Directive 2008/114/EC, 2008, art. 2). Након одређења или дефинисања критичне инфраструктуре приступа се њеној идентификацији, која представља први корак у заштити. Она се спроводи проценом последица које могу да наступе услед ометања или уништења критичне инфраструктуре или које могу да наступе у случају претњи по критичну инфраструктуру. Последице угрожавања критичне инфраструктуре могуће је сагледати кроз губитак живота и имовине, прекид пружања основних услуга (у сектору енергетике и саобраћаја, здравствене заштите, финансија, телекомуникације) и производа (снадбевање храном и водом), прекид функционисања државних органа, прекид уобичајеног начина живота и последица по животну средину. На крају, увек су присутне одређене здравствене, социјалне и психолошке последице. Идентификацију је могуће извршити према општим, секторским и међусекторским критеријумима, односно према општим критеријумима који се деле на квантитативне, квалитативне и временске (Стајић, Мирковић и Радивојевић, 2020, стр. 962). Квантитативни критеријум би могао бити критична размера (квантитативно исказивање последица у апсолутним или релативним износима – број критичних елемената или чворова инфраструктуре, број критичних услуга, величина популације или број погођених корисника, величина територије, број жртава, износ материјалне штете или чак број вишкова, бафера или других аспеката отпорности, број укључених међузависности), квалитативни би могао бити критични квалитет (квалитет пружене услуге или произведеног добра, поверење грађана у пружаоца услуга), а временски критично време (трајање прекида, брзину почетка, и специфичне критичне временске оквире време трајања нефункционисања) (Fekete, 2011, pp. 18-19).

Процењује се да се око 80% критичне инфраструктуре, бар у „западним“ земљама, налази у власништву приватног сектора као последица приватизације и глобализације у последње три деценије. Број и распрострањеност критичне инфраструктуре данас је велика и узимајући у обзир „расподелу“ послова безбедности између јавног и приватног сектора намеће се као јасан закључак да држава не може да буде једина одговорна за заштиту критичне инфраструктуре. Тако, заштита критичне инфраструктуре је одговорност како државе тако и приватног сектора. Приватни сектор у овом случају може имати две улоге: као власник који је одговоран за критичну инфраструктуру или као пружалац услуга безбедности.

У првом случају, приватни ентитет ће заштиту обезбедити или изнајмљивањем услужне безбедности (ангажовањем приватних ентитета које пружају услуге безбедности) или организовањем корпоративне безбедности (успостављањем организационе целине у чијој је надлежности целокупна безбедност критичне инфраструктуре чији је власник или са коју је одговоран) или њиховом комбинацијом. Комбиновањем ова два приступа ствара се интегрисани модел корпоративне безбедности где се одређене функције, које су по правилу „мање осетљиве“, препуштају спољним специјализованим пружаоцима

услуга безбедности (такозвани енг. *Outsourcing*) (Trivan, 2012, str. 108). Треба имати у виду да је, по правилу, држава такође на неки начин укључена у обезбеђивање безбедности критичне инфраструктуре.

У другом случају, приватни сектор ће пружати услуге приватне безбедности по уговору и уз договорену надокнаду. Додатна вредност приватне безбедности у заштити критичне инфраструктуре огледа се у њеној специјализацији, која јој омогућава да развије системе заштите који су специфични за ову врсту инфраструктуре, и то посебно за сваки сектор или секторски сегмент. У оба случаја, власници или оператори критичне инфраструктуре могу допринети националној безбедности тако што ће развити „свеобухватне стратегије које управљају ризиком без изградње баријера које ометају пословање“ (Lee, 2015, p. 24).

У регулативи Републике Србије, критична инфраструктура, као објекти од посебног значаја, спада у једине објекте који подлежу обавезној заштити. Већем делу те инфраструктуре услуге безбедности обезбеђује приватна безбедност. Изузетак су објекати чију заштиту обављају државни органи и објекати чија се заштита обавља сагласно прописима из области одбране. Код оног дела критичне инфраструктуре где се заштита обезбеђује уз коришћење услуга приватне безбедности примењује се интегрисан модел корпоративне безбедности. Тај модел би поред услуга које би биле „изнајмљене“ (физичко и техничко обезбеђење) могао да обухвати менаџере безбедности, организациону јединицу за безбедност и заштиту, организациону јединицу за безбедност докумената, организациону јединицу за информатичку заштиту, организациону јединицу за осигурање ризика (Vršec, 2011, pp. 59-60). Средином педесетих година прошлог века, критична инфраструктура била је заштићена интерном службом безбедности, уз помоћ полиције, војних служби безбедности и обавештајних служби. Од друге половине седамдесетих година критична инфраструктура, попут све остале имовине, била је заштићена такозваним системом друштвене самозаштите (Davidović, Kešetović and Pavićević, 2011, p. 60). Данас је у објектима критичне инфраструктуре Републике Србије најчешће присутан интегрисан модел корпоративне безбедности, а заштита критичне инфраструктуре представља један аспект јавно-приватног партнерства (Радивојевић, 2019). Успостављање одговарајућег модела јавно-приватног партнерства препознаје се као „кључна димензија за успешно успостављање свеобухватног и ефикасног система заштите критичне инфраструктуре у свакој земљи“ (RECIPE, 2015, p. 66). Чињеница да је велики део критичне инфраструктуре у власништву или под управом приватних субјеката успостављање јавно-приватног партнерста у области заштите критичне инфраструктуре чини неопходним. Ипак, Закон о критичној инфраструктури, као и Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама не препознају приватну нити корпоративну безбедност као субјекте који учествују у заштити критичне инфраструктуре.

Критична инфраструктура међутим није једино тржиште које користи услуге приватне безбедности ни у Републици Србији ни у свету. Поред ње, институционална, комерцијална и резиденцијална тржишта такође користе услуге приватне безбедности (Strom et al., 2010, pp. 4-11). Поред приватних војски које владе одређених земаља користе активно годинама уназад, оне изнајмљују и услуге приватне безбедности ради заштите сопствених објеката, заштите јавних паркова, зграда и станова чланова владе, обезбеђења појединих локација (Strom et al., 2010, pp. 4-15), док је конкретно корпоративна безбедност успостављена у државним организацијама попут одељења за националну безбедност или јавних општинских власти (Brooks and Corkill, 2014, x). Поред ових локација, институционално тржиште би на пример обухватило здравствене и образовне установе, док се резиденцијална тржишта односе на стамбене објекте,

приватне куће, зграде или стамбена насеља.[22] Комерцијално тржиште обухвата низ тржишта укључујући пословне зграде и канцеларије, финансијске институције, малопродају, објекте смештаја и угоститељства, ресторане, места за забаву попут клубова или казина. Према неким истраживањима, комерцијално тржиште доминира као водећи крајњи корисник услуга приватне безбедности (Saha, n.d.). Са друге стране, уз уважавање другачије категоризације корисника услуга приватне безбедности, као највећи се издвајају индустрија и то пре свега производна, затим резиденцијално тржиште, па финансијске институције (Technavio, 2024).

Развој „масовног приватног власништва", као што су тржни центри, пословни и индустријски комплекси, кампуси, затворене заједнице и спортски објекти у којима живи или борави велики број људи условио је и масовно ангажовање приватних безбедносних компанија и њиховог персонала у циљу заштите (Caparini, 2006, p. 267). Реч је о објектима у претежно приватном власништву који су намењени јавности. Ангажовање приватних безбедносних компанија у оваквим објектима почива и на аргументу да иако полиција треба да има примарну безбедносну улогу, њихова дужност је да служи јавности пре свега, а не власницима имовине. Стога, потребно је ако не самостално деловање полиције онда њихово заједничко деловање са сектором приватне безбедности. Примера ради, у једном од највећих трговачких комплекса у Холандији, са проценом од 40 милиона посетилаца годишње и површином преко 60.000 квадратних метара, брига за безбедност је подељена између приватне безбедности и полиције. Ипак, у неким државама обезбеђење на спортским догађајима се потпуно „пребацује" са полиције на сектор приватне безбедности (United Nations Office on Drugs and Crime, 2014, pp. 9-10). На аеродромима, послове контроле и спречавање неовлашћеног приступа, вршење прегледа пртљага и ствари путника данас обављају запослени у приватном сектору безбедности. Наиме, присуство службеника обезбеђења на аеродромима или рецимо поморским лукама је једна од најчешћих манифестација пораста сектора приватне безбедности коју људи виде (United Nations Office on Drugs and Crime, 2014, p. 11). У неким градовима, развијена је сарадња приватних безбедносних компанија са полицијом.[23] На основу тога, уколико запослени у овим компанијама примете сумњива лица или возила или виде било коју незакониту радњу, одмах ће обавестити свој контролни центар који ће без одлагања информације проследити полицији (Mihaljević, 2018, p. 52). Општепознато је да су технички системи заштите постали незаобилазно средство заштите у објектима различитих намена, од производних погона, складишта, пословних и стамбених зграда, угоститељских и малопродајних објеката, објеката за забаву преко образовних, здравствених, финансијских установа до објеката које користе државни органи и система критичне инфраструктуре. Уз то, све је заступљенија идеја о употреби безбедносне технологије као допуна услуга људске безбедности, попут употребе камера за видео надзор за одрживија решења паметних градова или аутоматизације зграда (Meyer, 2024). Услед усложњавање претњи, интегрисана безбедносна решења, која се у основи састоје од услуга као што су контрола приступа, детекција пожара и дима, физичко обезбеђење присутно 24/7 и видео надзор, постала су неопходна за резиденцијалне и комерцијалне клијенте (Technavio, 2024). Физичка

[22] Код коришћења услуга приватне безбедности на резиденцијалном тржишту, а посебно код стамбених насеља, постоји могућност да се јаве проблеми попут продубљивања јаза између богатих и сиромашних, прекорачења права користећи „параполицијске" методе. О овој проблематици видети више у: United Nations Office on Drugs and Crime. (2014). *State Regulation concerning Civilian Private Security Services and their Contribution to Crime Prevention and Community Safety*. New York: United Nations.

[23] Често узиман за пример ове сарадње јесте британски Пројекат Грифин (енг. *Project Griffin*) осмишљен да подстакне и промовише већи ангажман између јавног и приватног сектора око питања борбе против тероризма. Иако намењен за организације, пројекат доприноси свеукупној националној безбедности (National Counter Terrorism Security Office, n.d.).

заштита у виду ангажованих лица која пружају услуге физичке безбедности (обезбеђења) присутна је, иако у мањој мери него техничка заштита, ипак на сваком од наведених тржишта.

1.1.3.1. Проблем истраживања

Држава више нема довољно капацитета да заштити све потенцијалне „мете“ од претњи из различитих извора угрожавања. Из тог разлога, држава је ради заштите такозваних „меких“ мета усвојила нове мере безбедности које не пружа она већ недржавни субјекти. Меке мете или меки циљеви одређују се као „сва места са високом концентрацијом људи и ниским степеном безбедности од напада“. Реч је местима у које спадају: „школе, интернати, мензе, библиотеке; верски објекти и друга места где се врше обреди, трговачки центри, тржишна места и остали комерцијални објекти; биоскопи, позоришта, концертне дворане, места са забавним садржајима; окупљања, параде, протести, демонстрације; барови, клубови, плесни клубови, ресторани и хотели; паркови и тргови, туристички споменици и занимљивости, музеји и галерије; спортске арене и стадиони; важне транспортне локације, железничке и аутобуске станице, аеродромски терминали; болнице, медицински центри и други објекти здравствене заштите; јавни састанци, ходочашћа, сајмови; културни, спортски, верски и други догађаји; и заједнички/колективни центри“ (Станаревић, 2018, стр. 218). Нека од наведених места спадају у објекте критичне инфраструктуре.

Према регулативи Републике Србије којом се уређује заштита критичне инфраструктуре, поједина места на којима могу да наступе последице угрожавања и губитка живота људи не подлежу обавези обавезне заштите. Велики затворени и отворени објекти, дворане, хале, стадиони и други објекти намењени за окупљање грађана попут тржних центара или пословних зграда изгледа да остају испод радара када је реч о препознавању истих као критичних. Недавни напад у концертној дворани Крокус у Москви показао је да и ова места због својих карактеристика могу бити означена као мета тероризма. Раније, ова места су била одређена као обавезно обезбеђени објекти, чијим оштећењем или уништењем би могле наступити теже последице по живот и здравље људи. Од 2022. године, уредба која је регулисала заштиту обавезно обезбеђених објеката је стављена ван снаге и замењена новом уредбом чији је предмет идентификација и начин извештавања о критичној инфраструктури Републике Србије. На тај начин, категорија обавезно обезбеђених објеката је укинута и замењена категоријом критичне инфраструктуре. Добар део објеката који су припадали првој категорији је пренесен у другу категорију. Међутим, приликом ових промена, одређени објекти и места изостављени су новим регулативним актом.

Након 11. септембра 2001. године, заштита критичне инфраструктуре постаје једна од главних тачака дневног реда националних влада и међународне заједнице. С обзиром на значај који има за националну безбедност, изгледа да питање њене заштите не јењава ни три деценије касније. Технолошки развој који је омогућио софистициране начине извођења терористичких аката и озбиљност потенцијалних последица по живот и здравље људи учинили су тероризам сложеном и значајном претњом. У Републици Србији, Стратегијом националне безбедности идентификовани су изазови, ризици и претње безбедности и класификовани по последицама које могу изазвати. Оружана агресија, сепаратистичке тежње, противправно једнострано проглашена независност територије коју административно обухвата Аутономна покрајина Косово и Метохија, оружана побуна и тероризам свстане су у првих пет изазова, ризика и претњи. У светлу пружања аргумента за претходно изнет став о искључености елемента критичности за поједина места или објекте посебно се издваја један ризик. Реч је о тероризму који је чак препознат и као „велики ризик и озбиљна претња безбедности Републике Србије“

(Стратегија националне безбедности Републике Србије, 2019)[24]. Посебно се наводи ризик од терористичких напада у Копненој зони безбедности где од 1999. године има терористичког деловања, те опасност постоји и у наредном периоду (Дирекција полиције, 2017а, стр. 70). У *Националној стратегији за спречавање и борбу против тероризма за период 2017–2021. година, Сл. гласник, РС, бр. 94/2017*, као посебан стратегијски циљ (2.6) издвојен је „подигнут ниво заштите критичне инфраструктуре". Унапређивање система заштите критичне инфраструктуре представља један од најважнијих циљева у супротстављању тероризму, јер савремени тероризам „циља" на објекте и системе од посебног, виталног значаја за функционисање заједнице. У стратегији се наводи да ће остварење овог циља бити „постигнуто кроз напоре да се подигне ниво свести друштва о значају критичне инфраструктуре за функционисање заједнице, уреди нормативни и институционални оквир и подигну кадровски и материјални капацитети органа надлежних за заштиту критичне инфраструктуре који гарантује обезбеђивање ефикасне приправности, чиме се обезбеђује одговарајућа заштита за лица, виталне функције, системе и инсталације" (Национална стратегија за спречавање и борбу против тероризма за период 2017-2021. година, 2017). Тероризам као друштвено-политичка појава представља употребу насиља, или претњу насиљем, како би се изазивањем страха код маса утицало на владе или друштва да испуне захтеве терориста који су најчешће политичке, верске или идеолошке природе. Често, за мете се бирају оне на које би се нападом изазвале масовне жртве.

С обзиром на вредности које се огледају у броју људи и инфраструктури која карактерише урбане просторе, могуће је исте препознати као једну од главних мета међународних терориста (Coaffee, 2009, p. 343). Урбане локације, простори и градови постали су стратешки „бојни простор" (Graham, 2009, p. 278). Реч је о „местима колективног окупљања" каква су јавни тргови, пешачке зоне, туристичке локације, саобраћајна чворишта, богомоље, стадиони, концертне дворане, биоскопи и позоришта, велики тржни центри и пијаце, фестивали, сајмови, местима које карактерише велика флуктуација људи, снажни ефекти напада, као и могућност „лаког извлачења" починиоца (Талијан, 2016, стр. 205). Поред тероризма, проблеми јесу и различити облици асоцијалног понашања, улични имовински криминал и много озбиљнији организовани криминал, узнемиравање, вандализам и насилничко понашање, као и урбани ризици од катастрофа природног порекла попут земљотреса, поплава, урагана.

Према домаћој регулативи, јавна окупљања могу да се организују у отвореном и затвореном простору. У првом случају, када се организују јавна окупљања, ангажује се редарска служба или служба обезбеђења уз предузимање мера безбедности од стране полиције. У другом случају, када се организују јавна окупљања, ангажује се редарска служба или служба обезбеђења уз предузимање мера безбедности од стране полиције само онда када организатор окупљања процени да је предузимање мера неопходно. Даље, према домаћој регулативи, јавна окупљања јесу она окупљања зарад изражавања, остваривања и промовисања државних, политичких, социјалних и националних уверења и циљева, других слобода и права у демократском друштву, односно окупљања којима је сврха остваривање верских, културних, хуманитарних, спортских, забавних и других интереса. Одређена на овај начин, јавна окупљања која се обезбеђују ограничена су на одређене врсте јавних окупљања. На овај начин, делимично се решило питање безбедности одређених објеката као што су дворане, хале или стадиони. „Делимично" на овом месту треба подвући с обзиром на то да се питање безбедности ових објеката решава само када се у њима одржава такозвано „јавно окупљање". Додатно, а на шта је већ указано, субјекти безбедности зависиће од процене организатора. Овиме се међутим

[24] Стратегија није замењена новом, али се на овом месту помиње с обзиром на значај који даје препознавању претње од тероризма по критичну инфраструктуру.

не решава питање безбедности на местима колективног окупљања која не припадају наведеним случајевима. Дакле, испод радара поново остају одређени објекти попут тржних центара или пословних зграда.

Корпоративна безбедност не може да буде успостављена у свим урбаним просторима. Урбани простори нису организације. Међутим, поједини објекти окарактерисани као урбани простори јесу организације. На основу горе набројаних урбаних простора или места јавних окупљања, могуће је угрубо те просторе поделити у неколико група. Прва група обухвата просторе попут јавних тргова, пешачких зона, туристичких локација, саобраћајних чворишта, игралишта где је безбедност у надлежности полиције уз евентуално ангажовање приватног сектора безбедности (приватних безбедносних компанија). Друга група обухвата окупљања попут фестивала, сајмова, концерата где брига о безбедности може бити подељена између полиције, приватног сектора безбедности (приватних безбедносних компанија) и корпоративне безбедности. Корпоративна безбедност биће укључена у обезбеђивање овакве врсте окупљања само онда када се окупљање организује у простору који припада организацији за коју је корпоративна безбедност успостављена. Трећа група обухвата богомоље, стадионе, концертне дворане, биоскопе и позоришта, велике тржне центре и пијаце, као и пословне зграде где је брига о безбедности у надлежности корпоративне безбедности уз ангажовање приватног сектора безбедности (приватних безбедносних компанија) и полиције када је то потребно због окупљања, што опет зависи од врсте и карактера тог окупљања. Сумирано, постоје два режима рада корпоративне безбедности у организацији: редовно стање (када се не организује окупљање) и када се организује окупљање. Ради лакшег разумевања видети Илустрацију 3.

Илустрација 3: Режим рада корпоративне безбедности у организацији (Ауторка)

У Републици Србији, тренд успостављања корпоративне безбедности у организацијама заостаје у односу на глобални Север и Запад. Организације у државном власништву некада су имале своје организације корпоративне безбедности (познатије као службе обезбеђења). Реструктурирањем и приватизацијом, велики број ових организација (од оних које постоје и даље) изгубио је организацију корпоративне безбедности какву је имао раније или је у великој мери назадовао у том погледу. Мањи број оних организација које су успешно реструктуриране и приватизоване, сачувале су организацију безбедности, унапредили је или су успоставили нову. Поред ових организација, организацију корпоративне безбедности је могуће наћи углавном у великим

организацијама или корпорацијама, које су у највећем броју случајева мултинационалне. У неким организацијама постоји организациона целина која се бави пословима корпоративне безбедности, док су у другим ови послови подељени на више организационих целина.

У вези са наведеним, група аутора прави разлику између неколико облика организације корпоративне безбедности (службе обезбеђења) Републике Србије: 1) Корпорација као целина има сопствену службу обезбеђења; 2) Делови корпорације имају своју службу обезбеђења, 3) Корпорација користи безбедносне услуге; 4) Корпорација за послове безбедносног менаџмента, стандарда квалитета, планирање и развој корпоративне безбедности користи сопствену службу, док за обављање послова обезбеђења изнајмљује службу; 5) Корпорација за послове безбедносног менаџмента, стандарда квалитета, планирање и развој корпоративне безбедности користи сопствену службу, док за обављање послова обезбеђења користи своју службу физичко-техничког обезбеђења и/или изнајмљује службу и 6) Корпорације користе заједничку и истовремено затечену службу безбедности са намером да исту откупе (Талијан и Талијан, 2010, стр. 15-16).

Тренутни ниво успостављања корпоративне безбедности не разликује се у великој мери од стања које је Драган Триван описао пре једну деценију, што указује на незнатне помаке који су учињени у пракси у овој области. Исти аутор као разлоге за такво (овакво) стање наводи: „недостатак адекватних, законских и подзаконских аката и процедура који би требало да регулишу рад тог сектора; неускладеност постојеће организационе структуре са циљевима корпоративне безбедности; недовољна и нерегулисана сарадња са надлежним државним органима и службама; преклапање задатака сектора безбедности са задацима других организационих јединица корпорације; недостатак стручно оспособљеног кадра и неадекватна едукација менаџера безбедности; недостатак савремене информатичке опреме и других материјалних и новчаних средстава за реализацију процеса обликовања организационе структуре корпоративне безбедности“ (Trivan, 2014, str. 72). Добрим делом, ови разлози су присутни и данас и представљају кочницу у развоју корпоративне безбедности у Републици Србији. Касније у раду, приметиће се да су овде наведени разлози уско повезани са проблемима који су утицали на развој укупног сектора приватне безбедности у Републици Србији.

О корпоративној безбедности могуће је говорити као о систему, организацији, функцији или стању. Корпоративна безбедност се још схвата и као концепт, док се са научног становишта, у научно-истраживачком смислу схвата и као феномен, који са системима и процесима у (природи) и друштву представља предмет емпиријског, систематског и критичког испитивања. Такође, ипак је реч и о једној релативно новој наставно-научној области.[25]

[25] Корпоративна безбедност као посебна наставно-научна дисциплина из области безбедности обухвата појединачна истраживања проблема безбедности организације и сажима сва сазнања добијена тим истраживањима. Иако је корпоративна безбедност дисциплина која се изучава у оквиру наставних програма, дисциплина која има своје уџбенике, и даље постоји незаокруженост и непотпуност ове дисциплине, бар када је реч о Републици Србији. Неки од разлога наведеног стања јесу недостатак нормативног оквира, недостатак терминологије, научних појмова и метода рада. Ипак, значај постојања ове дисциплине и изучавања у оквиру ње има вишеструк значај – теоријски, практични, друштвени и педагошки. Најпре, устаљен је став да се теорија и пракса међусобно допуњују како теорија обликује праксу, а пракса примењује, проверава, мења и развија теорију. Друштвени значај могуће је објаснити кроз сталну тежњу друштва за унапређивањем опште безбедности у чему значајну улогу има управо изучавање безбедности организација чиме се повећава не само стање безбедности организација, већ и стање целокупне безбедности друштва. На крају, педагошки значај огледа се у настојању да се кроз научну дисциплину развију сазнања о елементима корпоративне безбедности која ће бити усвајана како

1.1.3.2. Предмет истраживања

Упркос постојању богате литературе о приватној безбедности, обим научних записа о корпоративној безбедности није на тако завидном нивоу. У истраживањима која су се бавила корпоративном безбедношћу, мало њих се фокусирало на утврђивање односа између ње и националне безбедности. Ситуација је нешто лошија уколико се у обзир узму истраживања која проучавају улогу корпоративне безбедности у заштити критичне инфраструктуре као једног од круцијалних елемената опстанка државе. Иако су аутори махом сагласни да је корпоративна безбедност значајан елемент националне безбедности, даља разматрања обично стају са тим. У вези са наведеним, одређен је предмет истраживања. Ради поједностављења у његовом одређењу, извршиће се шире и уже дефинисање предмета истраживања.

У ширем смислу, предмет истраживања односи се на теоријско разматрање феномена корпоративне безбедности и проблематике њене инкорпорираности у систем националне безбедности. Шире одређење предмета могуће је посматрати и као предмет у теоријској смислу. Схваћен кроз теоријску призму, предмет овог истраживања јесте продубљивање нашег разумевања о корпоративној безбедности, а посебно њеног односа према систему националне безбедности.

У ужем смислу, предмет дисертације јесте испитивање мере у којој корпоративна безбедност кроз заштиту критичне инфрастуктуре доприноси оптималном стању националне безбедности Републике Србије. Уједно, ово је и предмет истраживања у емпиријском смислу.

Разматрање предмета истраживања одређеног у ужем смислу представљаће централни део дисертације. Национална безбедност треба да се посматра као тоталитет, који схваћен као стање заштићености националних вредности и интереса може бити угрожен широким спектром претњи. Један од сегмената националне безбедности јесте безбедност националне критичне инфраструктуре. С обзиром на њихов однос, угрожавање критичне инфраструктуре државе имало би директне или посредне последице по стање безбедности те државе. У дисертацији се полази од претпоставке да су сви остали сегменти националне безбедности оптимални (раде у функцији обезбеђивања и унапређења стања националне безбедности), те се фокус усмерава на критичну инфраструктуру и као што је наведено, на допринос корпоративне безбедности националној безбедности и то посредством заштите критичне инфраструктуре. На овом месту треба имати у виду повезаност ових појмова, те имати у виду следеће:

- Корпоративна безбедност један је од предуслова заштићености критичне инфраструктуре, док је заштићена критична инфраструктура један од предуслова националне безбедности као стања.
- Систем националне безбедности један је од предуслова за остваривање националне безбедности као стања, као што је систем корпоративне безбедности један од предуслова за остваривање заштићености критичне инфраструктуре.
- Ако се систем националне безбедности посматра као један аспект, један од његових подскупова јесте корпоративна безбедност (и њен систем).

  Ако се стање националне безбедности посматра као један аспект, један од његових подскупова јесте заштићена критична инфраструктура.

у образовном систему, тако и на практичном нивоу. Видети више у: Стајић, Љубомир, и Лукић, Татјана. (2011). *Право приватне безбедности*. Нови Сад: Правни факултет, Центар за издавачку делатност.

1.1.3.3. Циљ истраживања

С обзиром на предмет који је постављен, циљ истраживања је могуће рашчланити на неколико нивоа. Најпре, теоријско-концептуални циљ јесте да се сагледавањем теоријског оквира и релевантних појмовних одређења пружи концептуализација централних појмова од значаја за целокупно истраживање. Уједно, извршена је и дескрипција основних концепата, а посебно, дато је дубинско објашњење места и улоге корпоративне безбедности у систему националне безбедности.

Након дескрипције, циљ је био објаснити начине на које имплементација и функционисање корпоративне безбедности утиче на заштиту критичне инфраструктуре и последично, на националну безбедност државе. У настојању да се одговори на постављен циљ, у истраживању се полази од теоријски утемељене претпоставке према којој је заштита критичне инфраструктуре посредујућа варијабла између корпоративне безбедности као дела система националне безбедности са једне стране и стања националне безбедности са друге стране.[26]

На крају, дескрипција и експликација омогућили су и коначни циљ истраживања. То је испитивање и утврђивање могућности и начина на које корпоративна безбедност кроз заштиту критичне инфрастуктуре може да допринесе функционисању система националне безбедности Републике Србије и тиме остварењу њене националне безбедности као стања.

1.1.4. Истраживачка питања

Научна истраживања почивају на претпоставкама о постојању неке врсте односа између сродних или различитих појава које су предмет истраживања. Ти почетни искази о, по могућству, узрочним везама између испитиваних појава познати су као хипотезе (Vuković and Štrbac, 2019, str. 99). С обзиром на то да ово истраживање почива на квалитативној истраживачкој пракси, уместо хипотеза поставиће се истраживачка питања.

Сагледавајући предмет и примарни истраживачки циљ овог истраживања, а то је пружање увида у начине на које корпоративна безбедност у области критичне инфраструктуре утиче и доприноси националној безбедности, као главно истраживачко питање дисертације поставља се следеће:

> П: *Који је допринос који корпоративна безбедност кроз заштиту критичне инфраструктуре може да пружи националној безбедности Републике Србије?*

Да би се пружио одговор на главно истраживачко питање, неопходно је пружити одговоре на више помоћних истраживачких питања како би се дао што садржајнији и потпунији одговор на главно или централно питање истраживања.

Помоћна истраживачка питања су:

> П1: *Због чега корпоративна безбедност представља важан конституенс у савременом моделу организације друштва?*
>
> П2: *У којој мери заштита критичне индраструктуре омогућава разумевање доприноса корпоративне безбедности на националну безбедност Републике Србије?*

[26] Варијабле ће бити посебно обрађене у тексту који следи.

П2.1: *На који начин је организован систем националне безбедности Републике Србије и у каквом је односу према корпоративној безбедности?*

П2.2: *На који начин је корпоративна безбедност правно регулисана у Републици Србији и које су евентуалне мањкавости тренутног позитивноправног регулисања ове материје?*

П2.3: *На који начин се критична инфраструктура Републике Србије штити и која је улога корпоративне безбедности у тој заштити?*

1.1.4.1. Варијабле

Развојем корпоративне безбедности на темељима приватне безбедности формира се нови субјекат у систему националне безбедности. Својом структуром, функцијама и циљем, корпоративна безбедност доприноси заштити вредности и интереса у динамичном окружењу најпре националне безбедности, а потом безбедности у исто тако динамичном али ширем окружењу, на регионалном и међународном нивоу. Њено егзистирање и функционисање у систему националне безбедности постављају је за *примарну независну варијаблу* истраживања.

Како се из приложеног види, корпоративна безбедност је овако одређена део шире варијабле система националне безбедности који се поставља за ширу или *секундарну независну варијаблу* истраживања.

Један од циљева националне безбедности и уједно једно од водећих питања система националне безбедности јесте заштита критичне инфраструктуре. Последње две деценије, а нарочито последњих година, са развојем сектора приватне и корпоративне безбедности, држава своју улогу у заштити критичне инфраструктуре дели са приватним сектором, односно са секторима корпоративне безбедности који се успостављају у објектима, системима и мрежама критичне инфраструктуре. Главно и последње секундарно истраживачко питање указује на један од видова доприноса корпоративне безбедности националној безбедности, те је у складу са постављањем заштите критичне инфраструктуре за *посредујућу варијаблу* истраживања.

Систем националне безбедности усмерен је на постизање циљева који су постављени пред исти, а у крајњој линији обезбеђивање стања националне безбедности. Како се стање националне безбедности постиже на различите начине, међу којима је и заштита критичне инфраструктуре, оно се намеће као варијабла која је променљива, односно *зависна варијабла* истраживања.

Изведене варијабле могуће је представити кроз следећи приказ (Илустрацију 4):

Илустрација 4: Приказ односа варијабли (Ауторка)[27]

[27] Систем националне безбедности директно обезбеђује стање националне безбедности (представљено крупно испрекиданом линијом); Корпоративна безбедност јесте елемент система националне безбедности (представљено пуном линијом); Корпоративна безбедност доприноси заштити критичне инфраструктуре (представљено ситно испрекиданом линијом); Заштићена критична инфраструктура доприноси укупном стању националне безбедности (представљено ситно испрекиданом линијом).

1.1.4.2. Индикатори

За сваку од наведених варијабли могуће је извести одређене индикаторе. Индикатори се односе на специфичне варијабле и користе се за процену одређених аспеката истраживања. Индикатори се користе за мерење концепата или варијабли, помажу у операционализацији концепата или варијабли, односно помажу у процесу прикупљања значајних података и извођења закључака на основу добијених одговора.

Приложени индикатори нису једини индикатори изложених варијабли, већ представљају конкретан одабир који је начињем у овој дисертацији. Одређени индикатори су обрађени засебно у поглављима који одговарају варијабли на коју се односе, док су неки индикатори формулисани за евентуална даља истраживања на ову или сличну тему.

Табела 1: Индикатори (Ауторка)

	ИНДИКАТОР	**ОПЕРАЦИОНАЛИЗАЦИЈА**	**ИЗВОР ПОДАТАКА**
ВАРИЈАБЛА 1 - СТАЊЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ	**Угрожавање критичне инфраструктуре**	Последице угрожавања су вишеструке и у крајњој линији утичу на националну безбедност. Директно, последице могу да угрозе националну безбедност као сектор критичне инфраструктуре, док индиректно могу да угрозе стање националне безбедности државе. Директне последице угрожавања могуће је сагледати са аспекта ремонта оштећених и/или уништених објеката и постројења, и губитака који настају услед прекида пружања робе и услуга или смањивања њеног обима. Индиректне последице могуће је сагледати са аспекта губитака који трпе крајњи корисници у погледу робе и услуга које су им неопходне за испуњење основних потреба и обављање делатности. Значајан део свих последица могуће је изразити номинално у виду економских губитака, па су **економски губици** вредан показатељ угрожавања.	European Commission. (2020). *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities* (SWD/2020/358 final). OECD. (2019). *Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies*. Paris: OECD Publishing. Доступно на: https://www.oecd-ilibrary.org/sites/76326acb-en/index.html?itemId=/content/component/76326acb-en. OECD. (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.* Paris: OECD Publishing. Доступно на: https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en. Истраживање аутора

Табела 1: наставак

	ИНДИКАТОР	ОПЕРАЦИОНАЛИЗАЦИЈА	ИЗВОР ПОДАТАКА
ВАРИЈАБЛА 2 - КОРПОРАТИВНА БЕЗБЕДНОСТ	**Укупни економски утицај сектора приватног обезбеђења**	Сектор приватног обезбеђења значајан је потрошач на глобалном нивоу. На овом месту, под сектором приватног обезбеђења мисли се на услуге физичког обезбеђења (службенике обезбеђења који су запослени у објектима без обзира на делатност за коју се ти објекти користе) и услуге техничког обезбеђења (безбедносне системе и опрему).	Global Peace Index (*global economic impact of violence*) *technavio.com (Private security services market)* *statista.com (Market size of security services; Security services; Industry revenue of „security guard and patrol services")* *futuremarketinsights.com (global private security market)* Истраживање аутора
	Правни инструменти успостављања и функционисања корпоративне безбедности *(Корпоративна безбедност као елемент система националне безбедности)*	Корпоративна безбедност је, имајући у виду њену организацију и функције, сегмент приватне безбедности, а тиме и чинилац националне безбедности и елемент попут било ког другог у систему националне безбедности. Због релативно кратке историје, бар оне званичне, корпоративна безбедност се може посматрати као нови елемент у наведеном систему. Ипак, да би се сматрала званично признатим елементом неопходно је да као таква буде одређена у **правним актима донетим на нивоу државе**.	(Marković, 2007; Даничић и Стајић, 2008; Кешетовић и Симоновић, 2009; Мијалковић и Милошевић, 2010; Mijalković і Milošević, 2011; Bošković і Bošković, 2011; Marjanović і Ćupić, 2017; Kozarev, 2017; Trifunović, 2019; Gjurovski and Alceski, 2021) Истраживање аутора
	Индикатори корпоративне безбедности	Индикатори корпоративне безбедности могу да се користе као алат за квантификовање вредности које корпоративна безбедност има за организацију којој служе. **Индикатори или метрике безбедности** се примењују за мерење ефикасности безбедносних програма или постављених функција. У основи реч је о следећем:	Campbell, George. (2014). *Measures and metrics in corporate security*. Elsevier. Истраживање аутора
	Интерна регулатива успостављања и функционисања корпоративне безбедности	Интерна документа из којих се види да постоје организациони и функционални елементи корпоративне безбедности, донесена на основу законских и других аката и редовно ажурирана;	

Табела 1: наставак

	ИНДИКАТОР	ОПЕРАЦИОНАЛИЗАЦИЈА	ИЗВОР ПОДАТАКА
ВАРИЈАБЛА 2 - КОРПОРАТИВНА БЕЗБЕДНОСТ - наставак	Организација корпоративне безбедности	Постојање организационе целине или организационих целина које ће спроводити функције корпоративне безбедности у складу са актом о систематизацији;	
	Ресурси корпоративне безбедности	Број и компетенција запослених на пословима корпоративне безбедности; број исправних средстава и опреме за рад ових запослених и спровођење функција корпоративне безбедности, као и стање безбедносне опреме;	
	Едукација	Програми и планови основне и допунске, заједничке и специфичне едукације;	
	Функција корпоративне безбедности	Мере и активности које су прописане интерном регулативом, а чије спровођење се документује извештајима и евиденцијама;	
	Извештаји и евиденције	Постојање и редовност писања извештаја и вођења евиденција од стране одговорних лица, као и редовност надзора и контроле од стране одговорних лица;	
	Угрожавање корпоративне безбедности	Број и врста угрожавања/штетних догађаја чије је бележење обавезно у евиденцијама предвиђеним за то;	
	Трошкови корпоративне безбедности	Директни трошкови (буџет који се издваја за корпоративну безбедност, односно све послове безбедности) и индиректни трошкови (могли би бити трошкови који настају услед угрожавања због неадекватне корпоративне безбедности);	

Табела 1: наставак

	ИНДИКАТОР	ОПЕРАЦИОНАЛИЗАЦИЈА	ИЗВОР ПОДАТАКА
ВАРИЈАБЛА 3 - ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ	**Нормативни аспект заштите критичне инфраструктуре**	Основа поступања било ког субјекта у заштити критичне инфраструктуре јесу **нормативна документа**. У првом реду издвајају се стратегије, политике, закони и подзаконски акти, а потом стандарди и добре праксе.	Нормативна акта у области заштите критичне инфраструктуре
	Практични аспект заштите критичне инфраструктуре	**Отпорност критичне инфраструктуре** (робусност, сналажљивост и опоравак ИЛИ припремљеност, мере ублажавања, способности реаговања и механизми опоравка).	Fisher, R. E., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Eaton, L. K., Haffenden, R. A., Hussar, N. E., Klett, M. S., Lawlor, M. A., Millier, D. J., Petit, F. D., Peyton, S. M., Wallace, K. E., Whitfield, R. G., and Peerenboom, J P. (2010). *Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program* (No. ANL/DIS-10-9). Argonne: Argonne National Lab (ANL). Petit, F., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., Fisher, R. E., Haffenden, R. A., Huttenga, A. A., Klett, M. S., Phillips, J. A., Thomas, M., Veselka, S. N., Wallace, K. E., Whitfield, R. G., Peerenboom, J. P., and Idaho National Laboratory. (2013). *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience* (No. ANL/DIS-13-01). Argonne: Argonne National Lab (ANL). Prior, Tim. (2014). *Measuring Critical Infrastructure Resilience: Possible Indicators*, Risk and Resilience Report 9. Zürich: Center for Security Studies, ETH.
		Заштита критичне инфраструктуре (физичка безбедност, управљање безбедношћу, безбедносне снаге, дељење информација, историја/позадина безбедносних активности).	Petit, F., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Haffenden, R. A., Klett, M. S., M. S., Phillips, J. A., Veselka, S. N., Wallace, K. E., Whitfield, R. G., and Peerenboom, J. P. (2013). *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability* (No. ANL/DIS-13/04). Argonne: Argonne National Lab (ANL).

1.2. Методолошки оквир истраживања

Методолошки оквир истраживања обухвата приказ типа истраживања, одлуку о типу и изворима података, избор метода за прикупљање података, просторни и временски оквир истраживања и технике обраде података.

1.2.1. Тип истраживања

Спроведено истраживање се претежно ослања на квалитативну истраживачку традицију и комплементарно коришћење секундарне анализе постојећих података и индивидуалног – експертског интервјуа, што га већ чини мултиметодским истраживањем. Квалитативна истраживања су по својој природи контекстуална, планирају се са циљем стицања дубљих увида у истраживани феномен (Ђурић, 2013а, стр. 1346). Као таква, ова истраживања карактеришу интерпретативност и натурализам и укључују разнолике стратегије за систематско прикупљање, организацију и интерпретацију искуствене евиденције (Ђурић, 2010, стр. 485). Значајна одлика ове истраживачке традиције јесте континуирано прикупљање и анализа података које се преплићу.

Под квалитативним истраживањима обично се подводе различите истраживачке технике, па и сходно томе, она могу да имају различите форме и могуће их је изводити у различитим условима. У вези са наведеним, могуће је говорити о два типа истраживања. Емпиријска истраживања су „она која се баве сазнавањем друштвене и политичке стварности на основу искуствених, чулних података“, док се теоријска истраживања „заснивају на мишљењу о већ постојећим научним сазнањима исказаним на неки начин, у неком облику“ (Милосављевић и Радосављевић, 2013, стр. 58-59). За спроведено истраживање могуће је рећи да је претежно теоријско. Међутим, истраживање тежи да буде и практично – емпиријско, дајући основ за унапређивање области истраживања.

1.2.2. Тип и извори података

Предмет и циљеви истраживања сугеришу на употребу како постојећих извора података, тако и података који су генерисани за потребе истраживања. Прикупљање више типова података и трагање за свим доступним изворима података пружа могућност стварања целовитијег увида у проблем истраживања. Од **постојећих извора података** користили су се:

1) домаћи и инострани научни радови, примарно из области наука о безбедности, права и политикологије, а који садрже теоријска и емпиријска сазнања из различитих подручја националне и корпоративне безбедности, као и област заштите критичне инфраструктуре,
2) нормативно-правни акти домаћег и иностраног законодавства који уређују области националне и корпоративне безбедности, као и област заштите критичне инфраструктуре и
3) домаћи и инострани институционални записи који су јавно доступни (документација националних институција, документација међународних институција).

Дакле, за добијање овог типа података као извор користили су се различити типови докумената:

1) У прву групу спадају научни извори података, документа научног и стручног карактера.
2) У другу групу спадају документа нормативног карактера, односно законски и подзаконски прописи у области националне, приватне и корпоративне безбедности, као и други системски прописи који су неопходни у циљу ширег и комплетнијег приказа нормативног уређења области од значаја за предмет рада.
3) У трећу групу се могу сврстати сва остала документа која се могу користити у научне сврхе иако нису у том циљу настала, попут различитих врста извештаја, водича, стандарда.

Поред постојећих извора података, анализа проблематике којом се дисертација бави извршена је и прикупљањем **података који су генерисани** за потребе истраживања. Извор ове групе података били су експерти у области корпоративне безбедности (безбедности инкорпориране у организацији). Конкретније, реч је о лицима која су одговорна за планирање, организовање, управљање, координацију и контролу свих безбедносних функција у оквиру организације без обзира да ли она припада приватном или јавном сектору. С обзиром на предмет истраживања, организације су у овом истраживању ограничене на велике техничке системе од значаја за одбрану (критична инфраструктура).

1.2.3. Методе за прикупљање података

У зависности од избора који је направљен у погледу типова података и извора који се користе у истраживању, врши се избор метода за прикупљање података. У истраживању се комплементарно користило више истраживачких метода. Квалитативни подаци су прикупљани секундарном анализом постојећих података и експертским интервјуима.

1.2.3.1. Преглед литературе

Почетни корак овог истраживања јесте **преглед литературе** и састављање прелиминарног пописа референци релевантних за предмет истраживања. Оправданост овог корака вишеструка је. Најпре, да бисмо испитали оправданост покретања истраживања, стекли увид у постојећа истраживања и теоријске концепте, те били у стању да прецизирамо своју иницијалну идеју и преточимо је у јасно дефинисано истраживачко питање преглед литературе се намеће као незаобилазна активност (Ђурић, 2013б, стр. 42). Преглед литературе не омогућава само стицање увида у постојећа сазнања о теми већ нам омогућава да је разумемо и утврдимо докле се стигло у њеном проучавању (Hart, 2001, p. 1) или „шта ми сада знамо" о њој и омогућава нам да стекнемо увид у процедуре, технике и истраживачке дизајне који су коришћени и које вреди користити (Neuman, 2012, pp. 91-92).

У раду се тежило остваривању систематичног прегледа литературе који се може посматрати као „метод давању смисла великим количинама информација и средство доприноса одговарању на питања о томе шта ради, а шта не – и многим другим врстама питања" (Petticrew and Roberts, 2006, p. 2). Систематски прегледи литературе се све више сматрају одрживим и важним средством за поуздано сажимање све већег броја научних доказа (Haddaway et al., 2020). Преглед литературе настоји да опише, сумира, процени, разјасни и/или интегрише постојеће садржаје које користи као своју базу података и тиме, не ствара нове садржаје у виду сазнања (Cooper, 1988, p. 107). Уважавајући неколико могућих циљева које преглед литературе може имати (Baumeister and Leary,

1997, p. 312; Jackson, 1980, p. 438), у раду циљ прегледа литературе јесте да испита знање о одређеној теми, пружи корисне прегледе и интегрише знања из области корпоративне и националне безбедности, као и области критичне инфраструктуре и њене заштите. Тако се обезбеђује спајање онога што је познато о феноменима којима се рад бави. Иако се овом предистраживачком радњом започиње истраживање, она се не завршава на том месту, већ се наставља паралелно са коришћењем метода за прикупљање података током читавог истраживања не би ли се искористиле све предности које (ова предистражна радња) нуди.

1.2.3.2. Секундарна анализа података

Као што је већ наведено, у истраживању су се користили постојећи подаци, те се према њима применила **секундарна анализа података**, која поред њиховог коришћења обухвата и њихово тумачење и извођење нових налаза (Ђурић, 2013б, стр. 111). Секундарна анализа података примењена је како на искуствену грађу стварану за потребе ранијих истраживања, податке других истраживача, тако и на податке који су настали из циљева који нису научни, односно податке из институционалних извора који имају правну снагу и институционалних извора који немају правну снагу, али су од значаја за разумевање проблематике истраживања и давања одговора на истраживачка питања. Секундарна анализа података треба да омогући приказ настанка и развоја концепта корпоративне безбедности, увид у њено теоријско одређење и њене елементе, приказ њеног места и улоге у систему националне безбедности који ће и сам бити теоријски одређен.

Посебно се издваја анализа нормативно-правних аката домаћег законодавства који уређују области националне и корпоративне безбедности, као и област заштите критичне инфраструктуре. У прилог оваквој одлуци наводи се следеће: „Право је основ али и граница организовања, функционисања и деловања свих система безбедности па тако и система приватне безбедности“ (Стајић и Радивојевић, 2016, стр. 154). Наведена констатација примењује се и на систем корпоративне безбедности. Усвајањем правног оквира функција корпоративне безбедности обезбеђује се очување и унапређивање безбедности правних лица и њихове имовине и пословања, а потом и сваког вишег нивоа безбедности. Стајић и Радивојевић указују на предуслове ефикасног и корисног функционисања приватног обезбеђења међу којима су дефинисање места и улоге, професионализација и сарадња са јавним сектором (2015, стр. 174). Ништа другачији предуслови не постоје ни када је у питању корпоративна безбедност. Донети правне норме којима ће се првенствено одредити место и улога корпоративне безбедности у свеукупном систему (националне) безбедности утврђујући начела деловања, између осталог питања надлежности и одговорности, сарадње и координације. Истина, тек када се најпре приватно обезбеђење (приватна безбедност), а потом и корпоративна безбедност препознају као равноправни партнери полицији или било ком другом државном/јавном субјекту могуће је говорити о правој интеграцији ових елемената у систем националне безбедности. Са друге стране, сама интеграција о којој је на овом месту реч доводи до „остваривања оптималног стања јавне, а онда и националне безбедности“ (Стајић и Радивојевић, 2017, стр. 152) што је уједно и њен крајњи циљ. Тако је и у области заштите критичне инфраструктуре. Иако постоје случајеви где су неке државе успоставиле необавезне, добровољне програме који веома добро функционишу[28], да би се осигурало поштовање одређеног оквира заштите неостављајући појединцима да одлучују о томе да ли ће и на који начин предузимати мере заштите, Законодавац треба

[28] Видети на примеру регулисања критичне информационе инфраструктуре у: ENISA. (2015). *Critical Information Infrastructures Protection approaches in EU*. ENISA.

да испуни своју улогу. Право и у овом случају треба да буде основ организовања и функционисања заштите критичне инфраструктуре. На тај начин, држава и у овој области друштва осигурава позитивне резултате заштите националне безбедности.

Секундарна анализа података и сазнања добијена њеном применом допринели су давању одговора на постављена истраживачка питања: у првом реду, на помоћно истраживачко питање првог нивоа *П1: Због чега корпоративна безбедност представља важан конституенс у савременом моделу организације друштва?* и делимично на истраживачко питање *П2: У којој мери заштита критичне индраструктуре омогућава разумевање доприноса корпоративне безбедности на националну безбедност Републике Србије?* укључујући помоћна истраживачка питања другог нивоа *П2.1: На који начин је организован систем националне безбедности Републике Србије и у каквом је односу према корпоративној безбедности?; П2.2: На који начин је корпоративна безбедност правно регулисана у Републици Србији и које су евентуалне мањкавости тренутног позитивноправног регулисања ове материје?* и *П2.3: На који начин се критична инфраструктура Републике Србије штити и која је улога корпоративне безбедности у тој заштити?*

1.2.3.3. Експертски интервју

За добијање увида у ставове и мишљења лица квалификованих у области корпоративне безбедности, а значајних за предмет истраживања користио се **експертски интервју** као метода за добијање овог типа података. Предност интервјуа као методе за прикупљање података огледа се најпре у остваривању непосредног контакта и вођењу двосмерне интеракције са субјектима истраживања, односно испитаницима. Конкретно, у истраживању је интервју спроведен у форми полуструктурисаног експертског интервјуа. Експертски интервју карактерише интервјуисање особа које има експертско знање које се, за разлику од општег знања, односи на комплексне, интегрисане области и конститутивно је везано за професију (Ђурић, 2016, стр. 15). Значајна карактеристика ове врсте интервјуа јесте чињеница да испитаник неће током интервјуа открити информације које су означене као осетљиве (поверљиве), односно неће говорити о пословима и активностима које су због делатности такве да се о њима не може говорити јавно. Оно што додатно компликује наведено јесте чињеница да се политике одређивања поверљивости података и информација разликују. Уз то, постоје и они подаци и информације који подлежу обавезном степеновању у складу са нормативном регулативом државе, те њихово степеновање није произвољно већ строго уређено нормативним одредбама. У вези са тим, на истраживачу је одговорност припреме упитника који неће обухватити ту врсту података, за шта од велике користи може бити спровођење прелиминарних или припремних интервјуа.

Ипак, за експертске интервјуе није толико значајно интересовање за ограничена специјална или специјализована знања или одвајање приватне сфере од професионалног контекста колико је значајно да су експерти од истраживачког интереса пре свега зато што су у позицији да своје сопствене интерпретације заиста спроведу у пракси (Bogner and Menz, 2009). С обзиром на то да је током прикупљања података фокус усмерен на практична знања и искуства експерата, а да је циљ прикупити систематична и потпуна обавештења, интервју се може окарактерисати као систематизујући интервју (Meuser and Nagel, 1991; Bogner and Menz, 2009).

Испитивање за потребе дисертације спроведено је са експертима – менаџерима безбедности, односно лицима која су запослена на руководећим пословима (корпоративне) безбедности у великим техничким системима од значаја за одбрану (критична инфраструктура). Циљ интервјуа било је добијање увида у ставове и мишљења испитаника о предмету конкретног истраживања, у првом реду степену

развоја корпоративне безбедности у Републици Србији, областима и начинима утицаја корпоративне безбедности на систем националне безбедности, позитивним релацијама и доприносима корпоративне безбедности, недостацима који постоје са препорукама за њихово отклањање и унапређивање улоге корпоративне безбедности у свеукупном систему националне безбедности. Поред наведеног, интервју обезбеђује увид у стварно стање уређености и функционисања области критичне инфраструктуре у Републици Србији. Приликом спровођења интервјуа треба тежити добијању поузданих података. Међутим, како група аутора примећује, поузданост не гарантује ваљаност резултата истраживања. Поузданост је неопходан, али не и довољан услов за валидност резултата истраживања који се заснивају на њима. Ипак, што су добијени подаци више поуздани, вероватније је да ће и валидност бити већа (Dorussen, Lenz and Blavoukos, 2005, p. 334).

Полуструктурисани експертски интервјуи реализовани су у периоду који је обухватио мај, јун и јул 2024. године. Пре сваког интервјуа, испитаници су упознати са сврхом научног разговора и структуром упитника. Интервјуи су обављени у већини случајева уживо, а са лицима са којима није било у датом периоду могуће исти обавити уживо телефонским путем. Интервјуи који су обављени уживо, а за које је постојало одобрење да буду снимљени, транскрибовани су и послати на увид испитаницима са којима је таква активност била договорена. Уместо пописа интервјуисаних лица, којих је укупно 14, а с обзиром на то да је било потребно сачувати њихову анонимност, ауторка ће дати попис правних лица са чијим запосленима је интервју био обављен. Овај попис, као и Упитник доступни су у делу дисертације који садржи прилоге (Прилог 1 и Прилог 2). Примена ове истраживачке технике треба да омогући проверу изнетих теоријских ставова, али и да допуни сазнања о кључним питањима којима је поверена дисертација.

Експертски интервју и сазнања добијена његовом применом допринели су допуњавању одговора на постављена истраживачка питања: у првом реду, на помоћно истраживачко питање првог нивоа *П2: У којој мери заштита критичне индраструктуре омогућава разумевање доприноса корпоративне безбедности на националну безбедност Републике Србије?* укључујући помоћна истраживачка питања другог нивоа која су обухваћена овим истраживачким питањем.

Резултати експертског интервјуа, подржани теоријским поставкама, од кључног су значаја били за давање одговора на главно истраживачко питање *П: Који је допринос који корпоративна безбедност кроз заштиту критичне инфраструктуре може да пружи националној безбедности Републике Србије?*

1.2.4. Просторни и временски оквир истраживања

Просторни оквир истраживања обухвата територију Републике Србије, као простор за који се испитују анализирани концепти у практичном смислу.

Корпоративна безбедност, иако саставни део различитих организација деценијама уназад, у 21. веку појављује се као примарни облик безбедности (Walby and Lippert, 2014, p. 1). У Републици Србији, период после 2000. године карактерише тенденција масовног пристизања страног капитала што је утицало на унапређивање приватног сектора безбедности (Лабовић, 2012, стр. 250; Tomić i Milićević, 2016, p. 191). Томе додајмо и бројне проблеме са којима су се суочавале земље у транзицији (Кешетовић и Симоновић, 2009, стр. 147-148; Стајић, 2013, стр. 194-195), као и све већи притисци како научне тако и стручне заједнице да се ова област правно уреди. Након озбиљног правног вакума, Република Србија је 2013. године, најкасније у односу на све земље из региона, добила први системски или кровни закон из области приватне безбедности који је, по неким

ауторима, неадекватно назван Закон о приватном обезбеђењу.[29] Овај закон требало је да буде *conditio sine qua non* за превазилажења бројних проблема који су се јављали у пракси (Стајић и Радивојевић, 2015, стр. 174).

Иако се критична инфраструктура као појам у Европској унији појавила средином деведесетих година прошлог века (RECIPE, 2015, p. 23), тек након терористичких напада 11. септембра 2001. године у Сједињеним Америчким Државама, овај појам постаје актуелан на глобалном нивоу. Наиме, како у теорији тако и у пракси, појам критичне инфраструктуре почиње све чешће да се користи услед увећања асиметричних претњи попут тероризма. Након напада, државе и међународна заједница постављају себи нове приоритете у вези са заштитом критичне инфраструктуре и уједно националном безбедношћу.

Критична инфраструктура постаје незаобилазни део националне безбедности, док њена заштита постаје једна од главних тачака дневног реда националних влада и међународне заједнице. И у овој области, Република Србија се као земља у транзицији суочавала са извесним потешкоћама и новинама попут све већег приватног капитала који мења власничку структуру правних лица која управљају критичном инфраструктуром. Република Србија добија свој први закон у овој области тек 2018. године и то под околностима европских интеграција. Наиме, један од задатака Републике Србије на путу придруживању Европској унији био је да усвоји нормативни оквир који ће бити усклађен са елементима Директиве Европског савета 2008/114/ЕС у области заштите критичне инфраструктуре. Усвајањем овог закона започет је поступак систематичне и организоване заштите критичне инфраструктуре на нормативној основи.

Имајући у виду предмет истраживања, временски домен истраживања обухвата тек период од једне деценије, период од доношења Закона о приватном обезбеђењу 2013. године обухватајући и период нормативног регулисања области заштите критичне инфраструктуре доношењем Закона о критичној инфарструктури 2018. године.

1.3. Структура дисертације

Структуру дисертације одређује укупно девет поглавља повезаних у конзистентну целину. Прво поглавље посвећено је уводним разматрањима, након којих следи друго поглавље које обухвата теоријско-појмовни и методолошки оквир истраживања. Теоријско-појмовни оквир састоји се од два дела, први који обухвата теорију система у коју се поставља дато истраживање и други који се користи за операционализацију појмова који чине основу датог истраживања и дисертације. У оквиру овог дела дати су одређење проблема, предмети и циљеви истраживања, као и истраживачка питања. Методолошки оквир истраживања обухвата избор конкретног типа истраживања, типа и извора података као и метода за њихово прикупљање и анализу. У оквиру овог дела представљени су и просторни и временски оквир истраживања.

Друго поглавље разматра теоријско дефинисање националне безбедности, као и систем који је обезбеђује и подржава, уз анализу нормативног оквира који регулише успостављање и функционисање националне безбедности у Републици Србији. Треће поглавље посвећено је теоријској анализи корпоративне безбедности и њених функција, а такође обухвата правни оквир организације и функционисања корпоративне безбедности у Републици Србији, сагледан управо кроз њене функције. Четврто

[29] Видети више у: Стајић, Љубомир, и Мандић, Ј. Горан. (2014). Неке контроверзе Закона о приватном обезбеђењу. *Зборник радова Правног факултета* 48 (2), стр. 131-150.

поглавље бави се појмовним одређењем критичне инфраструктуре и њене заштите, док се посебан акценат ставља на анализу развоја и тренутног стања критичне инфраструктуре и њене заштите у Републици Србији.

Пето поглавље је посвећено дискусији и садржи сумиране резултате истраживања о доприносу корпоративне безбедности националној безбедности и то у сегменту заштите критичне инфраструктуре. Посебан део овог поглавља чине препоруке за развој корпоративне безбедности у циљу пружања доприноса систему и стању националне безбедности, као и ограничења дисертације са правцима за будућа истраживања.

У закључним разматрањима представљени су сажеци кључних налаза из истраживачког дела. Након закључних разматрања следи поглавље са коришћеним библиографским референцама, као и поглавље које садржи два прилога. Рад уз све наведено садржи и табеле и илустрације везане како за теоријски, тако и за истраживачки део.

2. НАЦИОНАЛНА БЕЗБЕДНОСТ И СИСТЕМ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Путем анализе садржаја обимне теоријске концептуализације појма националне безбедности долази се до бројних сазнања која дају добру полазну основу за анализу стања и система националне безбедности Републике Србије. У овом поглављу је на систематичан начин представљена операционализација система националне безбедности и његових подсистема. Циљ је пружити обухватни увид у место и улогу коју подсистеми, укључујући и (систем) корпоративне безбедности, заузимају у односу на виши систем националне безбедности. На крају поглавља, дата је теоријска анализа тренутног стања националне безбедности и актуелног система националне безбедности Републике Србије.

2.1. Теоријске основе националне безбедности

Широко је заступљено схватање да је термин национална безбедност први пут употребио Волтер Липман (*Walter Lippmann*) одређујући исту као способност нације да заштити своје унутрашње вредности од спољних претњи – „нација је безбедна када не мора да жртвује своје легитимне интересе да избегне рат и способна, ако је изазвана, да их одржи у рату“ (1943, p. 51). Ова, вероватно најчешће цитирана дефиниција, припада конвенционалном реалистичком приступу у међународним односима који у средиште интересовања поставља одбрану основних вредности у рату. Како Волферс запажа, ова дефиниција имплицира да безбедност расте и опада са способношћу нације да одврати напад или да надјача противника у том нападу (Wolfers, 1952, p. 484). Код многих аутора се наилази на одређење националне безбедности у традиционалном смислу (као војну или спољну безбедност државе), када се дефиниције врте око државног (националног) интереса. Таква одређења међутим не одговарају савременом схватању националне безбедности па се на овом месту не могу сматрати довољним.

Књига *Раздор и сарадња,* поменута у ранијем поглављу, била је једно од места где је концептом безбедности доминирала идеја националне безбедности.[30] Као разлог тога, могуће је узети чињеницу да је ова књига написана у јеку Хладног рата (Buzan, 1983, p. 4). Наиме, од Другог светског рата концепт националне безбедности имао је претежно војни карактер под претпоставком да је главна претња војног карактера и долази од других држава.[31] Нове претње, попут, на пример, оних које произилазе из исцрпљивања нафте, ерозије и деградације земљишта, смањења шума и уопште пропадања зелених површина, као и климатских промена биле су занемариване. Управо су такве претње угрожавале привреду, а потом и националну економску и политичку безбедност, као и стабилност међународне економије (Brown, 1986, p. 25, 30).[32]

[30] Конкретније, реч је о поглављу Национална безбедност као двосмислен симбол, које је поново штампано. Видети: Wolfers, Arnold. (1952). “National Security” as an Ambiguous Symbol. *Political Science Quarterly* 67 (4), pp. 481-502 и Wolfers, Arnold. (1962). *Discord and Collaboration – Essays on International Politics*. Baltimore: THE JOHNS HOPKINS PRESS.

[31] На пример, током Хладног рата управо због перцепција спољне претње основним вредностима америчка моћ је мобилисана као никада до тада. Маршалов план, оснивање НАТО-а или улагање милијарди долара за рехабилитацију европских економија добри су примери мобилизације (Leffler, 1990, p. 148). Видети и: Sorensen, C. Theodore. (1990). Rethinking National Security. *Foreign Affairs* 69 (3), pp. 1-18.

[32] За пример како национална безбедност може бити угрожена употребом „економског оружја“ (ембарга) може бити употребљен и такозвани „нафтни шок“ из 1973. године (Taylor, 2012, p. 8).

Усложњавање безбедности препознато је и као процес који се одиграо у четири правца. Први, концепт безбедности се проширује од националне безбедности до безбедности група и појединаца (наниже од нација до појединаца). Други, концепт безбедности се проширује од националне безбедности до међународног система (навише од нације до међународне заједнице). Трећи се огледа у врстама ентитета чија је безбедност, концепт безбедности се проширује хоризонтално (са војне на политичку, економску, друштвену, еколошку и људску безбедност). На крају, четврти правац се ослања на политичку одговорност за осигурање безбедности те се безбедност шири „навише на међународне институције, наниже на регионалне или локалне власти, а бочно према невладиним организацијама, јавном мњењу и штампи, и апстрактним силама природе или тржишта“ (Rothschild, 1995, p. 55).

Један од оснивача Теорије регионалних безбедносних комплекса, Бери Бузан (Barry Buzan), о националној безбедности говори на следећи начин: „На безбедност људских колективитета утичу фактори груписани у пет главних сектора: војни, политички, економски, друштвени и еколошки“ (1991). Војна безбедност се односи на офанзивне и дефанзивне оружане могућности државе и перцепцију држава о намерама других држава. Политичка безбедност односи се на организациону стабилност државе, системе владавине и идеологије које им дају легитимитет. Економска безбедност се односи на приступ ресурсима, финансијама и тржиштима. Друштвена безбедност односи се на прихватљиве услове за развој језика, културе, религије и националног идентитета и обичаја. Еколошка безбедност треба да осигура очување локалне и планетарне биосфере, као система од којег зависе све остале људске творевине (Buzan, 1991, p. 19).

Упркос ставу Чарлса Шулца (Charles Schultze) да „концепт националне безбедности не подлеже уредној и прецизној формулацији, већ се бави широким спектром ризика о чијим вероватноћама имамо мало знања и непредвиђеним околностима чију природу можемо само нејасно да уочимо“ (1973, pp. 529-30), велики број аутора је настојао да дефинише националну безбедност како у страној тако и у домаћој литератури.

Национална безбедност је појам којим се баве различите дисциплине и врло вероватно да представља централно питање студија безбедности или науке о безбедности (Липовац, 2016, стр. 29; Форца, 2019, стр. 41) па не изненађује веома велики број дефиниција овог појма.[33] Сет одређења националне безбедности представио је Бузан још у двадесетом веку у својој књизи *People, states, and fear: An agenda for international security studies in the post-cold war era*. На овом месту, тај сет одређења биће табеларно приказан (видети Табелу 2). Потом видети и Табелу 3 са дефиницијама домаћих аутора.

Табела 2: Нека одређења националне безбедности у страној литератури (Buzan, 1991, pp. 16-17)

ДЕФИНИЦИЈА	**АУТОР**
Национална безбедност је онај део владине политике чији је циљ стварање националних и међународних политичких услова који су повољни за заштиту или ширење виталних националних вредности насупрот реалним и потенцијалним противницима.	Френк Трагер и Френк Симони (*Frank Trager and Frank Simonie*), 1973, p. 36

[33] О дефинисању националне безбедности и терминолошким објашњењима видети више у: Илић, Предраг. (2012). О дефинисању и дефиницијама националне безбедности. *Војно дело* 64 (2), стр. 123-138; Маринковић, Немања. (2016). *Однос спољне политике и националне безбедности* (Докторска дисертација). Београд: Универзитет у Београду, Факултет политичких наука; Ivanović, R. Aleksandar. (2017). Pojam i elementi nacionalne bezbednosti. *Pravne teme* 5 (9), str. 186-211. Ђурчић, Милица. (2023). *Национални интерес као аналитички оквир за истраживање политике националне безбедности Републике Србије* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

Табела 2: наставак

ДЕФИНИЦИЈА	АУТОР
Национална безбедност укључује традиционалну одбрамбену политику и невојне активности државе како би у потпуности осигурала свој опстанак као политички ентитет у поретку, са циљем утицаја или остваривања својих унутрашњих и међународних циљева.	Мајкл Лоу (*Michael Louw*), 1978
(Национална) Безбедност је релативна слобода од рата, заједно са релативно високим очекивањем да пораз неће бити последица било каквог рата који би требало да се догоди.	Јан Белани (*Ian Bellany*), 1981, p. 102
(Национална) Безбедност је осигурање будућег благостања.	Лоренс Мартин (*Laurence Martin*), 1983, p. 12
Претња националној безбедности је акција или низ догађаја који (1) прети драстично и током релативно кратког временског периода да деградира квалитет живота за становнике државе, или (2) прети да значајно сузи опсег политичких избора који су доступни влади државе или приватним, невладиним субјектима (особама, групама, корпорацијама) у држави.	Ричард Улман (*Richard Ullman*), 1983, p. 133
Национална безбедност је способност нације да успешно следи своје националне интересе, како их види, било где у свету.	Пенелопе Хартланд-Тунбер (*Penelope Hartland-Thunberg*), 1982, p. 50
Национална безбедност се може дефинисати као способност да се одупре агресији из иностранства (споља).	Ђакомо Лучани (*Giacomo Luciani*), 1989, p. 151

Табела 3: Нека одређења националне безбедности у домаћој литератури (Ауторка)

ДЕФИНИЦИЈА	АУТОР
Национална безбедност одређује се као „унутрашња и спољна безбедност у односу на безбедносне изазове, ризике и претње, с једне стране, и активности специјализованих институција и система националне безбедности у остваривању државне самобитности и заштите виталних националних интереса, уз поштовање владавине права, с друге стране".	(Савић, 2007, стр. 59)
Слично претходним одређењима, Стајић и Гаћиновић националну безбедност дефинишу као „способност државе да самостално или у сарадњи са другим државама или организацијама заштити виталне вредности и интересе друштва од спољних и унутрашњих облика угрожавања и угрожености, и да самим тим обезбеди опште услове за несметан политички, економски, социјални и културни развој друштва и благостање својих грађана".	(Стајић и Гаћиновић, 2007, стр. 57)

Табела 3: наставак

ДЕФИНИЦИЈА	АУТОР
Мијалковић наводи да је национална безбедност „стање несметаног остваривања, развоја, уживања и оптималне заштићености националних и државних вредности и интереса које се достиже, одржава и унапређује функцијом безбедности грађана, националног система безбедности и наднационалним безбедносним механизмима, као и одсуство (појединачног, групног и колективног) страха од њиховог угрожавања, те колективни осећај спокојства, извесност и контрола над развојем будућих појава и догађаја од значаја за живот друштва и државе“, односно то је „безбедност и заштита друштва (становништва и нације) и државе од свеколиког (војног и невојног, унутрашњег и спољног) угрожавања, као и њихово партиципирање у сферама међународне и глобалне безбедности“.	(Мијалковић, 2009, стр. 181, 189)
У ужем смислу, национална безбедност може да представља „стање заштићеног, слободног, стабилног и извесног постојања, функционисања и развоја једне државе (земље), односно „стање у коме нема озбиљних претњи и опасности за опстанак једне државе, за њену независност, територијални интегритет, уставно-правни поредак и друге битне вредности“. У ширем смислу реч је о „свеукупности објективних и субјективних околности и чинилаца (односа, процеса, организација, институција и активности) од којих зависе опстанак, функционисање, развој и друге битне вредности једне државе (њена независност, територијална целокупност, друштвено-политички и економски поредак, њено становништво и животна средина).	(Илић, 2012, стр. 137-138)

Из изложених дефиниција уочава се да се национална безбедност одређује као унутрашња и спољна безбедност, стање заштићености независности, територијалног интегритета, поретка и свих других вредности државе од свих безбедносних изазова, ризика и претњи које се постиже активностима специјализованих институција и система националне безбедности и све то са циљем обезбеђивања функционисања и развоја државе. Употребом институционалних механизама националне вредности се штите чиме се остварују национални интереси.

Дакле, објекти заштите су друштво, држава и грађани, као и њихове вредности (*шта се штити*); субјекти и облици угрожавања су сви спољашњи и унутрашњи субјекти који својим понашањем стварају облике и доводе до угоржавања (*од чега*); субјекти заштите су држава и сви субјекти (државни и недржавни) који чине систем националне безбедности (*ко штити*); средства и методе заштите су сви механизми које користе субјекти заштите (*чиме/како се штити*).

Из приложених дефиниција могуће је уочити и неке специфичности националне безбедности. Национална безбедност стављена је у политички контекст, са акцентом на државу, њене вредности и интересе. Као најважније елементе дефиниције националне безбедности могуће је издвојити следеће: државна самобитност (суверенитет, независност и територијалну целовитост); безбедност националног окружења; унутрашња и спољна безбедност државе у односу на изазове, ризике и претње; активности националних безбедносних институција путем организованих специфичних апарата државе, и безбедност државе и заштита виталних вредности друштва у функцији слобода и права грађана (Савић, 2006, стр. 58). Поједностављено, реч је о стању безбедности и заштићености свих вредности и интереса државе од свих угрожавања без обзира да ли су војна или невојна, да ли су спољашња или унутрашња. Према системском

приступу, остваривање националне безбедности се посматра кроз систем националне безбедности. Уједно систем националне безбедности јесте апарат који обезбеђује националну безбедност схваћену као стање.

Национална безбедност увек зависи од неких чинилаца. Неки од унутрашњих чинилаца од којих у великој мери зависи стање националне безбедности јесу економски раст и развој, просперитет; социјална равномерност, праведност и равнотежа; одговорна и сразмерна елита моћи и власти; компромис и консензус око стратешких циљева и јединственог стратешког опредељења и поуздана савезништва (Кнежевић, 2016, стр. 122). На овом месту, нема потребе задржавати се на анализи свих наведених чинилаца. Довољно је указати на то да од њих зависи како понашање државе изнутра, тако и њено деловање према окружењу, чији фактори такође у извесној мери одређују њену националну безбедност. Окружење (нпр. социоекономски и политички контекст или политичке, културолошке и етничке контрадикције које могу да постоје) игра значајну улогу у организовању националне безбедности. Анализа и разумевање актуелних безбедносних токова од суштинске је важности у креирању адекватних политика безбедности које треба да обликују стање и систем безбедности. Наиме, „на бази анализе безбедносног окружења и идентификовања изазова, ризика и претњи безбедности, утврђују се националне вредности, интереси и циљеви и пројектује начин њихове одбране и заштите, организовањем адекватног система националне безбедности“ (Forca, 2021, str. 423).

Да би се приступило појмовном одређењу стања и система националне безбедности било је неопходно осврнути се на дефиницију националне безбедности. Систем националне безбедности обухвата функцију и структуру на подручју националне безбедности, које не делују самостално већ и заједно са осталим друштвеним подсистемима ради даљег развоја друштва (Гаћиновић, 2017, стр. 94). Стање националне безбедности постиже се управо безбедносном делатношћу система националне безбедности.

Дакле, о систему националне безбедности се може говорити одређењем националне безбедности, а национална безбедност се пак, попут безбедности, може посматрати као систем, функција, организација или стање.[34] На овом месту, национална безбедност ће бити анализирана као систем и то уважавајући неколико ставова. Прво, „у теорији и нормативном уређењу ове функције најчешће се говори о систему или сектору националне безбедности“ (Ковач, 2010, стр. 143); друго, (национална) безбедност се „најсвеобухватније може одредити као систем“ (Мијалковић и Поповић, 2015, стр. 111); и треће, у домаћој националној регулативи користи се појам систем националне безбедности (Стратегија националне безбедности Републике Србије, 2019).

2.2. Општа разматрања о систему националне безбедности

На националном нивоу, савремене државе обезбеђују безбедност својих грађана кроз деловање својих система националне безбедности. Ефикасност ових система данас одражава не само способност држава да заштите своје основне друштвене вредности од унутрашњих и спољашњих претњи (тј. да одрже мир и гарантују слободу), да спрече опасност и страх, већ и њихову способност да обезбеде друштвени развој, и као благостање њиховог становништва (Grizold, 1994, str. 44). Систем националне безбедности један је од основних конституенаса савременог друштва. Од њега зависи да ли ће се остваривањем националних интереса попут очувања суверености, независности

[34] Видети више у: Стајић, Љубомир. 2015. *Основи система безбедности – са основама истраживања безбедносних појава*. Нови Сад: Правни факултет у Новом Саду.

и територијалне целовитости, унутрашње стабилности и безбедности, идентитета постићи и заштити националне вредности, као што су слобода, независност, безбедност, демократија и владавина права, социјална правда и једнакост. Стога, он није сам по себи циљ или сврха већ инструмент којим држава остварује своју функцију безбедности.

Са теоријског аспекта, страни и домаћи аутори понудили су завидан број дефиниција. Ради прегледности, неке од њих представљене су у табели која следи (видети Табелу 4).

Табела 4: Дефиниције система националне безбедности (Ауторка)

ДЕФИНИЦИЈА	**АУТОР**
Систем националне безбедности данас представља „синтезу свих подсистема у друштву, јер обезбеђује основне услове неопходне за опстанак и развој друштва и квалитет живота, као и активности усмерене на јачање способности друштва и природе да издрже опасност“. Такође помаже у отклањању последица које изазивају извори опасности.	(Grizold, 2000, str. 128)
Група домаћих аутора систем националне безбедности дефинише као „облик организовања и функционисања друштва у спровођењу мера и радњи на превентивном и репресивном плану, које се предузимају ради очувања виталних вредности једног друштва од свих извора и облика угрожавања“.	(Стајић, Мијалковић и Станаревић, 2004, стр. 135)
Реч је о скупу „функционално повезаних државних органа, органа локалне самоуправе и других организација, који делујући у складу са правним поретком државе теже да заштите унутрашњу и спољну безбедност државе, друштва и грађана“.	(Драгишић, 2011, стр. 17)
Систем националне безбедности је „облик организовања и функционисања друштва у спровођењу мера и активности на превентивном и репресивном плану, које се предузимају ради очувања суверенитета и интегритета државе, уставом утврђеног поретка, права и слобода грађана, као и свих осталих друштвених и међународних вредности од свих облика и носилаца угрожавања, без обзира на место и време извршавања“.	(Стајић, 2015, стр. 41)
Национални систем безбедности, у ширем смислу, обухвата све потенцијалне (природне, људске, материјално-техничке, нормативно-политичке и институционалне ресурсе) једне земље, који су ангажовани на очувању виталних националних и државних, али и међународних и глобалних вредности и интереса. У ужем смислу, то су само делови ових ресурса који су специјализовани и професионално, легално и легитимно, директно или индиректно, реализују функцију националне безбедности. Конкретније, национални систем безбедности је форма организовања и функционисања државе и друштва у спровођењу превентивних, репресивних и санационих мера и радњи којима се националне вредности и интереси достижу/остварују, унапређују, омогућава њихово уживање и штите од безбедносних изазова, ризика и претњи, односно ревитализују уколико су угрожени.	(Мијалковић, 2015, стр. 242)

Из наведених дефиниција издваја се следеће: Систем националне безбедности јесте друштвени систем који има своју структуру и организацију, функцију и активности и ресурсе, који му омогућавају да проактивно и реактивно[35] делује у циљу заштите националних вредности и остваривања интереса од свих претњи без обзира на место и време њиховог испољавања. Систем националне безбедности као друштвени систем представља организациони систем који је уређен стратегијом (и политиком) националне безбедности која одређује хијерархијски устројену структуру и циљеве. Као део који постоји у ширем друштвеном контексту – као подсистем ширег друштвеног система, систем националне безбедности не функционише сам и само за себе – он није сам себи сврха. На функцију система утичу како његови елементи и карактеристике, тако и други системи и окружење. Исто тако, систем својим функционисањем утиче на друге системе и друштвено окружење. Систем националне безбедности има трајан карактер јер је потреба за безбедношћу националних вредности трајна.

2.3. Систем унутрашње безбедности као извршни део система националне безбедности

Из текста који је претходио, изводи се закључак да се систем националне безбедности структурално најопштије може поделити на управљачки и извршни део. За потребе рада фокус се усмерава на извршни део и његов подсистем – унутрашњу безбедност. Тако, изршни део система националне безбедности чине систем одбране, систем унутрашње безбедности, безбедносно-обавештајни систем и други субјекти значајни за националну безбедност. Систем унутрашње безбедности поред надлежних органа државне управе, чине и правна лица, предузетници и физичка лица која врше послове приватног обезбеђења.

Систем унутрашње безбедности јесте неизоставна компонента сваког система безбедности, која се јавља као одговор на унутрашње појаве угрожавања (Стајић, 2015, стр. 44). У домаћој националној регулативи, унутрашња безбедност се дефинише као систем који је намењен „за обављање послова којима се обезбеђује безбедност грађана и имовине, пружа подршка владавини права, обезбеђују Уставом и законом утврђена људска и мањинска права и слободе, спроводе превентивне и оперативне мере и извршавају задаци заштите и спасавања људи и добара од последица елементарних непогода и других несрећа, укључујући и мере опоравка од тих последица (Стратегија националне безбедности Републике Србије, 2019, 5). Наведено одређење би било потпуније да садржи и део о начину на који се штити, или којим активностима (Марковић, 2023а, стр. 81). С обзиром на то да на овом месту није циљ детаљно разматрати унутрашњу безбедност са аспетка теорије система, избећи ће се разрада у том погледу и фокус ће се ставити на ближе разумевање унутрашње безбедности и њеног односа са другим елементима националне безбедности.

У контексту наведеног, правећи разлику између унутрашње и спољне безбедности, Мијалковић прву дефинише као „заштићеност виталних друштвених вредности и интереса унутар граница земље, од угрожавајућих појава које првенствено настају изнутра или су комбиноване (потпомогнуте) са угрожавајућим факторима који долазе споља“, где под виталним друштвеним вредностима подразумева пре свега уставно

[35] Проактивно и реактивно су два појма која ће се провлачити кроз текст рада. У вези са тим, пожељно је приложити и одређења ова два појма (Мандић и Станојевић, 2020, стр. 39). Проактивно значи елиминацију и/или смањење услова који погодују наступању штетног догађаја, што значи да проактивно делује на услове да се догађај не догоди. Реактивно значи елиминацију и/или смањење последица штетног догађаја, пошто он већ наступи, што значи да реактивно делује на последице.

уређење, политички, социјални и економски систем, људске слободе и права и животну средину (2015, стр. 85). Унутрашња безбедност се може сагледати и са аспекта референтних објеката и референтних субјеката. У контексту тога, политички и друштвено-економски поредак, уставно-правни поредак и јавни ред и мир су референтни објекти, док је систем националне безбедности државе референтни субјекат (Ivanović, 2017, str. 202). Иако би можда, прецизније било рећи да је референтни субјекат систем унутрашње безбедности, с обзиром на његову уску повезаност са осталим сегментима система националне безбедности, оправдано је задржати првобитно тумачење (Марковић, 2023а, стр. 81-82).

„Према непосредном објекту заштите" као референтном објекту (Милошевић, 2001, стр. 3) могуће је направити дистинкцију између државне и јавне безбедности као компоненти унутрашње безбедности. Државна безбедност обухвата заштиту политичког, друштвено-економског и уставно-правног поретка, док јавна безбедност обухвата заштиту јавног реда и мира (Ivanović, 2017, str. 201). Оба наведена правца заједно са „законом одређеним пословима управе" чине област унутрашњих послова (Милетић и Талијан, 2011, стр. 9). Поред државне и јавне безбедности, аутори са једне стране, одређују и војну безбедност (Милошевић, 2001, стр. 3; Милетић и Талијан 2011, стр. 9), односно са друге стране, додају заштиту и спасавање у ванредним ситуацијама и, у најширем смислу, заштиту животне средине (Форца, 2019, стр. 62) као део шире (унутрашње) безбедности. Овакво тумачење указује на корелацију између унутрашње и јавне безбедности као корелацију вишег и нижег појма.

Између ова два појма могуће је ставити знак једнакости.[36] Када се први разлика између спољне и унутрашње безбедности уствари се прави разлика између националне и јавне безбедности. Прва се традиционално односи на одбрану од спољне агресије, док се унутрашњом, односно јавном безбедношћу одржава јавни ред и мир (Станаревић, 2018, стр. 197).

Постоје аутори који безбедност деле на унутрашњу (индивидуална, социјетална и национална) и међународну (регионална, глобална, заједничка, колективна и кооперативна) безбедност (Стајић и Гаћиновић, 2007, стр. 35). Тако се унутрашња безбедност, која се „често поистовећује са заштитом економске, политичке, правне и социјалне сигурности грађана" (Ђукић, 2019, стр. 71) састоји од индивидуалне, социјеталне и националне безбедности, и сходно томе, национална безбедност је виши појам од унутрашње безбедности.

На основу изнетих тумачења, могуће је закључити да је реч о „концепту којим се обезбеђује заштита и континуирано функционисање унутрашњег уставног поретка, друштвеног, политичког, правног, економског, еколошког и сваког другог система на којем почивају вредности једног друштва и државе". Ови циљеви остварују се интегрисаним деловањем субјеката унутрашње безбедности, који су подељени у две групе: 1) надлежне органе државне управе и 2) правна лица, предузетнике и физичка лица која врше послове приватног обезбеђења (Марковић, 2023а, стр. 83).

[36] Уколико се у разматрање узме концепт унутрашње безбедности и његова разрада у сратешким документима наше земље – у стратегијама националне безбедности термин јавна безбедност се не користи, у Закону о полицији се користи у контекстима поступања полиције у стању повећаног ризика по стање јавне безбедности и израде процене јавне безбедности (Закон о полицији 2016, чланови 24, 25 и 29). Из наведеног, уочава се терминолошка неусклађеност како између аутора који су се бавили овом тематиком, тако и у оквиру нормативних докумената, што представља озбиљну препреку разумевању ових концепта и њихових корелација (Марковић, 2023а, стр. 82-83).

2.4. Јавна и приватна безбедност у систему националне безбедности

У контексту ранијих теоријских схватања и поделе безбедности да јавну и државну, прва се схватала као „стање заштићености јавног поретка“ (јавних интереса заштићених општим или појединачним правима), односно „заштита грађана и њихове имовине у држави“ (Милошевић, 2001, стр. 5). Аутори Милетић и Талијан се надовезују на наведено сматрајући да безбедност грађана у ширем смислу у виду заштите од свих врста угрожавања, по свом садржају, одговара појму јавне безбедности (2011, стр. 14).

Јавна безбедност се још може одредити према два мерила – органско и функционално. Према органском мерилу, сва питања из надлежности полиције јесу питања која се сврставају у област јавне безбедности. Са друге стране, према функционалном мерилу, сва питања која омогућавају остваривање јавне безбедности, без обзира у чијој надлежности се налазе, сврставају се у област јавне безбедности. Такође, јавна безбедност има два појавна облика: први је да се у области јавне безбедности манифестује јавни (општи) интерес који се конкретизује кроз остваривање безбедности свих људи, и други је да се у области јавне безбедности манифестује лична (индивидуална) безбедност човека, кроз његову заштићеност од опасности (Милетић и Талијан, 2011, стр. 10). На основу прве дистинкције, могуће је уочити да схваћена у функционалном смислу, јавна безбедност обухвата доста шири спектар послова, невезујући се стриктно за полицију. Сходно наведеном, могуће је јавну и унутрашњу безбедност поставити у исту раван.

Полиција се одувек сматрала традиционалним субјектом јавне безбедности. Све до приватизације јавне безбедности она је сматрана и главним субјектом, а данас, полиција „најчешће“ (Милетић и Талијан 2011, стр. 9) спроводи послове јавне безбедности. Према Ратку Марковићу, основна функција полиције као државног органа везује се за јавни поредак, и у првом реду, превенцију његовог нарушавања, репресију против оних који га нарушавају и стварање и одржавање услова стабилизације јавног поретка (2010, стр. 355). Управо услед приватизације безбедности, јавна безбедност се може поделити на традиционални јавни сектор и приватни сектор (Савић, 2007, стр. 72), тако да су поред полиције у остваривању јавне безбедности задужени и приватни субјекти. Данас, приватна безбедност има великог утицаја на јавну безбедност, те држава треба и мора да „гарантује квалитет услуга“, првенствено успостављањем ефикасног надзора над законитошћу рада оних који те услуге пружају (Кековић, 2011, стр. 217).

У контексту разумевања јавне безбедности, аутори (Даничић и Стајић, 2008, стр. 15; Мијалковић и Поповић, 2015, стр. 195; Kesić, 2009) често обухватају и полицијско деловање или „полисинг“[37], те праве разлику између јавног (енг. *Public Policing*) и приватног „полисинга“ (енг. *Private Policing*). У прилог овој тези се најпре може приложити извештај из 1985. године који документује убрзани раст ресурса приватне безбедности и говори о фундаменталном померању одговорности примарне заштите са јавног на приватни сектор (Cunningham and Taylor, 1985). Такав развој сматра се и олакшаним „фундаменталним променама у природи имовинских односа“ (Shearing and Stenning, 1981, p. 193).

Историјско разграничење између јавног и приватног „полисинга“ је међутим доста нејасно, јер се раније јавне функције поверавају приватним пружаоцима услуга (Zedner, 2006, p. 272). Постоји став да на овом месту није реч о подели рада између јавне и приватне полиције већ расподела „полисинга“ са приватним сектором (Shearing, 1992, p. 411). Данас се ова два сектора разликују по институционалном уређењу, заузимају

[37] „Полисинг“ (енг. *Policing*) се одређује као полицијско деловање или рад полиције. Како је термин присутан и у страној и у домаћој литератури, у раду ће се користити у овој форми.

прилично одвојене позиције у друштву и имају сасвим различите улоге и одговорности (Stenning, 2009, p. 23). У почетку, модерна приватна полиција била је манифестација политике дозвољавања самоодбране (која је првобитно била обезбеђена интерно, а потом и доступна унутар услужне делатности), па њено регулисање није изазивало забринутост (Shearing, 1992, p. 411). Данас, њихова нормативна уређеност се такође разликује. Док је јавни „полисинг" задужен да ради у јавном интересу, приватни „полисинг" је уређен тако да јавност буде заштићена и од њега (нпр. осигуравајући да у њих не инфилтрирају криминалци или не покушавају да врше овлашћења која немају) (Stenning, 2009, p. 24). Према Стенингу (Stenning) то је разлог зашто је у већини јурисдикција уговорни сектор безбедности (комерцијалне фирме које пружају услуге обезбеђења клијентима по уговору), а не интерни сектор (одељења безбедности, која пружају услуге обезбеђења за организацију која их запошљава) предмет државне регулативе (2000, p. 339).[38] У Републици Србији, законска регулатива која уређује област приватног обезбеђења, а о којој ће детаљније бити речи у наредном поглављу, са једне стране уређује питања приватног обезбеђења (као уговорни сектор безбедности), док са друге стране уређује самозаштитну делатност (као интерни сектор, или бар његов део).

Док је за јавни „полисинг" одговорна полиција, а пре свега кроз „рад полиције у заједници", приватни „полисинг" у најширем облику обухвата полицијско деловање грађана, приватно обезбеђење и приватну истражитељску делатност (Мијалковић и Поповић, 2015, стр. 195).[39] У литератури се може наћи и детаљнија класификација по којој у приватни „полисинг" спадају волонтери (нпр. посматрање комшилука), правно лице за комерцијалну безбедност, специјалисти запослени у профитним или непрофитним организацијама (нпр. службеници обезбеђења, чувари, патрола), запослени који нису специјалисти у профитним или непрофитним организацијама (запослени са општијим дужностима од којих се ипак тражи да обрате пажњу на безбедносна питања, нпр. посада авиона) и јавна полиција (службеници су ван дужности или раде прековремено за приватног купца или су на дужности, али су посвећени специфичној полицијској операцији коју на нивоу агенције плаћа приватни клијент) (Sparrow, 2014, p. 2). Приватни „полисинг", схваћен на овај начин, чини интегрални део система унутрашње безбедности, док се приватна безбедност може сматрати за „оперативни" део приватног „полисинга" (Давидовић, 2011, стр. 460). Дакле, приватни „полисинг" као део полицијског деловања јесте веза између система унутрашње безбедност са једне стране и приватног обезбеђења са друге стране; или је полиција веза између приватне и јавне безбедности (Даничић и Стајић, 2008, стр. 15), а тиме и између приватне безбедности и система националне безбедности.

На основу ставова бројних аутора, Кесић је препознао извесне паралеле између јавног и приватног сектора безбедности. Према томе, јавни сектор безбедности карактерише: финансирање из буџета, рад у јавном интересу, обухвата све безбедносне услуге, оријентисан је на претњу, усмерен на смањење стопе криминалитета, реактивно делује, има централизовану бирократију, строго је контролисан и има интензивну обуку. Са друге стране, приватни сектор безбедности карактерише: финансирање од сопствених профита, рад у приватном интересу, обухвата селективне безбедносне услуге, оријентисан је на власништво, усмерен на смањење губитака, проактивно делује, има фрагментисану организацију, мање је контролисан и има минималну обуку (Kesić, 2009, str. 68-69).

[38] О регулисању интерног сектора приватног „полисинга" (приватне безбедности) видети више у: Stenning, Philip. 2009. Governance and accountability in a plural policing environment – The story so far. *Policing: A Journal of Policy and Practice* 3 (1), pp. 22-33, стр. 29.

[39] Упоредити са и видети шире у: Joh, E. Elizabeth. 2005. Conceptualizing the Private Police. *Utah Law Review,* 2005 (2), pp. 573-617; Kesić, Zoran. 2009. *Privatni sektor u kontroli kriminaliteta*. Beograd: Dosije studio.

Термин приватна безбедност (енг. *Private Security*) користи се да означи „читав скуп делатности обезбеђивања имовине, лица и пословања које врше приватна правна лица за пружање услуга обезбеђења". У страној литератури, користе се и изрази „индустрија (привреда) приватне безбедности" (енг. *Private Security Industry*) и „приватна полиција" (енг. *Private Police*), док је сам термин приватна безбедност тесно повезан са појмом приватни „полисинг" (енг. *Private Policing*) (Давидовић, 2011, стр. 456; Kesić, 2009, str. 33).[40] Заправо, велики број страних аутора опредељује се за термине приватни „полисинг" и приватна полиција (Stenning, 2000, p. 326).

У литератури се могу наћи дефиниције приватне безбедности са извесним разликама у њиховом садржају. Пионири истраживања приватне безбедности у Сједињеним Америчким Државама указују на то да она „почиње тамо где јавна полиција престаје и да стога не задире у јавну полицију" (Shearing and Stenning, 1981, p. 220), јер она предузима оно што „јавно полиција или не ради због ограничења ресурса или не може да ради због законских ограничења" (Kakalik i Vildhorn, 1971, p. 19). Ово је једноставна дефинција која ипак не нуди много. Са друге стране, детаљније одређење односило би се на „запослене појединце и организације/правна лица који за новац пружају безбедносне услуге клијентима, појединцима или организацијама који их ангажују или су их запослили, а у циљу заштите особља, приватне имовине и интреса тих клијената од различитих облика угрожавања" (Dempsey, 2010, p. 2). Слична одређења дају и други аутори (South, 1994, p. 220; Kalesnikas, 2003, p. 22). Свеобухватније дефинисана, приватна безбедност је „планска и организована самостална или заједничка дјелатност и функција појединаца, организација, приватних или професионалних агенција, усмјерених на сопствену заштиту или заштиту других, као и заштиту одговарајућих лица, простора, објеката, пословања или дјелатности, а који нису покривени ексклузивном заштитом државних органа" (Даничић и Стајић, 2008, стр. 14).

Страни и домаћи аутори су као адекватну препознали дефиницију коју је дало Америчко друштво за индустријску безбедност, а које приватну безбедност дефинише као „невладину праксу приватног сектора заштите људи, имовине и информација, спровођења истрага, и на други начин чување имовине организације" и која има улогу у „помагању приватном сектору да обезбеди своје пословање и критичну инфраструктуру, било од природне катастрофе, несрећа или планираних акција, као што су терористички напади, вандализам..." (Strom et al., 2010, pp. 2-3; Кековић и Димитријевић, 2017, стр. 235).

Из наведених дефиниција уочљиво је да приватна безбедност обухвата послове који не потпадају у надлежност државе, односно њених органа, да се послови обављају у два правца – или за сопствене потребе или за потребе других уз новчану надокнаду и увек са циљем заштите лица, имовине (простора, објекатата, информација) и пословања (делатности), од било каквог облика угрожавања.

Конкретно, послови приватне безбедности се могу различито класификовати. Обично се они групишу у делатности, па је одатле могуће направити разлику између услуга физичког обезбеђења, услуга техничког обезбеђења и истражитељске делатности (Newburn and Reiner, 2012, p. 823). Оваква подела могла би да одговара уколико приватну безбедност посматрамо у ужем смислу, односно више као приватно обезбеђење. Друга класификација коју наводимо прави разлику између криминалистичких истрага, корпоративне безбедности, приватних истрага и физичке заштите (Murray and McKim,

[40] О односима појмова „полисинг" (policing) и полиција (police) видети више у: Newburn, Tim and Reiner, Robert. 2007. „Policing and the police". In: M. Maguire, R. Morgan, and R. Reiner (Eds.). *The Oxford Handbook of Criminology* (pp. 910-952). Oxford: OUP; Давидовић, Душан. 2011. Приватна безбедност у Србији. У В. Н. Цветковић (Ур.), *Ризик, моћ, заштита – Увођење у науке безбедности* (стр. 452-467). Службени гласник и Универзитет у Београду, Факултет безбедности.

2003, p. 637). Ова класификација више одговара пословима оног дела приватне безбедности који је повезан са полицијом, па бисмо поново пре могли говорити о приватној безбедности у ужем смислу.

Врло свеобухватна класификација услуга приватне безбедности развијена је од стране експерата који су присуствовали симпозијуму Америчког друштва за индустријску безбедност. Они су идентификовали 18 елемената: физичко обезбеђење, кадровско обезбеђење, безбедност информационих система, истраге, спречавање губитка, управљање ризиком, правни аспекти, планирање за непредвиђене и ванредне ситуације, противпожарна заштита, управљање кризама, управљање катастрофама, борба против тероризма, конкурентска интелигенција, извршна заштита, насиље на радном месту, спречавање криминала, превенција криминала кроз пројектовање животне средине и безбедносна архитектура и инжењеринг (ASIS Foundation, 2009, p. 4).

Оно што се међутим може приметити јесте да се ни у једној од наведених одређења не спомињу послови приватних војних компанија. То се може оправдати чињеницом да се у литератури прави дистинкција између приватних компанија које обезбеђују безбедносне услуге и оних које пружају војне услуге, о чему је детаљније написано у тексту који следи.

Као закључак одређења приватне безбедности, правимо разлику између:

- **приватне безбедности у ужем смислу** или приватно обезбеђење (приватни „полисинг“) и
- **приватне безбедности у ширем смислу** или индустрија приватне безбедности

На основу изведене класификације, корпоративна безбедност се може посматрати као део приватне безбедности у ужем смислу или приватног обезбеђења. У вези са тим, адекватно је разликовање корпоративне безбедности и уговорног обезбеђења као два сектора приватног обезбеђења. Прва се одређује као безбедносна функција у власништву организације и којом се управља у оквиру организације, а друга се састоји од организација које продају и пружају своје безбедносне производе и услуге другим организацијама, институцијама и приватним лицима (Kovacich and Halibozek, 2003, p. 48-49). Међутим, како је корпоративна безбедност значајан део недржавног сектора безбедности поред приватних безбедносних и војних компанија и детективске делатности, она се сасвим оправдано може посматрати и као део ширег оквира – индустрије приватне безбедности.

Синтагма „недржавни сектор безбедности“ често се погрешно користи као синоним за приватну безбедност. Најпре, тек ако се недржавни сектор безбедности схвати у ужем смислу као „правно утемељене делатности професионалног типа, које су организоване ради пружања одређених безбедносних услуга“ (Trivan, 2012, str. 171) могуће је ставити знак једнакости. У супротном, појам „недржавни сектор безбедности“ шири је од појма „приватне безбедности“ јер садржински, поред делатности приватних фирми и агенција за пружање различитих безбедносних услуга на комерцијалној основи, обухвата и специфичне послове корпоративне безбедности“ (Trivan, 2012, str. 172). Овакво схватање јасно повлачи паралелу између приватне безбедности недржавних субјеката и јавне безбедности државних служби. За недржавни сектор безбедности често користи и синтагма „цивилна безбедност“. Тиме се наглашава супротност традиционалном поимању националне безбедности као заштићености државних интереса средствима војне, политичке и економске моћи. Ипак, како није јасно да ли је реч о безбедности цивила (грађана) или о безбедности коју пружају невојни (недржавни) субјекти, аутор сматра да овакво изједначавање није оправдано (Мијалковић, 2015, стр. 102).

Уважавајући друго одређење недржавног сектора безбедности, могуће је направити разлику између профитних и непрофитних субјеката тог сектора. Профитни субјекти недржавног сектора безбедности, по принципима тржишне економије, пружају услуге безбедности за договорену надокнаду, и по правилу су регистровани за обављање те делатности. Са друге стране, непрофитни субјекти јесу они који у оквиру своје делатности могу да решавају безбедносне проблеме, али то није њихова основна или регистрована делатност. У прву групу спадају они субјекти који се називају и приватним компанијама (у области безбедности), док у другу групу спадају невладине организације, хуманитарне организације, удружења грађана (Trivan, 2014, str. 36).

2.5. Национална безбедност и систем националне безбедности Републике Србије – начин организовања система националне безбедности

Национална безбедност Републике Србије и њен систем на овом месту се посматрају искључиво кроз главни стратегијски документ у области безбедности, а то је Стратегија националне безбедности Републике Србије из 2019. године. То је „највиши стратешки документ чијом реализацијом се штите национални интереси Републике Србије од изазова, ризика и претњи безбедности у различитим областима друштвеног живота“ (Закон о одбрани, 2007, члан 4, став 1), која представља „полазну основу за израду других стратешких и доктринарних докумената, докумената јавних политика и нормативно-правних аката … ради очувања и заштите безбедности грађана, друштва и државе“ и којом се „представљају основна стратешка опредељења Републике Србије у области националне безбедности“ (Стратегија националне безбедности Републике Србије, 2019). Са друге стране, ставови који су заузетих у стратегији националне безбедности операционализују се кроз политику унутрашње безбедности (Стајић, Радивојевић и Мирковић, 2017, стр. 1340). Из приложених одредаба, одлука о избору предмета анализе садржаја се намеће као исправна и довољна с обзиром на предмет овог истраживања.

Национална безбедност Републике Србије одређује се у објективном и у субјективном смислу. У објективном, то је „објективно стање заштићености њених националних вредности и интереса од свих облика угрожавања“, док у субјективном представља „субјективан осећај безбедности грађана Републике Србије“ (Стратегија националне безбедности Републике Србије, 2019). Национална безбедност зависи и уједно представља „резултат утицаја стратегијског окружења и предузетих мера и активности државних органа и институција у извршавању безбедносних функција, те деловања других субјеката у свим областима друштвеног живота“ (Стратегија националне безбедности Републике Србије, 2019).

Национална безбедност Републике Србије постиже се њеним системом националне безбедности. Наиме, улога система националне безбедности јесте да „обезбеди“ безбедност као једну од основних функција државе од којих зависи опстанак и развој.

Када је реч о одређењу система безбедности, односно система национане безбедности са нормативног аспекта, Устав Републике Србије, као највиши правни акт, користи неуједначену терминологију безбедности, попут појмова безбедности, јавне безбедности или националне безбедности, али не користи појам „систем (националне) безбедности“. Тако, са нормативног аспекта, систем националне безбедности дефинисан је једино у *Стратегији националне безбедности Републике Србије*. У наведеном документу систем националне безбедности одређен је тако да „представља нормативно, структурно и функционално уређену целину, која се састоји од управљачког и извршног дела са прецизно утврђеним надлежностима и одговорностима и чијом се делатношћу

обезбеђује свеобухватно и усклађено управљање и деловање у извршавању послова и задатака ради превенције, ублажавања и неутралисања изазова, ризика и претњи безбедности и отклањања последица њиховог испољавања, са крајњим циљем заштите и остваривања националних интереса Републике Србије“ (Стратегија националне безбедности Републике Србије, 2019, 5).

Из приложене дефиниције уочава се циљ система, а то је на првом месту заштита националних интереса. Стратегија националне безбедности Републике Србије као националне интересе наводи: очување суверености, независности и територијалне целовитости; очување унутрашње стабилности и безбедности; очување постојања и заштита српског народа где год он живи, као и националних мањина и њиховог културног, верског и историјског идентитета; очување мира и стабилности у региону и свету; европске интеграције и чланство у Европској унији; економски развој и укупни просперитет и очување животне средине и ресурса Републике Србије. Сви наведени интереси (укупно 7) операционализовани су на 33 циља. Национални интереси су од значаја, између осталог, јер се „остваривањем националних интереса штите основне националне вредности“. У основне националне вредности Стратегија националне безбедности Републике Србије убраја следеће: слобода, независност, мир, безбедност, демократија, владавина права, социјална правда, људска и мањинска права и слободе, једнакост и равноправност грађана, толеранција, транспарентност, солидарност, родољубље и здрава животна средина (Стратегија националне безбедности Републике Србије, 2019, 3).

Дакле, национални интереси се операционализују на циљеве да би се њиховом реализацијом одбраниле националне вредности. Схваћене на овај начин, националне вредности су „више“ у односу на националне интересе. То потврђује и став да су вредности „константа и као такве, најчешће, утврђују се највишим правним актом држав, док су Интереси и циљеви променљива категорија (Forca, 2021, str. 434). Уважавајући редослед представљања националних интересау највишем стратешком акту наше земље, и више је него јасно да је брига за независност и самосталност од суштинског значаја за остваривање свих осталих интереса и свих националних вредности. У првом реду, то је опстанак државе и друштва, препознат као једна од најопштијих и уједно стратешких вредности свеукупне националне безбедности.

Даље, из приложене дефиниције уочава се и структура система и заједно са њом субјекти који суделују у остваривању националне безбедности. Структуру система чине управљачки и извршни део, односно државни органи, Народна скупштина, председник Републике, Влада и Савет за националну безбедност као управљачки део и систем одбране, систем унутрашње безбедности, безбедносно-обавештајни систем и други субјекти значајни за националну безбедност као извршни део (Стратегија националне безбедности Републике Србије, 2019, 5.1.).

Са аспекта предмета рада, издваја се систем унутрашње безбедности[41] који поред надлежних органа државне управе, у свом саставу има правна лица, предузетнике и физичка лица која врше послове приватног обезбеђења. У прву групу спадају службе безбедности, министарство надлежно за унутрашње послове, правосудни органи, док другу

[41] Уколико се у разматрање узме концепт унутрашње безбедности и његова разрада у стратешким документима наше земље – стратегијама националне безбедности Републике Србије из 2009. и 2019. године, чини се да је учињено назадовање. У стратегији из 2009. године политика унутрашње безбедности препозната је као посебан елемент у оквиру политике националне безбедности. То није случај са тренутно важећом стратегијом у којој се обрађује свеобухватна политика националне безбедности без политике унутрашње безбедности. Иако су одређене одредбе претходне стратегије сасвим оправдано изостављене постоје одредбе које је требало задржати новом стратегијом (Марковић, 2023а, стр. 89).

групу чине субјекти из области приватног обезбеђења.[42] Поред система унутрашње безбедности издвајају се и други субјекти значајни за националну безбедност у које се убрајају органи државне управе и институције надлежне за спољне послове, правосуђе, здравство, демографију, људска и мањинска права, економију, образовање и научну делатност, привреду, енергетику, телекомуникације, саобраћај и транспорт, инфраструктуру, заштиту животне средине, културу, затим органи аутономних покрајина и јединица локалне самоуправе, организације цивилног друштва, медији, правна лица и грађани који доприносе остваривању циљева националне безбедности (Стратегија националне безбедности Републике Србије, 2019, 5.1.2.).

Функције система националне безбедности треба разумети са два аспекта. Са једне стране, системска функција (мисија, циљ, улога) система националне безбедности јесте безбедност државе и грађана. Са друге стране, функције система националне безбедности, као подсистема државе, испољене као послови, активности и одређене мере, јесу: управљање, одбрана, заштита, безбедносно-обавештајна функција, функција приватне и корпоративне безбедности, контрола и надзор и санкционисање (Форца, 2019, стр. 66). Деловање система националне безбедности преко којег се остварује системска (безбедносна) функција усмерено је у два правца – проактивно и реактивно. Управо је извршни део система националне безбедности одговоран како за проактивно деловање, тако и за ефикасно реаговање и отклањање последица угрожавања безбедности у циљу очувања националних вредности и заштите и остваривања националних интереса (Стратегија националне безбедности Републике Србије, 2019, 5.1.).

2.5.1. Однос система националне безбедности према корпоративној/приватној безбедности

Концепт корпоративне безбедности није усвојен у нормативним актима Републике Србије. У вези са тим, две су могуће анализе које се могу спровести. Најпре, могуће је анализом обухватити начин на који је приватна безбедност обухваћена нормативним оквиром националне безбедности, што је представљено на овом месту. Друго, могуће је анализом обухватити начин на који су појединачне области (функције) корпоративне безбедности обухваћене нормативним оквиром од којег зависи и национална безбедност, а што је представљено у наредном поглављу. Однос система националне безбедности према приватној безбедности могуће је сагледати као однос вишег и нижег система и организације. Одатле проистиче да је однос система националне безбедности према корпоративној безбедности могуће сагледати на исти начин.

У тексту који је претходио, у највишем стратешком документу Републике Србије, субјекти приватног обезбеђења су препознати као један од субјекта или елемената система унутрашње безбедности извршног дела система националне безбедности. У тексту Стратегије националне безбедности, уочава се употреба различитих термина када се говори о приватном обезбеђењу. На једном месту се помињу службе и агенције за обезбеђење личности и објеката (када се дефинише извршни део система), док се на другом месту помињу правна лица, предузетници и физичка лица која врше послове приватног обезбеђења (када се наводе субјекти система унутрашње безбедности извршног дела система) (Стратегија националне безбедности Републике Србије, 2019, 5.1.2.).

Област приватног обезбеђења, условно речено, добила је свој матични закон 2013. године. Од тада је нормативно уређена област приватног обезбеђења, или конкретније, рад правних

[42] У раду се брани став групе аутора да би адекватан термин био *субјекти приватне безбедности*, „чији су субјекти приватног обезбеђења део, поред субјекта из области детективске делатности и тзв. приватних војних компанија“ (Стајић, Радивојевић и Мирковић, 2017, стр. 1337).

лица и предузетника који врше послове приватног обезбеђења, рад службе обезбеђења и редара. Регулисањем ове материје, обухваћена је и сарадња са другим субјектима система националне безбедности тако што је Министарство унутрашњих послова овлашћено да врши надзор испуњености услова и начина обављања делатности, примену овлашћења и вођење евиденција и спровођење прописа о држању и ношењу оружја приватног обезбеђења (Закон о приватном обезбеђењу, 2013, члан 70). Међусобна сарадња ових субјеката биће предмет наредног поглавља.

Закон о полицији, Сл. гласник РС, бр. 6/2016, 24/2018, 87/2018, садржи на само два места одредбе које се тичу приватног обезбеђења: одредба која у полицијске послове сврстава и извршавање послова утврђених прописима о оружју, приватном обезбеђењу и детективској делатности (члан 30) и одредба која се тиче права на ношење тамно-плаве униформе у односу на субјекте у које се убрајају правна и физичка лица на која се примењују одредбе о приватном обезбеђењу (члан 39). За разлику од ранијих нормативних решења, тренутни Закон нигде децидно не спомиње сарадњу са субјектима приватног обезбеђења. Највише што је учињено у том правцу јесте навођење да полиција развија сарадњу и партнерство са грађанима и другим субјектима заједнице… (члан 27). Из наведене одредбе могуће је претпоставити да се под овим субјектима мисли и на субјекте приватног обезбеђења, али то остаје непотврђено. Такође, у овом Закону се нигде не спомиње Стручни савет за унапређивање приватног обезбеђења и јавно приватног партнерства у сектору безбедности као посебна радна група у овом области као што је то учињено Законом о приватном обезбеђењу (члан 75). Пропуштање навођења субјеката приватног обезбеђења и сарадње полиције са њима, као што је учињено у Закону о полицији, није учињено и у документу *Стратешка процена јавне безбедности* из 2017. године, као ни у *Стратешком плану полиције за период од 2018-2021. године.* У оба документа наводи се сарадња са субјектима приватног обезбеђења и њихово укључивање у спровођење безбедносне превенције. У документима се такође позива на „пуну примену Закона о приватном обезбеђењу, како би сектор приватног обезбеђења у наредном периоду постао партнер полицији у очувању безбедности грађана и имовине и одржавању стабилног јавног реда и мира“ (Дирекција полиције, 2017а, стр. 10, 126; Дирекција полиције, 2017б, стр. 11). *Стратегија развоја Министарства унутрашњих послова за период од 2018-2023. године, Службени гласник РС, бр. 78/2018*, такође прописује пуну примену Закона о приватном обезбеђењу (област 4, стратешка област 1, циљ 1), али не иде даље од тога.

На Конференцији Привредне коморе Србије која је одржана 18. септембра 2024. године, истакнуто је да је у области приватног обезбеђења издато скоро 1.800 лиценци правним лицима и више од 65.000 лиценци физичким лицима, што „говори о обиму и квалитету овог сегмента безбедности нашег друштва“ (Привредна комора Србије, 2024). На истој конференцији подвучена је потреба за „интензивним нивоом сарадње и интеракције између јавног и приватног сектора безбедности“ да би се побољшала безбедносна ситуација (Привредна комора Србије, 2024).

Из приложене анализе нормативног оквира уочава се да Законодавац није у довољној мери препознао приватну безбедност као значајан елемент система националне безбедности. С обзиром на недовољно обухваћену област приватне безбедности, односно приватног обезбеђења у представљеном нормативном оквиру, не би требало очекивати било какво обухватање корпоративне безбедности, или заштите/безбедности привредних друштава или правних лица уопште. Због пропуста у вези са нормативним оквиром, у извесној мери је ограничен развој и унапређивање како места и улоге приватне безбедности у систему националне безбедности, тако и сарадње овог елемента са другим елементима, у првом реду, са полицијом. Посредно, ограничено је и увођење новог елемента у систем националне безбедности као што је корпоративна безбедност.

3. КОРПОРАТИВНА БЕЗБЕДНОСТ

„Успешна, профитабилна и дугорочно одржива је само она компанија чији је менаџмент способан да препозна, предупреди, умањи или отклони ризике пословања“
(Стојановић и Павловић, 2014, стр. 14).

Корпоративна безбедност је у већој или мањој мери развијена и ефикасна као део организације. Препозната је као „центар трошкова“ јер обично не ствара приход, али готово по правилу „додаје вредност“ организацијама на много начина (Kovacich and Halibozek, 2003, p. 226). Обезбеђујући део услова опстанка и функционисања у једној држави организација посредно доприноси и самој држави. Заштитом интереса организације у оквиру које је успостављена, корпоративна безбедност омогућава друштву и држави да задовоље своје потребе (Mijalković i Milošević, 2011, str. 485). Дакле, значај и улога корпоративне безбедности утичу не само на организацију или пословни систем, већ и на појединца, друштво у целини, директно или индиректно утичући и дајући одговарајући допринос систему националне безбедности (Lečić, p. 179). У окружењу које карактеришу бројне глобалне претње попут тероризма, организованог криминала или климатских промена, „приватне компаније су све више позване да управљају питањима националне безбедности“ (Petersen, 2013, p. 222; Petersen, 2014, p. 78). Тако, питања корпоративне безбедности су и питања националне безбедности (Bergin, Williams and De Wilde, 2019, p. 3), а безбедносне способности организације уједно и могућности система националне безбедности.

У овом поглављу, разматраће се најпре корпорација, у смислу организације, као место успостављања корпоративне безбедности, а уједно и као један од термина од којих је скован термин корпоративна безбедност. Потом, биће анализиран феномен корпоративне безбедности кроз сагледавање њеног развоја из оквира приватне безбедности и функција које је одређују. Поглавље треба да резултира теоријским увидима у проучавану област, као и дескрипцијом организовања и функционисања корпоративне безбедности у Републици Србији.

3.1. Корпорација као референтни објекат корпоративне безбедности

У литератури је могуће пронаћи став да се неки од ефеката корпоративне форме[43] могу пратити од раног тринаестог века због чега је она све до касног осамнаестог века држана под контролом државе. Потом су уследиле империјалистичке тежње које су почеле постепено да одвајају корпоративну форму од директне политичке контроле (Veldman and Willmott, 2013, p. 607). У средњем веку, у периоду када су занати били на економском врхунцу, корпорације су сачињавали мајстори истих заната. У њиховим рукама се налазио монопол прераде и продаје, као и управа у корпорацији (Драговић, 2013, стр. 211). Током већег дела деветнаестог века корпорација је посматрана као ентитет и наглашавана је конститутивна улога државе. Међутим, у последњим деценијама деветнаестог века дошло је до опадања улоге и овлашћења државе по питању правног регулисања активности корпорација, па су се корпорације пре посматрале као агрегати, а не правни ентитети (Millon, 1990, p. 202). Такав процес се наставио, па су у једном периоду корпорације имале исту или већу моћ над појединцима него владе (Ratner, 2001, p. 461).

[43] Аутори (Veldman and Willmott) под „корпоративном формом“ подразумевају (имагинарно) представљање корпорације (нпр. у правној или економској сфери) (2013).

Џелетовић сматра да се корпорација, као облик организовања, у непотпуном виду, појавила већ у шеснаестом веку како би се регулисала прекоокеанска трговина робом. Тако је основана Источноиндијска компанија (енг. *East India Company*) која се сматра првом корпорацијом (Dželetović, 2020, str. 4-5). Корпорације, или акционарска друштва како су их обично називали крајем осамнаестог века, биле су релативно ретке. Уз то, водећи економисти тог периода, Адам Смит (*Adam Smith*) и Стјуарт Мил (*John Stuart Mill*) били су поприлично забринути због потенцијалне неефикасности корпоративне форме, а пре свега недовољне контроле над управом (Mueller, 1992, p. 148). До деветнаестог века већина корпорација у Америци функционисала је у контексту јавног интереса (изградња окретница, мостова и канала, рад банака и осигуравајућих компанија и стварање ватрогасних бригада), да би тек након 1800. године корпорације ушле у област индустрије. Једна од првих таквих била је текстилна фирма из Бостона (енг. *Boston Manufacturing Company*) која је послужила као „прототип корпорација каснијег датума“ (Berle and Means, 1991, p. 11). У Великој Британији 1844. године донет је први Закон о акционарским друштвима и 1857. године, извршено је институционализовање модерне компаније, па се деветнаести век узима као одредница настанка савремене корпорације као „институционалног облика организовања привредних субјеката“ (Dželetović, 2020, str. 5).

У деветнаестом веку типична пословна јединица била је у власништву појединаца или малих група, њоме су управљали власници или њихови намештеници и била је, углавном, ограничена личним богатством власника. Постепено, ове јединице су замењене великим агрегацијама у којима се комбинују десетине или чак стотине хиљада радника и имовина вредна стотине милиона долара, која припада бројним појединацима. Пример корпорације која је имала можда најнапреднији развој корпоративног система јесте Америчка телефонска и телеграфска компанија (Berle and Means, 1991, p. 4). У друштву капитализма агрегација је добила форму „огромне, мултинационалне фирме и њених подружница“ (Veldman and Willmott, 2013, p. 607).

Данас, нарочито услед глобализације, јасно је да су корпорације заузеле поприлично стабилна места. Критичари сматрају да је од осамдесетих година прошлог века дошло до тога да је економија заузела кључно место у друштвеним процесима и даље до дехуманизације, отуђења и експлоатације. Са једне стране, због високих пореза корпорације су почеле да напуштају високоразвијене земље, док са друге стране, тржишне привреде су биле примамљиве као места за стварање капитала. Тако, глобализација је подупрела „глобалну експанзију транснационалних корпорација, насталих хоризонталним и вертикалним повезивањем, које послују у више земаља и које су у власништву акционара из различитих земаља“ (Јеличић и Ковинић, 2017, стр. 438). Данашњи свет је свет корпорација чија моћ превазилази чак и моћ неких држава.

Модерну корпорацију као правни облик могуће је дефинисати као акционарско друштво. Одликује се раздвајањем имовине ентитета и имовине оних који у њега улажу, акционара (Veldman and Willmott, 2013, p. 608). Корпорацију признаје закон, те стога она може да се понаша као да је лице кад су у питању радње попут склапања уговора, поседовањаимовине, одбране. У ери глобализације, модерна корпорација је све чешће транснационална или мултинационална, те послује на новом тржишту заједно са новим облицима удруживања као што су холдинг компанија (корпорација која контролише једну или више корпорација) или труст (група корпорација). Данас, корпорације без обзира да ли су веће или мање од државе, међудржавне или недржавне, политичке природе или посвећене циљевима попут стицања новца, заштите животне средине, ширења вере или заговарања неког општег добра имају идентитет (Kreveld, 2012, str. 403). Тај идентитет свака корпорација има обавезу да брани и штити, јер је то она. Без идентитета корпорација не би постојала.

Са правног аспекта дакле, корпоративна форма је замишљена као „ентитет“, „субјект“ или „особа“ (Veldman and Willmott, 2013, p. 615) или као агрегат.[44] Када се корпорација посматра као ентитет, њено постојање је одвојено од њених акционара и других учесника, а када се посматра као агрегат, она је агрегација физичких појединаца без чијег постојања ни она не постоји (Millon, 1990, p. 201). Тумачећи корпоративну безбедност као филозофију, Слободан Марковић на основу анализе тумачења корпорације у преисторијском доба исту дефинише „друштво устројено на крвном сродству чија је безбедност зависила од односа међу члановима у том сродству“ (2014, str. 15). Са оснивањем државе, држава је постала једна врста корпорације, попут универзитета, синдиката или цркве. Она је се може сматрати корпорацијом јер „представља самостално правно лице, што значи да има права и дужности и да може учествовати у разним активностима као да је права, жива особа од крви и меса“. Ипак, она се разликује од других корпорација по томе што она за друге корпорације „даје одобрење, док њу одобравају (признају) искључиво њој једнаки; затим, то што одређене функције (које се заједничким именом називају атрибутима суверенитета) обавља само она; и, напослетку, то што она те функције извршавају над одређеном територијом унутар које је њена надлежност и искључива и свеобухватна“ (Kreveld, 2012, str. 9).

На темељима своје анализе, Слободан Марковић истиче да је све до настанка државе, функција безбедности припадала корпорацији, која је схваћена на овај начин била племе, клан или каква слична заједница. Оснивањем државе, функције безбедности и заштите су припале њој. Са једне стране, за безбедност државе и њеног друштва није могла да буде одговорна „корпоративна безбедност“ јер нико осим државе није имао легитимно право на употребу силе која је предуслов функције безбедности и заштите. Са друге стране, у време убрзаног процеса глобализације, мање се говори о корпорацији као друштвеном субјекту у ширем смислу, а више као привредном субјекту (2014, str. 16).

Према истом аутору, данашњи појам безбедности у друштву има корпоративни карактер (Marković, 2014, str. 16) и могуће га је довести у везу са корпоративизмом.[45] Корпоративизам је доктрина која се односи на ширење корпоративног утицаја и контроле у различитим аспектима друштва, укључујући безбедност. Подробном анализом разумевања и одређења корпоративизма, Новак Гајић исти одређује, у најједноставнијем приступу, као „политичко организовање друштва кроз узајамно и политичким системом признате групе (додала ауторка: политичке корпорације) саздане према улози коју у том друштву имају“ (2020, стр. 264). У основи термина „корпоративизам“ налази се термин „корпорација“. Оснивањем (енг. *Incorporation*) ствара се нова корпорација (енг. *Corporation*). Гајић указује на то да би нека „корпоративна држава” (енг. *Corporate State*) или неко „корпоративно друштво” (енг. *Corporate Society*) означавали ону државу или друштво који су плен пословних корпорација где држава и друштво нису оно што би требало да буду, политичка заједница грађана, односно слободно друштво. На основу тога, у позадини такве праксе, могуће је говорити о „корпоративизму” (енг. *Corporatism*). Ипак, према овом аутору, за такву праксу би прикладнији израз био корпоратократија (енг. *Corporatocracy*) и зато овакво тумачење корпоративизма сматра упитним (2020, стр. 262-263). Иако се термини корпоратократија и корпоративизам могу погрешно користити као синоними због њиховог назива, реч је о посебним појмовима, где се први односи на политички систем којим доминирају корпорације. Корпоративизам је као доктрина коришћен од стране различитих идеологија и група, с тим да је на овом месту довољно извести закључак да су се на темељима корпоративизма развиле како корпорације, тако и корпоративна безбедност.

[44] О томе шта је корпорација и теоријама корпорација видети више у: Millon, David. (1990). Theories of the Corporation. *Duke LJ*, pp. 201-262.

[45] Корпоративизам или корпоратизам (енг. *Corporatism*).

Веома битан елемент корпорације јесте корпоративно управљање које у основи подразумева „структуре и процесе за вођење и контролу привредних друштава“ (Međunarodna finansijska korporacija, 2011, str. 6). Оног тренутка када је дошло до раздвајања власничке и управљачке функције унутар једне компаније успостављено је корпоративно управљање. За зачетке корпоративног управљања везује се рани седамнаести век, конкретно оснивање поменуте Источноиндијске компаније у Великој Британији. Наиме, испоставило се да власник или власници капитала (компаније) немају знања која би им омогућила успешно вођење компаније. У ту сврху, почели су да ангажују менаџере[46], односно професионалце који ће управљати компанијом а на основу капитала и циљева којим власници располажу и које су власници поставили. Постоји и став да је се са стварањем „квази-јавне“ корпорације (корпорације у којој је дошло до велике мере раздвајања власништва и контроле кроз повећање броја власника) појавио корпоративни систем (Berle and Means, 1991, p. 5). Оквир корпоративног управљања поставља циљеве, политике, вредности, културу, одговорност и учинак (Smith and Brooks, 2013, p. 33). Савремено корпоративно управљање без преседана укључује широк спектар мера у области безбедности укључујући управљање ризицима. Отуда се говори о посебној грани менаџмента, безбедносном менаџменту.

Према Организацији за економску сарадњу и развој, корпоративно управљање „укључује скуп односа између управе компаније, одбора, акционара и заинтересованих страна“. На тај начин обезбеђују се „структура и системи кроз које се компанија усмерава и постављају њени циљеви, а одређују се средства за постизање тих циљева и праћење учинка“. Корпоративно управљање према томе има неколико циљева. Најпре, помаже компанијама да побољшају приступ финансијама, да промовишу инвестиције, иновације и раст продуктивности и шире економску динамику; потом, пружају оквир за заштиту инвеститора; и на крају, подржавају одрживост и отпорност корпорација што, заузврат, доприноси одрживости и отпорности шире економије“ (Organisation for Economic Co-operation and Development, 2015). Корпорације нису више само приватни ентитети већ су значајни економски субјекти имају директан утицај на друштвени, економски и политички живот заједнице (Millon, 1990, p. 230). Већ неколико деценија уназад, корпорације имају карактер мултинационалних, јер послују у две или више држава. Глобализација, висок степен знања и технологије којима располажу ове корпорације учинили су их једним од водећих играча на међународном али и националним тржиштима. Балансирајући између властитих интереса и конкуренције, поред економске супериорности коју остварују, оне стичу доминацију и у политичкој, економској и културној сфери (Дуловић, 2019, стр. 42). Према подацима за 2015. годину, 69 од 100 највећих привредних субјеката су корпорације, а не државе, односно 10 највећих светских корпорација има комбиновани приход од више од 180 „најсиромашнијих“ држава (Global Justice Now, 2016).

[46] Менаџери и акционари имају различите улоге. Акционари управљају корпорацијом на основу закона, а менаџери управљају корпорацијом на основу овлашћења које им дају власници. Менаџери воде пословање корпорације на професионалној основи, док акционари користећи своја власничка права, врше надзор над учинком менаџера и пословним корпорацијама (Dželetović, 2020, str. 4).

3.2. Генеза корпоративне безбедности

Уколико заузмемо став по којем је корпоративна безбедност инкорпорирана у приватну безбедност[47], онда нема сумње да је развој корпоративне безбедности могуће пратити у контексту развоја приватне безбедности. Иако се испрва чини да је реч о модерном концепту, корени приватне безбедности сежу вековима у прошлост. Древна утврђења, употреба брава или чак животиња попут паса или гусака које би се оглашавале како би упозориле на крађу или неку опасност указују на то да концепт приватног обезбеђења постоји већ вековима (George and Kimber, 2014).

Током већег дела људске историје, војске су биле приватно организоване те их је носилац власти „изнајмљивао" и користиле су оружје чија производња, бар директно, није била у рукама власти. Тек са настанком националне државе почиње да се говори о праву државе на монопол силе и војци састављеној од грађана по обавези коју су имали. Сви елементи одбране и безбедности налазили су се под њеним окриљем, били су њена обавеза и право. Паралелно са развојем националних војски, традиционални плаћеници и војници из древних времена развили су се у индустрију приватне безбедности. Све до средине деветнаестог века држава је успевала да задржи и очува тај монопол силе. Са индустријском револуцијом, долази до поновног преокрета када приватни сектор почиње да подупире приватизацију производње чиме остварује далеко интензивнији технолошки развој од државе. Повећани ризик, трошкови, сложеност и значај технолошког развоја су последњих деценија повећали важност мултинационалних компанија (Brooks, 2005, p. 39). Тако, индустрија приватне безбедности почиње да цвета, да би данас представљала масовну индустрију коју карактерише специјализација, професионализација и разноликост у услугама безбедности које нуди.

3.2.1. Настанак и развој приватне безбедности

Да бисмо говорили о развоју приватне безбедности, кренимо од човекове потребе за безбедношћу. Идеја, а пре свега потреба заштите живота и имовине стара је колико и сам човек, па се може и рећи да је она једна од његових урођених потреба. Уколико се оде корак даље, ова потреба је у неком облику развијена код свих живих организама, који имају урођене, а себи својствене механизме одбране од различитих претњи које се развијају и постоје у њиховом окружењу. Човек као живо биће није изостављен из овог корпуса. Да је потреба за заштитом својстевена човеку проистиче и из можда једне од најпознатијих теорија мотивације, теорије о хијерархији потреба заступника хуманистичке психологије који је развио такозвану Масловљеву хијерархију потреба. Абрахам Маслов (*Abraham Maslow*) потребе за сигурношћу ставља на друго место по важности, односно одмах након основних, биолошких човекових потреба као што су ваздух, вода, храна, одећа (1943). Ове потребе могу да задовоље породица и друштво (држава са својом управом) узимајући ове ентитете као две стране једног новчића. Шта би то значило? Сваком појединцу бар док одраста, до тренутка када постаје способан за бригу о себи, потребу за сигурношћу најпре обезбеђује породица, а предуслове за то обезбеђује друштво, односно држава.

[47] Овакав став није нужно усвојити уколико се у обзир узме следеће: Корпоративна безбедност не испуњава у потпуности услов да се третира као приватна безбедност из два разлога: 1) постоје статусно правне различитости (корпоративна безбедност може бити и јавног и приватног власништва, док приватна безбедност може бити само приватног власништва) и 2) послови корпоративне безбедности штите интересе компаније и могу на тржишту да купују услуге безбедности, док су послови приватне безбедности увек намењени тржишту у циљу стицања профита, дакле они нуде услуге на тржишту (Лалић, Ћеранић и Сикимић, 2019, стр. 66).

О неизоставној потреби за заштитом сведоче и искуства прикупљана кроз различите историјске епохе развоја друштва. Почев од периода када су мушкарци ловили или сакупљали храну постојала је потреба да се заштити све оно што су животиње или припадници других племена могли да узму или униште. То су били храна, оружје за лов, крзно. Уз то, постојала је потреба да се заштите и они слабији, жене и деца. Када су људи почели да се баве узгојем животиња и биљака вредности које је требало штитити су се значајно увећале. Можда су управо ово први примери „приватне безбедности" када су људи тежили да заштите своје породице и имовину. Касније, ове улоге су са појединца биле преношене у надлежност професионалаца, најпре државних служби, а потом и специјализованих организација које пружају услуге безбедности по уговорној обавези.

Једна од историјских прекретница у вези обезбеђивања заштите било је стварање државе. Тек је монополизовање легитимног насиља путем политичке групе означило развитак у примени насиља ради заштите сопствених интереса (Veber, 1999, str. 68). Да би обезбедили себи опстанак (Хобс, 2004), сачували своју имовину (Лок, 2002) или обезбедили самоодржање (Русо, 1993) људи су почели да склапају друштвене уговоре иоснивају државну власт. На тај начин, они формирају државу напуштајући природно стање у којем су живели пре стварања ове друштвене творевине „које његови чланови називају *државом*, кад игра пасивну улогу, *сувереном* кад је активно, а силом кад га упоређују са њему сличним" (Ruso, 1993, str. 36). До тада уживајући у природним правима и старајући се о властитој безбедности, стварањем државе људи су своја права пренели на врховног владара или суверенаи прихватили да се о њиховој безбедности стара држава. У првобитним заједницама задатак безбедности је припао неком облику војне организације где су чланови племена уједно били и војници који су се старали о спољашњој безбедности, а у миру о одржавању реда односно унутрашњој безбедности. Развој друштва пратио је развој посебних организација које су у својој надлежности имале очување унутрашње безбедности. Тако је дошло до развоја полиције (Милосављевић, 1997, стр. 55-56).[48] Филип Ејдус (*Filip Ejdus*) сматра да се почев од седамнаестог века појам безбедности везује се за јавну безбедност (лат. *securitas publica*), која се односила на заштиту поданика у миру, као и на подршку поданика владару током рата, а од верских ратова у првој половини седамнаестог века јавила се идеја да о безбедности појединца може бринути само суверена држава (2012, str. 27). Дакле, држава је та која располаже „монополом над легитимном употребом физичке силе". Она делује као видљива сила која људе држи у страху и кроз страх од казне обавезује их на извршавање уговора и поштовање закона. Заштита сигурности и јавног поретка за коју је одговорна полиција једна је од њених темељних функција (Veber, 1999, str. 119, 162).

Наиме, свако политичко тело[49] којем су грађани били подређени имало је неку врсту безбедносне групације која је требало да ради у интересу грађана. Ипак, владарима су неретко биле потребне посебне групације које би се старале о њиховој безбедности. Постепено, ту потребу су све више изражавали и сви они који су желели додатне мере заштите властите безбедности или имовине, а истовремено то могли да приуште.[50] Унајмљивање лица која би штитила имовину могло би се оправдати идејом да је имовина била приватна, па је обавеза и одговорност њене заштите припадала власнику (South,

[48] Једна од активности витезова, краљевске гарде или других облика војне организације, а потом и полиције била је наплата пореза. Ова активност се можда издваја и као најстарија функција полиције у име државе јер како би се држава (ентитет креиран из незадовољства јавности) издржавала без новца (Nalla and Newman, 2012)?

[49] Политичко тело, према Жан Жак Русоу (*Žan Žak Ruso, фран. Jean-Jacques Rousseau*) јесте општа личност која настаје спајањем појединачних личности путем друштвеног уговора (1993, str. 36).

[50] Крајем двадесетог века, становници насеља су почели да издвајају таксе за услуге приватне безбедности као што се догодило у деловима Глазгова у Шкотској, Лондона у Енглеској и Мелбурна у Аустралији (Bayley and Shearing, 2001, p. 7).

1987). Овој идеји врло стабилан ослонац даје претпоставка да је заштита сопствене имовине одувек била право човека, па је и коришћење овог права претходило идеји да би помоћ владе у ту сврху могла бити доступна у облику јавне полиције или тела за спровођење закона (Burstein, 1999, p. 1). Интерну безбедност – тзв. „безбедност унутар куће" – традиционално су обезбеђивали „корпоративни ентитети", а од раних 1960-их дошло је до енормног раста уговорне безбедности, која пружа (полицијске) услуге свима који су тражили и могли да плате (Coleman, 1974 према Shearing and Stenning, 1983, p. 494). Сходно томе, приватно обезбеђење није нова појава већ има дугу историју (Becker, 1974, p. 438).

Постоји претпоставка да је у Енглеској приватна полиција (оно што у раду називамо приватна безбедност) претходила и била неопходна за увођење јавне полиције (Nalla and Newman, 2012). Од средњег века, у градовима су деловали нижи државни службеници попут фењерџија, ноћне страже, пијачних и кланичних контролора, стражарских дружина и затворских чувара. Осим њих, постојале су разне снаге за очување безбедности у унутрашњости земље (van Kreveld, 2012, str. 163-164).[51]

Интересанто је да се Енглеска сматра „колевком система приватне безбедности" (Лабовић, 2015б, стр. 17), док су се модерне полицијске службе, какве данас познајемо, појавиле тек у деветнаестом веку и то у Енглеској[52] (Ortmeier, 1999, p. 53; Dempsey, 2010, p. 2) и Француској[53] (Никач и Павловић, 2012, стр. 20) или Немачкој и Италији (Trivan, 2014, str. 35). У Сједињеним Америчким Државама, чувари су били ангажовани да патролирају улицама ноћу представљајући „примарне мере безбедности све до успостављања полицијских снага са пуним радним временом средином 1800. година" (van Meter, 1976 према Fischer, Halibozek and Walters, 2012, p. 6). Иако тада са недефинисаним оквирима, јавна и приватна безбедност су почеле да се развијају широм света, често се и преплићући.

Ране цивилизације ослањале су се на владара и владареву војску која је требало да штити народ. Током средњег века, јављају се не тако ефикасна тела за спровођења закона и изоловани случајеви приватног обезбеђења када су ова тела била неефикасна. Од средњег, па све до деветнаестог века „историја приватног обезбеђења је испреплетена са историјом јавног спровођења закона". Тек у деветнаестом веку јавно спровођење закона и приватно обезбеђење су почели да се јасно раздвајају. Од тада, полиција је прихваћена као носилац функције безбедности, а додатна заштита је тражена у виду услуга приватне безбедности (Hess, 2009, p. 4). Управо се средина деветнаестог века узима као период развоја модерне индустрије приватне безбедности (Fischer, Halibozek and Walters, 2012, p. 6) и то у државама попут Енглеске и Француске, када је дошло и до развоја полиције (Никач и Павловић, 2012, стр. 20). Упркос томе што је држава тежила да монополизује јавну заштиту кроз успостављање јавних полицијских снага у деветнаестом веку, приватни ентитети су наставили да себи пружају додатну заштиту кроз приватно обезбеђење (Spitzer and Scull, 1977, p. 21). У Републици Србији, почетке

[51] У Енглеској су, на пример, дуго постојали шерифи (чланови окружне управе који нису добијали надокнаду) и констабли (службеници који су се издржавали од удела у порезима) (van Kreveld, 2012, str. 164).

[52] Упореди са: Last, M. David. (2007). „Evolution of Policing and Security: What it Means for Diverse Security Sectors". In *Conference, Defending Democracy Accommodating Diversity in the Security Sector Queen's University School of Policy Studies November 1-3, 2007*; Rawlings, Philip. (2012). „Policing before the police". In T. Newman (Ed.), *Handbook of policing* (pp. 75-99). Routledge; van Kreveld, Martin. (2012). *Uspon i propadanje države*. Beograd: Albatros plus; Fakultet bezbednosti.
Мартин ван Кревелд (*Martin van Kreveld*) наводи да је прва државна полиција формирана шездесетих година осамнаестог века у Француској, где је касније Наполеон основао државну полицију одговорну за све врсте државне безбедности (2012, str. 164-165).

[53] Упореди са: Bayley. David H., and Shearing, Clifford D. (2001). *The New Structure of Policing. Description, Conceptualization, and Research Agenda*. Washington: U.S. Department of Justice, National Institute of Justice.

приватне безбедности могуће је пратити од почетка двадесетог века.[54] Додатно, током деведесетих година прошлог века фактори попут смањења броја националних снага, фокус на исплативе војске, ширење регионалних сукоба, јавна подршка страној интервенцији, већа техничка софистицираност рата допринели су порасту приватне безбедности (Schreier and Caparini, 2005, p. i).

Подела послова безбедности карактеристична је за савремену епоху у првом реду због продорности и степена до којег је приватна безбедност „пустила корене" и на јавна места. Можда је држава и даље „једини извор права за примену силе", док се „другим организацијама и појединцима приписује право на употребу физичке силе само у оном обиму у којем то држава са своје стране допушта" (Veber, 1999, str. 162). Веберов став да држава има монопол над применом силе озбиљно је пољуљан у савременом добу, а можда чак и превазиђен.

3.2.1.1. Приватизација послова безбедности

Брза индустријализација и пораст криминала оптерећивали су полицију, убрзавајући развој приватног „полисинга"[55] или приватне безбедности. Тако, поред историјске употребе изнајмљених војника у оружаним сукобима (Avant, 2004, p. 153), а и из разлога попут финансијске ефикасности и технолошке супериорности, владе су почеле да сарађују и са приватним субјектима како би унапредили безбедност грађана (Markusen, 2003). Иако се економска објашњења најчешће наводе као разлози приватизације безбедности (White, 2012), постоји став да повећане захтеве грађана и организација за безбедношћу једноставно није могла да испуни полиција, која је била преоптерећена и ограничена својим фокусом на контролу криминалитета, као и постојећим законима о приватној својини (Shearing and Stenning, 1983). У литератури је могуће пронаћи став да постоје два процеса приватизације – „приватизација одозго", где држава делегира неке своје надлежности приватним субјектима и „приватизација одозго" до које долази када држава нема капацитета да пружи и гарантује безбедност свим својим грађанима (Trivan, 2014, str. 65). Безбедност није једина сфера коју је захварио тренд приватизације. Исто се догодило и са другим областима попут образовања, здравства, инфраструктурних послова.

Уз то, преношење дела јавних функција на приватну безбедност, по неким ауторима треба да буде тумачено у другачијем облику и то као „формализација секундарних активности друштвене контроле". Наиме, услед опадања контроле од стране оних који су исту вршили као секундарну функцију (попут чувара паркова, железничке страже, кондуктера), дошло је до пораста примарних облика друштвене контроле, односно јавне, али и приватне полиције (Jones and Newburn, 2002, p. 142). Роналд ван Стеден (*Ronald van Steden*) истиче шест фактора који су утицали на ширење приватне безбедности: пораст криминала и повезани проблеми, масовно повећање приватне својине, економски разлози, владине политике усмерене на сарадњу са приватним сектором, преоптерећеност полицијских структура и професионализација приватног обезбеђења (2007).

---

[54] О тим почецима видети више у: Talijan, Momčilo. (2008). „Prve ustanove privatne bezbednosti (policije) u Srbiji". U: *Privatna bezbednost: stanje i perspektive: zbornik radova: prvi međunarodni skup* (str. 40-62). Novi Sad: Fakultet za pravne i poslovne studije; Кешетовић, Желимир, и Симоновић, Бранислав. (2009). Сектор корпоративне и приватне безбедности у Србији. *Годишњак Факултета безбедности*, стр. 147-171.

[55] О развоју приватног „полисинга" и његовом утицају на будуће управљање у „колективном животу" видети више у: Kempa, Michael; Carrier, Ryan; Wood, Jennifer and Shearing, Clifford. (1999). Reflections on the Evolving Concept of 'Private Policing'. *European Journal on Criminal Policy and Research* 7 (2), pp. 197-224.

„Саморасклапање“ или „демонтажа“ државе створило је услове за настанак приватних фирми за обезбеђење било директно кроз преношење раније јавних функција или индиректно кроз процесе одговорности. Уз то, држава им је обезбедила и идејне капацитете у виду друштвено признатог облика легалитета и признате експертизе. На тај начин, омогућено им је да своје већ велике материјалне капацитете даље шире (Abrahamsen and Williams, 2011, p. 93). Понашање државе у комбинацији са друштвеним, економским и политичким факторима, укључујући и дефендолошке факторе (Vejnović i dr., 2008, str. 13) убрзало је развој приватног сектора безбедности, створивши услове за развој „живе, разнолике и глобалне трговине“ услугама безбедности (Loader, Goold and Thumala, 2014, p. 470), које се све више сматрају робом којом се тргује (Crawford, 2006).[56]

Како запажа Дебора Авант (*Deborah Avant*), о импликацијама приватизације безбедности у контексту контроле силе воде се расправе између песимиста који тврде да окретање приватној безбедности прети да поткопа државну контролу и демократске процесе, док оптимисти верују да приватна безбедност нуди решења за одређене безбедносне проблеме који могу бити значајни како за националну, тако и за међународну безбедност (2005, p. 3-5). Роберт Мандел (*Robert Mandel*) додаје да постоје тензије између циљева безбедности и профита, које се врте око два значајна питања: „1) да ли перпетуација режима или максимизација прихода треба да имају предност и 2) да ли принудна сила треба да буде тржишна роба или прерогатив државе“ (2001)?

У економски слабијим земљама, услед друштвених проблема попут незапослености, неефикасности јавне администрације, високог степена корупције и организованог криминалитета, ограничавање слобода, све више се стварају услови за развој приватног сектора безбедности (Rakić, 2008, str. 162). Искуство је показало да постоји уочљива разлика између приватног сектора безбедности у земљама западне демократије, земљама у транзицији и неразвијеним земљама (Vejnović i dr., 2008, str. 13). Такође, разлике су значајне и када се анализира развој приватне безбедности у ауторитарним државама, земљама у развоју и индустријализованим демократијама које нису англосаксонске (Singh and Light, 2019). У бившим социјалистичким државама развој приватне безбедности био је условљен факторима попут процеса транзиције, економског стања, нижег или вишег степена социјалне и правне (не)уређености држава (Кешетовић и Симоновић, 2009, стр. 148).

Овакав развој догађаја могао би се описати Теоријом принципал-агент (Avant, 2005). Иако је реч о економској теорији из седамдесетих година прошлог века, која се превасходно користила за анализу подстицаја у уговарању (Wright, 2015), њене поставке се могу применити и на сферу безбедности и пружања услуга безбедности. Према овој теорији, принципал представља некога ко делегира овлашћење, а агент представља некога коме је делегирано овлашћење. У нашем случају, принципал је држава која делегира део јавних функција и послова безбедности, а агент представља организације којем су те функције и послови делегирани. Иако се ова теорија у сфери безбедности углавном разматрала у контекту вођења сукоба (Feaver, 2003; Salehyan, 2010), она може послужити и као објашњење *приватизације послова безбедности*. Међутим, у литератури постоји и нешто другачија примена ове теорије по којој се однос принципал-агент може посматрати као однос приватних фирми за обезбеђење и оних који контролишу или поседују имовину којој се обезбеђује заштита (Abrahamsen and Williams, 2011, p. 108). У овом случају, принципал јесу појединци, групе или организације које требају услуге безбедности ради заштите и које у те сврхе ангажују агенте у виду приватних фирми за

[56] О томе коју заштитну робу треба куповати и продавати, а која треба да буде вођена нетржишним вредностима које постоје у друштву, као и моралној економији безбедности видети у: Loader, Ian, Goold, Benjamin and Thumala, Angélica. (2014). The moral economy of security. *Theoretical criminology* 18 (4), pp. 469-488.

обезбеђење. Односно најосновнији облик ауторитета приватних безбедносних компанија јесте онај који проистиче из „односа принципал–агент између приватног обезбеђења и приватне својине њихових клијената“ (Abrahamsen and Williams, 2007, p. 241). На овом месту се може сугерисати да се оваквим активностима ни на који начин не пориче веза између државе и безбедности, већ се артикулишу односи између субјеката и послова које врше. Наиме, „ауторитет није нужно игра са нултом сумом“, а исто тако могуће је да приватна безбедност може ојачати и подржати ауторитет државе (Abrahamsen and Williams, 2007, p. 238).

У литератури се може пронаћи и нешто другачији став. Џејмс Вилијамс (*James Williams*) одбацује идеју да су неке функције јавне полиције приватизоване зато што јавни сектор није могао да се носи са растућом потражњом за овим услугама. Према њему, реч је о две одвојене гране безбедности које се крећу у различитим јурисдикцијама. Корпоративна безбедност је према њему суштинска за организације које се суочавају са проблемима финансијског губитка и репутационог ризик (2005, pp. 323, 325). На овом месту, корпоративна безбедност се поистовећује са широм, приватном безбедношћу.

Када су се створили услови за стварање приватних фирми за обезбеђење бројни појединци попут Хенрија Филдинга (*Henry Fielding*), Видока (*Eugene-Francois Vidocq*), Алана Пинкертона (*Allan Pinkerton*), Хенрија Велса (*Henry Wells*), Едвина Холмса (*Edwin Holmes*), Пери Бринка (*Perry Brink*), Вилијама Бернса (*William Burns*) и Вилијама Фаргоа (*William Fargo*) видели су прилику за давањем свог доприноса обезбеђивању услуга безбедности[57] ако занемаримо њихову евентуалну идеју за стицање профита. Допринос се огледао у оснивању фирми које су пружале различите услуге обезбеђења, од заштите лица, обезбеђења транспорта новца до пружања детективских и истражних услуга. Неке од њих попут фирме Алана Пинкертона[58] и Пери Бринка[59] послују и данас. Сматра се да модерна индустрија приватне безбедности у Сједињеним Америчким Државама „у великој мери дугује своје порекло Алану Пинкертону“ (Dempsey, 2010, p. 28).[60] Постепено је долазило до реструктурирања полиције и пролиферације „полиције ван полиције“, услед чега је плурализован, фрагментован и диференциран „прекривач“ (енг. *patchwork*) заменио идеју полиције као монополистичког чувара јавног реда (Crawford, 2014, p. 147). Стварање „проширене полицијске породице“ и „светлоплави полицијски плурализам и партнерство“ добило је свој замах (Zedner, 2006, p. 82).

Двадесети век окарактерисала су два светска рата и Хладни рат, као и све јача свест о новој реалности у којој се државе не могу ослонити искључиво на сопствене снаге војске и полиције. У овом периоду, заштита имовине и посебно заштита информација добијају доста већи фокус него у ранијим периодима. Тако су за информације које су се сматрале најкритичнијим за националну одбрану, били успостављени строжи нивои контроле (Kovacich and Halibozek, 2003, p. 51). Владе почињу да успостављају посебне снаге за заштиту индустријских постројења значајних за одбрану, а власници индустрија почињу да формирају сопствене снаге или да ангажују снаге по уговорној основи ради обезбеђивања индустријских постројења и друге имовине (Button and George, 2001;

---

[57] О њиховом доприносу развоју приватне безбедности видети више у: Лабовић, Дејан. (2015б). *Приватна безбедност у Републици Србији-правни аспекти и компаративна искуства* (Докторска дисертација). Крагујевац: Универзитет у Крагујевцу, Правни факултет.

[58] Фирма је основана 1850. године под именом енг. *Pinkerton's National Detective Agency*. Данас носи назив енг. *Pinkerton Consulting and Investigations*.

[59] Фирма је основана 1859. године под именом енг. *Brink's Chicago City Express Company*. Данас носи назив енг. *The Brink's Company*.

[60] Пинтерктонову организацију је председник Линколн ангажовао да обавља обавештајне дужности током грађанског рата. Пинкертон је такође заслужан за ангажовање прве жене која је постала детектив у Сједињеним Америчким Државама, и то много пре него што је покрет за право гласа жена остварио своје циљеве (Levine, 1963 према Fischer, Halibozek and Walters, 2012, p. 7).

Dempsey, 2010, p. 28). На том основу, развијају се две „стратегије деловања“ приватне безбедности: као самостална служба при правним лицима и као агенцијски посао професионалних организација (Никач и Павловић, 2012, стр. 20), односно две врсте приватне безбедности: власничке услуге (енг. *Proprietary Services*) и уговорне услуге (енг. *Contract Services*) (Hess, 2009, p. 4; Kovacich and Halibozek, 2003, p. 45). Прва стратегија у виду стварања сопствене службе у чијој надлежности је остваривање безбедносне функције организације није ништа друго него обезбеђење (заштита имовине и људи) као једна од кључних менаџерских активности које Анри Фајол (*Henri Fayol*) уводи кроз своју теорију организације и управљања. Како истиче, обезбеђење као активност има за циљ да заштити имовину и лица од крађе, пожара и поплава, спречи штрајкове и кривична дела и уопште све друштвене поремећаје који могу да угрозе напредак, па чак и пословање. Генерално, то су све мере које се предузимају ради заштите запослених (Fayol, 2016). У овако одређеној менаџерској функцији могуће је пронаћи обрисе корпоративне безбедности, јер је менаџерска функција усмерена ка подржавању реализације основних активности организације. Успостављање корпоративне безбедности био је један од начина на који организације прихватају на себе део обавеза које произилазе из ризичног друштва и безбедносних проблема који из њега произилазе, а својствени су карактеру и активностима организације.

Развој мултинационалних корпорација на америчком тлу повукао је за собом нове безбедносне претње, као што су терористичке претње и отмице руководилаца корпорација и њихових породица. Такав тренд је додатно подстакао раст корпоративне безбедности (Dempsey, 2010, p. 14). Други аутори сматрају да је раст одговорности и акценат на безбедности у корпоративном смислу био вођен поред Хладног рата и геополитичким факторима. Један од примера ширења безбедносних мера у корпоративни свет јесу безбедносне провере које су почеле да врше корпоративне безбедносне службе онда када је требало ангажовати велику и поуздану радну снагу, а нарочито када за рад у осетљивим областима по државу или на поверљивим пројектима (Kovacich and Halibozek, 2003). Петерсен сугерише да је кључни покретач раста корпоративне безбедности у двадесет првом веку „одговорност“ и прихватање корпоративног окружења од стране владе услед све озбиљнијих претњи националној безбедности попут тероризма и организованог криминала (Petersen, 2013).

3.2.1.2. Укупни економски утицај сектора приватног обезбеђења данас

У деценији која је претходила, тржиште услуга безбедности (безбедносни системи, приватно обезбеђење и консултантске услуге у области безбедности) било је у сталном порасту. Према извештају *Глобални индекс мира* (енг. *Global Peace Index*) за 2023. годину, приватно обезбеђење чини 9% економског утицаја обуздавања насиља (енг. *Violence Containment*), односно 6% укупног глобалног економског утицаја насиља (енг. *global economic impact of violence*).[61] Укупни трошкови за приватно обезбеђење износили су у 2023. години 1,3 трилиона долара и то је чини трећим највећим потрошачем у оквиру категорије економског утицаја насиља.

[61] Појам економски утицај насиља „обухвата комбиновани ефекат директних и индиректних трошкова и ефекат мултипликатора, док економски трошак насиља представља директну и индиректну цену насиља“ (Institute for Economics & Peace, 2024, p. 47). Економски утицај насиља броји 18 индикатора који су категоризовани у три целине: обуздавање насиља, оружани сукоби, међуљудско насиље и самоповређивање. Приватно обезбеђење припада целини обуздавања насиља (Institute for Economics & Peace, 2024, p. 46). Дефинише се као категорија обезбеђења које је запослено у приватним ентитетима, попут обезбеђења које запошљавају правна лица (Institute for Economics & Peace, 2013, p. 58). О начину на који се врши процена трошкова приватног обезбеђења видети више у: Institute for Economics & Peace. (2013). *Global Peace Index 2013*. Sydney: Institute for Economics & Peace (p. 72).

У 2020. години, Азија је претекла Европу и Северну Америку и постала највеће тржиште за безбедносне услуге широм света, у вредности од 37 милијарди америчких долара. Европа је била друго највеће тржиште безбедносних услуга, процењено на 36 милијарди америчких долара (Statista Research Department, 2023). Већина запослених у индустрији физичког обезбеђења налази се управо у Азији, са 58% од укупног броја, а следе је Европа и Северна Америка (Meyer, 2024).

Кључни налази истраживања које је спровела међународна организација за менаџере безбедности (енг. *ASIS International*) указују на то да тржиште физичког обезбеђења запошљава више од 30 милиона људи широм света, од којих је 210.000 на тржишту опреме, око 7,87 милиона на тржишту услуга и 22,6 милиона који раде као крајњи корисници обезбеђења.[62] Процењена вредност индустрије физичког обезбеђења била је скоро 405 милијарди долара 2023. године (Meyer, 2024). Поред тога, очекује се да ће глобално тржиште опреме за физичку безбедност порасти на 70 милијарди долара, односно укупно тржиште опреме и услуга физичког обезбеђења порасти на скоро 500 милијарди долара до 2026. године (ASIS International, 2024), или за 181,2 милијарде долара између 2023. и 2028. године (Technavio, 2024).

3.2.2. Развој корпоративне безбедности

Као што је на почетку поглавља наведено, развој корпоративне безбедности неопходно је пратити кроз развој приватне безбедности. Суштински, потреба за безбедношћу коју човек има одувек изнедрила је безбедност као функцију различитих ентитета, јавних и приватних. Ипак, за све време постојања тих ентитета, човек не престаје да обезбеђује заштиту за свој живот и имовину. Тако, корене корпоративне безбедности могуће је тражити у људској потреби за безбедношћу, али могуће је и њен развој везати за још неке елементе. Један од тих елемената може бити тренутак раздвајања услуга безбедности које пружа уживалац тих услуга за себе (власничке услуге) и услуга безбедности које се пружају уживаоцу тих услуга (уговорне услуге). У првом случају, могуће је говорити о корпоративној безбедности, док се други случај оставља у надлежности приватне безбедности схваћене у смислу компанија које пружају безбедносне услуге.

Развој корпоративне безбедности могуће је пратити од 1880. године. Те године основана је америчка телефонска компанија Бел (енг. *Bell*) која је користила патент Александра Грејема Бела (*Alexander Graham Bell*) из 1876. године. Врло брзо директори компаније су схватили да им је потребна повећана заштита патента у време када је вођена борба за монополизацију националне телефонске услуге (Reich, 1980, p. 507). Интересантно је да су лабораторије у склопу ове компаније имале одељење безбедности које је било одговорно за издавање идентификационих картица, као и безбедносне значке различитих боја које означавају различите нивое безбедности (Noll, 2015, pp. 12, 30).

За развој корпоративне безбедности, конкретније, успостављања унутрашњег обезбеђења у приватним организацијама везује се компанија Форд. Двадесетих година прошлог века, у оквиру компаније је формирана посебна канцеларија која је требало да застраши и омета растући синдикални покрет међу радницима аутомобила. Реч је било о „Фордовом одељењу за услуге“, званичним безбедносним снагама компаније. На челу

[62] Оно што може бити интересантно јесте податак да је пре две деценије број службеника обезбеђења на нивоу Европске уније износио 1,1 милион у односу на 1,3 милиона полицајаца (Harborne, Dorotinsky and Bisca, 2017, p. 282). И данас, у неким земљама, број припадника приватног обезбеђења је исти или чак премашује број полицајаца (нпр. Кина, Индија, Сједињене Америчке Државе). Чињеница је међутим да је добијање тачних података веома тешко, ако не и немогуће (поред регистованих службеника, има и оних који раде „на црно“; обелодањивање оваквих информација зависи од воље оних који истим располажу).

овог одељења постављен је Бенет (*Harry Herbert Bennett*), 24-годишњи бивши морнарички шампион у лакој категорији, који је послове безбедности трансформисао из аматерске операције у чврсто вођену корпоративну безбедност. Одељење је имало и спољашње и унутрашње одреде који су надзирали раднике неуспостављајући разлику између посла и приватног живота, а често и бришући границе између законитости и незаконитости употребе силе. Касније, када је Хенри Други (*Henry Ford II*), унук оснивача Форда, спојио „сигурност синдиката" са „безбедношћу компаније", испоставило се да је синдикат надгледао Фордове фабрике доста боље од Одељења за услуге (Weiss, 2014). Како истиче Роберт Вајс (*Robert Weiss*), који се опсежно бавио корпоративном безбедношћу у Фордовој компанији, „историја Фордове корпоративне безбедности пружа живописну илустрацију међусобног прожимања приватног и јавног сектора, као и променљиве природе учешћа државе у корпоративној безбедности; најпре, толеранцијом владе и директном подршком радничкој репресији, а затим, у промењеној политичкој економији, применом овлашћења Конгреса да примора корпорације да прихвате помирљив приступ индустријској синдикализацији" (2014, p. 18).

У литератури се може пронаћи став да „корпоративна безбедност почиње у заједници". Ово је тврдња коју је изнео менаџер рудника Бату Хијау (енг. *Batu Hijau*), другог по реду највећег рудника бакра и злата у Индонезији, и иначе бивши пуковник и војни аташе америчке војске. Он ју је објаснио истакавши да је у корпоративном контексту примењивао искуство стечено у америчкој војсци, а нарочито оно које је имао у вези коришћења развојне помоћи као средства за реализацију безбедносних циљева попут култивисања савезника или остваривања територијалног приступа (Welker, 2009, p. 147). Изнет став се може објаснити и развојном стратегијом корпоративне безбедности која се заснивала на ангажовању локалних елита као прве линије одбране корпорације (Welker, 2009, p. 143).

Следећи значајан елемент јесте оснивање Америчког друштва за индустријску безбедност 1955. године, које данас носи назив АСИС (енг. *ASIS International*). Под покровитељством ове организације корпоративна безбедност се развија и професионализује (Walby and Lippert, 2015a, p. 2). У оквиру сертификације коју нуди ова организација, постоје четири програма за: сертификованог професионалца за заштиту, стручног сарадника за заштиту, професионалног сертификованог истражитеља и стручњака за физичко обезбеђење. Уз то, нуде различите вебинаре, курсеве и друге програме за унапређивање знања и професионални развој. Издавачка делатност у виду приручника попут Пакета заштите имовине (енг. *Protection of Assets – POA*) унапређује међународну заједницу приватне и корпоративне безбедности (ASIS International, n.d.).

Развој корпоративне безбедности Денис Далтон (*Dennis Dalton*) прати од улоге ноћног чувара пре шездесетих година прошлог века. Посао ноћних чувара углавном је значио осматрање ради раног упозорења у случају инцидената као што је пожар. У том контексту, развој је могуће сагледати кроз четири фазе. Прва фаза или ера „зелених колиба" била је карактеристична по веома ниској позицији коју су запослени на овим пословима заузимали и недостатку корпоративних безбедносних ресурса. Следећа фаза или ера „физичке безбедности" ставила је фокус на заштитуматеријалне имовине на местима која су се користила као улази и излази. У наредној фази, фази „корпоративне безбедности", формиране се јединице под тим називом које су у својој надлежности имале више задатака од пуког физичког обезбеђења. Ова фаза се може окарактерисати као значајна јер се на корпоративну безбедност почело гледати као на део плана пословања и као најбољу пословну праксу. Четврта фаза, ера „тоталне заштите имовине", означила је трансформацију карактера корпоративне безбедности као глобалног и фокус ставила на заштиту како материјалне, тако и нематеријалне имовине (2003, p. 21-23). Група аутора је на трагу Далтоновог рада идентификовала и пету фазу коју карактерише пренос

корпоративне безбедности на јавне и државне органе и њену све већу професионализацију. Тако се отварају бројна питања не само о одговорности влада и о односима између владине корпоративне безбедности, јавне полиције и приватног обезбеђења, већ и о пракси надзора (Lippert and Walby, 2014, p. 883).

Како смо сведоци све озбиљнијих претњи и ризика унутрашњег и спољашњег окружења организација, можемо се сложити са тим да управљање економском, али и сваком другом безбедношћу у организацијама треба и мора да постане приоритет највишег менаџмента (Kalina et al., 2022, p. 335) како би се обезбедило првенствено оно што се назива управљање ризицима, а потом и свеукупна безбедност. У литератури је идеја о служби унутрашње безбедности у великим корпорацијама (корпоративној безбедности) препозната као ефикаснија од три друге академске идеје: идеја поделе – интеракција друштвене контроле између приватних и јавних полицијских снага, идеја плурализације полиције и идеја о нодалној контроли безбедности[63] (Ocqueteau, 2011). Прва идеја подразумева и приватизацију друштвене контроле коју карактерише неспецијализовано обезбеђење (Shearing and Stenning, 1983). Друга идеја, о плурализацији полиције, произашла је из новоуспостављеног стања у којем послове безбедности не врши само полиција већ целокупан систем састављен од „владиних, комерцијалних и друштвених тела“ услед чега је дошло до „фрагментације“ или „плурализације“ полиције (Jones and Newburn, 2006, p. 1). Плурализацију је могуће довести у везу са постепеном променом „од владања до управљања“ (енг. *from government to governance*) чиме се број одговорних за безбедност увећава (Trivan, 2014, str. 65). Трећа идеја се заснива на претпоставки о нодализацији полиције, односно диверзификацији „полисинга“ и стварању других чворова у „полисингу“ услед чега се у „добу нодалног управљања безбедношћу“, „полисинг“ не ограничава на полицију већ и на друге „чворне групе као што су војска и сада огроман и растући приватни сектор безбедности“ (Shearing, 2005, p. 58; Walby and Lippert, 2015б, p. 241).

3.3. Корпоративна безбедност као део индустрије приватне безбедности

„Попут плаћеника који су производ света који верује у ефикасност силе, безбедносне компаније су производ света коме је потребна безбедност“ (Zarate, 1998, p. 162).

Када се говори о индустрији приватне безбедности прва асоцијација обично су приватне безбедносне компаније и услуге које ове компаније пружају. Углавном се мисли на 1) приватне фирме за обезбеђење које своје услуге пружају трећим странама, 2) приватни интерни безбедносни сервиси, 3) приватни алармни надзорни центри и 4) приватне фирме за транспорт вредности. Односно реч је у широком спектру услуга: надзор и заштита покретне и непокретне имовине; чување имовине и надзор на јавном простору; транспорт новца и других вредности; заштита лица; управљање алармним надзорним центрима; унутрашње обезбеђење и контрола приступа; обезбеђење догађаја; притвор и надзор затвореника; чување кључева; обезбеђење паркинга укључујући мега-молове; надзор над стамбеним блоковима; курирске услуге, услуге рецепције и портира; руковање алармима и алармним системима; мониторинг видео обезбеђења; реаговање у ванредним ситуацијама; рутинска контрола саобраћаја; безбедносне консултације (de Waard, 1999, pp. 144-145). У литератури је присутна класификација основних функција приватне безбедности где се у исте убрајају: физичка заштита, безбедносне услуге, приватне истраге, корпоративна безбедност и криминалистичке истраге (Krstić, 2008, str. 69).

[63] Под нодалном контролом полиције подразумева се постојање хоризонталне једнакости субјеката друштвене контроле унутар мреже.

Овакав приступ, где се примат даје приватним безбедносним компанијама, не треба да изазива забуну с обзиром на то да ове компаније постоје много дуже и њихово тржиште је далеко веће и конкурентније од тржишта војних услуга (Schreier and Caparini, 2005, p. 26). Експоненцијалним растом индустрија приватне безбедности се проширила и на друге секторе који су раније били у искључивом домену државе, односно на војне и обавештајне службе (George and Kimber, 2014, p. 34). Тако, послове приватне безбедности обављају субјекти приватне безбедности, који се најопштије, могу класификовати на приватне војне компаније и комерцијалне добављаче услуга (Савић, 2007, стр. 70) или како се чешће називају, приватне безбедносне компаније. На овом месту би међутим сасвим сигурно требало додати и приватне детективске компаније. Реч је о субјектима организованим као легитимни корпоративни ентитети, који имају посебан правни статус и пружају широк спектар услуга безбедносног карактера.

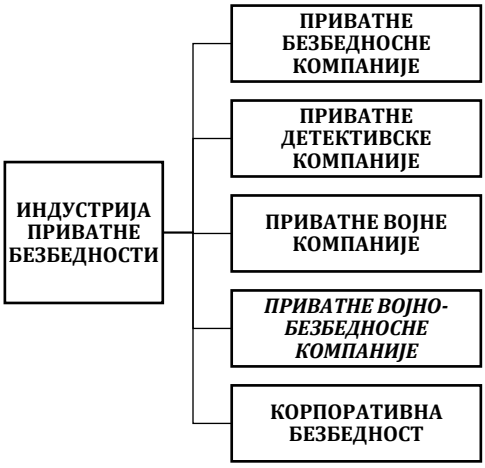
Успон савремене међународне приватне војне и безбедносне индустрије за чији почетак се узима период деведесетих година прошлог века могуће је објаснити трима факторима: 1) модел државног слободног тржишта након хладног рата постао је доминантан, уз пратећи тренд преношења традиционалних владиних функција на недржавне актере; 2) дошло је до глобалног смањења националне војске, што је даље довело до обезбеђивања огромног броја обученог бившег војног особља за регрутацију од стране приватних компанија; и 3) велике силе су се постепено повлачиле из многих делова света у развоју (Holmqvist, 2005, p. 2).

Данас се употреба термина „индустрија приватне безбедности“ којим би се обухватили сви ентитети од приватних војних компанија до корпоративне безбедности чини и више него адекватном. Ипак је индустрија приватне безбедности много више од онога што се под њом подразумева у широј јавности попут избацивача испред ноћног клуба, чувара који патролирају у локалном складишту или чувара у супермаркету (George and Kimber, 2014, p. 21). Ова „индустрија” обухвата мноштво индустрија, великих и малих, које се поред приватних војних компанија односе и на пружање услуга обезбеђења, истраге, превенцију криминала, одржавање реда, планирање система, техничко саветовање и безбедносни дизајн, те није једноставна хомогена група (van Steden and Sarre, 2007, p. 223). Према појединим ауторима, правна лица специјализована за пружање безбедносних услуга могу пружати и неке друге услуге као шти су „успостављање система корпоративне заштите у компанијама; временски ограничено пружање услуга корпоративне заштите; системску подршку корпоративној заштити; супервизију система корпоративне заштите; безбедносну едукацију менаџмента и друго“ (Стојановић и Петровић, 2014, стр. 208). У таквом случају, ови субјекти приватне безбедности могу да пруже три врсте услуга: „(1) потпуна услуга корпоративне заштите по моделу „кључ у руке"; (2) делимична услуга по изабраној области корпоративне заштите и (3) изабрани комплекс услуга (по систему „паушал") које се реализују по потреби“ (Стојановић и Петровић, 2014, стр. 208).

Индустрију приватне безбедности или субјекте приватне безбедности могуће је разврстати на 1) приватне војне компаније, 2) приватне безбедносне компаније и 3) приватне војно-безбедносне компаније (Никач, 2013, стр. 21). Њима додајемо 4) приватне детективске агенције (Стајић и Лукић, 2011, стр. 67) и 5) субјекте приватне безбедности који делају интерно, за организацију којој припадају (субјекте корпоративне безбедности) (видети Илустрацију 5).[64] У литератури је могуће пронаћи и

[64] Приватне војно-безбедносне компаније ретко када се посматрају као посебна категорија приватних компанија које пружају безбедносне услуге. На овом месту су наведене под претпоставком да ипак постоје приватне компаније које врше чисто безбедносну делатност и приватне компаније које врше чисто војну делатност. У тексту који следи оне се неће обрађивати с обзиром на тематику рада, али је на

другачију класификацију субјеката приватног сектора безбедности. На основу прегледа литературе, група аутора је дошла до закључка да би приватни сектор обухватао следеће делатности: (1) приватну полицију, (2) приватну детективску делатност, (3) приватне војне компаније (4) приватне обавештајне компаније и (5) приватне казнене установе (Лалић, Ћеранић и Сикимић, 2019, стр. 54). Треба имати у виду и постојање приватних обавештајних компанија (енг. *Private Intelligence Companies*) (Schreier and Caparini, 2005, p. 27; Bošković, 2006, str. 19) чији је рад усмерен превасходно на податке и информације, њихово прикупљање, анализу и експлоатацију.



Илустрација 5: Приказ индустрије приватне безбедности (Ауторка)

3.3.1. Приватне безбедносне компаније

Приватна безбедносна компанија се може одредити као „јасно структурисана и хијерархијски устројена регистрована корпоративна асоцијација која пружа услуге безбедносног карактера, такмичећи се за добијање послова са другим таквим фирмама на тржишту“. Приватна безбедносна компанија може да пружа услуге физичког и техничког обезбеђења лица, објеката и имовине и тада се може назвати и приватна фирма за физичко-техничко обезбеђење (енг. *Private Security Companies*) (Centar za civilno-vojne odnose, 2008, str. 118).

Према нешто сложенијој, али и ограничавајућој дефиницији, то је „регистрована цивилна компанија која је специјализована за пружање комерцијалних услуга по уговору домаћим и страним субјектима са намером да заштити особље и хуманитарну и индустријску имовину у складу са правилима важећег домаћег права” (Goddard, 2001, p. 8). Ове компаније деле исте организацијске структуре као и приватне војне компаније и послују као правна лица. Једна једноставна дефиниција је да су приватне безбедносне компаније „приватне компаније које продају војне услуге“ (Kinsey, 2005, p. 270). Оваква дефиниција је међутим дискутабилна. Уколико бисмо је прихватили то би значило да не признајемо постојање приватних војних компанија или да не правимо разлику између војних услуга и оних које то нису, али спадају у домен безбедности. Прихватање овакве дефиниције значило би ограничавање домена услуга приватних безбедносних компанија на чисто војну сферу, што би само по себи било погрешно. Управо из тог разлога, значајно је направити дистинкцију између услуга које пружају. Тај опсег услуга јесте оно што и представља главну разлику између приватних безбедносних и приватних војних компанија.

основу приложеног текста о приватним безбедносним и приватним војним компанијама могуће закључивати и о делатности ових „мешовитих“ компанија.

Приватне безбедносне компаније се претежно баве питањима јавног реда и превенцијом криминала. Када је реч о пословима одржавања јавног реда, поред рада са полицијом на задацима попут контроле масе на великим јавним догађајима или *заштите критичне инфраструктуре*, приватне безбедносне компаније раде са затворским службама у казнено-поправним установама, са граничним властима у области имиграције или управљања границом или са обавештајним службама у пружању података и анализи података или других услуга тог типа (Chappuis, 2021, p. 72). Постоје компаније које врше обуку државних безбедносних служби, обезбеђивање транспортних и информационих путева (Beyani and Lilly, 2001, p. 18). Када је реч о пословима превенције криминала, они се могу груписати у неколико категорија: спречавање или откривање упада, неовлашћеног уласка или активности, вандализма и ометања приватног власништва; спречавање или откривање крађе, губитка, проневере или прикривања робе, новца, обвезница, акција, новчаница, докумената или хартија од вредности; заштита појединаца од телесних повреда; обезбеђивање присуства; поштовање и спровођење утврђених правила, прописа, мера, политика и пракси компаније у вези са смањењем криминала; пријављивање и привођење прекршилаца; пријављивање инцидената и позива (United Nations Office on Drugs and Crime, 2014, p. 7).

Конфедерација европских безбедносних служби (енг. *The Confederation of European Security Services*) у услуге безбедности убраја комерцијално обезбеђење са особљем, патролу, интерно обезбеђење (може бити схваћено као корпоративна безбедност), обезбеђење догађаја, обезбеђење на улазу, телохранитељ, транспорт готовине и транспорт драгоцености, обрада готовине, мобилне алармне услуге и услуге одговора на позиве, аларм и видео надзор, услуге мониторинг центра, тражење и праћење, ваздухопловна безбедност, скрининг, услуге коришћења обучених паса, поморска безбедност, *заштита критичне инфраструктуре*, комбинована решења, корпоративна истрага, услуге прве помоћи, услуге превенције и заштите од пожара, урбана безбедност, превенција губитака, рецепционер/консијерж, безбедносни консалтинг, специјализовано обезбеђење, обука за приватно обезбеђење и многе друге (CoESS, 2016, p. 6). Наиме, све услуге које пружају могуће је диференцирати у три области (van Bergen Thirion, 1998; Schreier and Caparini, 2005, p. 27):

- Сектор обезбеђења који обухвата патролирање аеродромима, пословним зградама, стамбеним комплексима, тржним центрима, спортским аренама, магацинима, железничким и аутобуским станицама, карго терминалима, паркингима...
- Сектор електронске безбедности, сензора и надзора који укључује имплементирање аларма, контроле приступа, заштите и уређаја за брзо реаговање, често са сервисима за реаговање, као и услуге детекције упада.
- Сектор за истраге и управљање ризиком који се састоји од приватних истражитеља чије се активности крећу од брачних спорова, радних питања, провера, услуга вештачења, приватне и индустријске шпијунаже, контраобавештајног рада и контранадзора, до заштите одређених лица.

Уколико се у разматрање узме последња област, не би било погрешно рећи да ова група послова заправо више одговара посебној врсти приватних компанија и то оним специјализованим за детективске односно истражне послове. За те компаније користи се израз приватне детективске или истражне компаније. С обзиром на приложену класификацију, долази се до закључка да је реч о једној врсти приватних безбедносних компанија, док са друге стране, не би било погрешно разматрати их као посебну групу у оквиру онога што се назива индустрија приватне безбедности.

Све чешће се прави разлика између ових компанија и комерцијалних безбедносних компанија (енг. *Commercial Security Companies*) као већих компанија у јавном власништву

које имају униформисане и (углавном) ненаоружане чуваре за комерцијалне, владине и међународне организације широм света (Kinsey, 2001, p. 18). Овакво одређење међутим прави забуну, с обзиром на то да се наводи да је реч о компанијама у јавном власништву. Такође, употреба овог термина није до краја јасна, с обзиром на то да се читава индустрија приватне безбедности некада одређује као комерцијална индустрија безбедности (енг. *Commercial Security Industry*) (Kruck and Spencer, 2013, p. 334) или се чак приватне безбедносне компаније одређују као једна врста субјекта који пружа комерцијалне услуге (Cockayne, 2006). Сходно наведеном, вероватно најбоље решење би било да се комерцијалне безбедносне компаније третирају искључиво као део комерцијалне индустрије безбедности, односно као приватне безбедносне компаније које пружају услуге зарад стицања профита.

Сумирано, приватне безбедносне компаније део су индустрије приватне безбедности и представљају правна лица која пружају услуге безбедносног (али не и војног) карактера уз одређену надокнаду. Крајњи циљ ових компанија јесте стицање профита. Услуге које ове компаније пружају бројне су и прилагођене специфичним потребама клијената. Неке од основних услуга су: физичко обезбеђење, техничка заштита уз мониторинг, заштита транспорта новца и вредности, консултантске услуге, и под одређеним условима одржавање јавног реда и мира.

3.3.1.1. Приватне безбедносне компаније и корпоративна безбедност

Користећи дефиницију приватних безбедносних компанија могуће је извести дефиницију корпоративне безбедности. Тако, корпоративна безбедност се може одредити као (цивилна) организациона целина која је специјализована за пружање безбедносних услуга *организацији у оквиру које је успостављена* са намером да заштити особље и имовину, а у складу са нормама домаћег права, стандардима и интерном регулативом.

Ипак, корпоративна безбедност не може бити врста приватних безбедносних компанија. Најпре, корпоративна безбедност не постоји као засебна организација у смислу регистрованог правног лица, већ као организација односно организациона целина у оквиру неког правног лица. Поред тога, за разлику од приватних безбедносних компанија које пружају услуге другим компанијама односно правним лицима, корпоративна безбедност искључиво пружа услуге правном лицу у оквиру којег је успостављена. Дакле, прве „раде“ за другога, док корпоративна безбедност „ради“ за себе – организацију која ју је успоставила. С тим у вези`, иако услуге приватних безбедносних компанија и корпоративне безбедности могу бити идентичне, реч је о две суштински различите врсте ентитета.

3.3.2. Приватне детективске компаније

Алан Пинкертон, о коме је било речи у претходним деловима рада, заправо се сматра зачетником приватне детективске делатности, бар у Сједињеним Америчким Државама. Пинкертон је развио своју стручност у шпијунажи током грађанског рата (Weiss, p. 88) и остао је познат, између осталог, и по увођењу неколико истраживачких техника у оперативном раду, као што су праћење или присмотра осумњиченог и попримање криминалне улоге или рад са прикривеним идентитетом, познато као прикривени иследник (Лабовић, 2015б, стр. 51). Најчешће криминалистичке радње које детективи данас предузимају јесу вођење информативних разговора са грађанима, праћење и присмотра (Стајић и Лукић, 2011, стр. 94-95).

У литератури се може пронаћи схватање да се рани равој приватне детективске делатности везује за пружање радне снаге која је била дисциплинована за покретање капиталистичке индустријализације, док се „промена у природи политичке економије“ узима за покретача развоја ове делатности (Weiss, p. 87).

За појединце који обављају послове под окриљем приватне детективске делатности, користе се два термина: детектив и истражитељ. Постоје аутори који сматрају да се оба термина равноправно користе јер је заправо реч о синонимима.[65] Кесић запажа да се термин детектив више везује за литерарни приказ ове делатности и извештавање медија[66], док је у стручним радовима чешће коришћен термин истражитељ. Ипак, имајући у виду домаћу законску регулативу ове области, код нас се „одомаћио“ управо термин детектив (Кесић, 2013, стр. 85). Реч је о појединцима који самостално или као запослени у организацији пружају комерцијалне услуге не само прикупљања информација и података, већ и прикупљања доказа (Bošković, 2006, str. 23; Vejnović i dr., 2008, str. 53).

Када се говори о врстама детективских услуга, у литератури се може пронаћи класификација на брачне и породичне истраге, истраге дисциплине на раду, истраге осигурања, такозвано праћење имовине, вршење оперативних провера кандидата за рад у правним лицима, прикупљање података у вези са нарушавањем ауторских права и активности усмерене на поновно враћање у посед имовине (Кесић, 2013, стр. 93-97).[67] Томе се могу додати и услуге попут трагања за несталим лицима и возилима, провера бонитета физичких и правних лица, коришћење информација о привредним субјектима и располагање пословном базом корисних информација, обезбеђивање транспорта новца и других вредности, давање безбедносних савета, провера пословних партнера, осигуравање доказа и предмета, објављивање фотографија лица и предмета за којима се трага или нуђење награде за добијене податке (Bošković, 2006, str. 48).[68]

Могуће је говорити и о корпорацијским детективима који спроводе интерне и екстерне истраге за корпорације како због злоупотреба од стране запослених као што су проневере и крађе материјалних добара или информација, тако и због откривања и спречавања злоупотреба од стране пословних партнера или клијената (Vejnović i dr., 2008, str. 17).

Како се закључује, приватне детективске компаније у основи је могуће дефинисати као правна лица која пружају различите услуге истраживања и сакупљања информација или доказа за клијенте који траже помоћ у решавању проблема. Спектар услуга је веома широк, док је на овом месту значајно подвући могућност коришћења детективске

[65] О употреби ових термина видети више у: Лабовић, Дејан. (2015б). *Приватна безбедност у Републици Србији-правни аспекти и компаративна искуства* (Докторска дисертација). Крагујевац: Универзитет у Крагујевцу, Правни факултет; Радивојевић, Ненад. (2019). *Јавно-приватно партнерство у области јавне безбедности у развијеним земљама са посебним освртом на Републику Србију* (Докторска дисертација). Нови Сад: Универзитет у Новом Саду, Правни факултет у Новом Саду.

[66] Видети опширније о утицају популарне културе на перцепцију приватних детектива у: Gill, Martin, and Hart, Jerry. (1997b). Private investigators in Britain and America: Perspectives on the impact of popular culture. *Policing: An International Journal of Police Strategies and Management* 20 (4), pp.631-640.

[67] Мартин Гил (*Martin Gill*) и Џери Харт (*Jerry Hart*) наводе следеће услуге: уручивање судских налога и других докумената, истраге потраживања, истраге саобраћајних незгода, брачне истраге, криминалистичке истраге, истраге превара и откривање финансијских извора и материјалног стања појединца (1997a, p. 553).

[68] Овај скуп наведених услуга захтева од нас да будемо обазриви приликом анализе и потенцијалног усвајања. Неке од ових активности попут објављивања фотографија или „утеривања дугова“ и сам аутор види као проблематичне. Активност попут транспорта новца и других вредности данас је у надлежности приватних фирми за обезбеђење, док су активности попут давања безбедносних савета, провере бонитета и пословних партнера у надлежности корпоративне безбедности организације.

делатности како у приватне сврхе, тако и у сврху заштите правног лица или вредности правног лица, Дакле, детективске услуге могу бити и предмет склапања уговора у склопу корпоративне безбедности правног лица.

3.3.3. Приватне војне компаније

Проучавајући приватне војне компаније, Лабовић истиче да термин приватна војна компанија није постојао ни у једном међународном документу или конвенцији до 2006. године, с тим да је прва приватна војна фирма основана у Великој Британији 1967. године, под називом Вочгард Интернешнл (енг. *WatchGuard International*) (2015б, p. 40). Појам приватне војне компаније (енг. *Private Military Companies – PMC*) јесте општи појам за све приватне компаније које се баве пружањем војних услуга и обуке (Centar za civilno-vojne odnose, 2008, str. 118). Реч је о корпорацијама које су регистроване као правна лица, које подлежу закону и ангажоване су од стране влада, наводно да обезбеде јавну безбедност (Beyani and Lilly, 2001, p. 16 према Kinsey, 2006, p. 14) нудећи војне услуге у распону од војне обуке и саветовања до борбених активности (Chesterman and Lehnardt, 2009, p. 1). Дакле, приватне војне компаније су организације са успостављеном структуром, функцијама и широким спектром активности из области безбедности и оружаних снага, регистроване као правни субјекти чије редове попуњавају професионалци, најчешће бивши војници, које пружају услуге различитим субјектима на широком географском подручју мотивисане финансијском добити.[69]

Услуге које пружају приватне војне компаније нису орјентисане само на директно учешће у борбеним операцијама већ обухватају и друге попут саветовања, обуке, логистичке подршке, одржавања, обавештајног рада, извиђања, надзора и праћења, као и услуга разминирања (Schreier and Caparini, 2005, pp. 23-25). У вези са услугама, односно према њиховој удаљености од бојног поља, Питер Сингер (*Peter Singer*) приватне војне фирме дели на војне фирме које пружају борбене услуге и које се налазе у најближој близини бојног поља (енг. *Military Provider Firms*), војне консултантске фирме (енг. *Military Consultant Firms)* и војне фирме које пружају услуге подршке и помоћи (енг. *Military Support Firms*) (2008).[70] У вези са наведеним, могуће је говорити и о приватним борбеним компанија (енг. *Private combat companies*) које Берг (Berg) описује као приватне војне компаније које су специјализоване за „оштар крај безбедносне индустрије", што би значило предузимање искључиво борбених операција, препуштајући борбену подршку и логистику војним компанијама. Суштина ових компанија јесте организовање борбене снаге која је способна да се у врло кратком року распореди у борбену зону, и уколико је потребно, сузбије агресора војном силом (Kinsey, 2006, p. 13).

---

[69] Упоредити са: Milošević, Nenad and Jukić, Jadranko. (2017). Private military and security companies: Legal, moral and social implications. *Vojno delo* 69 (7), str. 161-173.
О дефиницијама видети више у: Лабовић, Дејан. (2015б). *Приватна безбедност у Републици Србији-правни аспекти и компаративна искуства* (Докторска дисертација). Крагујевац: Универзитет у Крагујевцу, Правни факултет. Упореди са: Litavski, Jan. (2012). Izazovi privatnog sektora bezbednosti u novom veku. *Novi vek, Tromesečnik Centra za evroatlantske studije*, novembar 2012. и Schreier, Fred and Caparini, Marina. (2005). *Privatising security: Law, practice and governance of private military and security companies* (Vol. 6). Geneva: DCAF.
О проблему дефинисања приватних војних компанија и начину на који њихов успон и развој утичу на ауторитет држава да дефинишу и регулишу употребу силе видети у: Leander, Anna. (2004). *Eroding State Authority? Private Military Companies and the Legitimate Use of Force*. Soveria Mannelli: Rubbettino.

[70] Аутор користи термин приватне војне фирме за „нове пословне организације које тргују професионалним услугама замршено повезаним са ратовањем. Приватне војне фирме су приватни пословни субјекти који потрошачима пружају широк спектар војних и безбедносних услуга, за које се некада сматрало да су само унутар јавног контекста" (Singer, 2008, p. 8).

Услуге које пружају ове компаније не само да нису ограничене на директну борбу, већ нису ограничене ни на субјекте којима услуге нуде. Тако, поред влада, чести клијенти могу бити и корпорације, политички покрети, невладине организације или хуманитарне организације. Очигледно је да је „приватна сила" еволуирала од пружања најамничких услуга до професионалног корпоративног субјекта који је легализован од стране држава.[71]

Приватне војне компаније се ангажују у војним операцијама предузимајући активности које премашују активности других приватних безбедносних групација од плаћеника па све до приватних безбедносних компанија.[72] Као такве, оне могу да промене преовлађујуће стратешко окружење у којем делују што их представља као „крајњу еволуцију у способностима и на свим нивоима операције" (O'Brien, 2009, p. 38). У литератури о приватним војним компанијама аутори обично полазе од дефинисања плаћеника. Важно је направити дистинкцију између приватних војних компанија и плаћеника, како је термин плаћеник коришћен да опише различите појединце или организације, од појединаца који убијају за најам, преко трупа које је подигла једна земља и које раде за другу, до приватних војних компанија које пружају војне услуге својој земљи (Avant, 2005, p. 22). Није нетачно рећи да су се плаћеници кроз историју унајмљивали како би пружали безбедносне услуге онима који су за исте плаћали. Серж Јаличев (*Serge Yalichev*) је проучавао унајмљивање плаћеника током историје закључивши да је „сасвим јасно да је војничка најамнина – као и проституција – изузетно древна забава, можда скоро исто толико стара колико и сам организовани рат" (1997, p. 1). Најамничка војска или плаћеници обучени и опремљени за борбе били су и више него потребни владарима у време када грађани нису могли или нису били довољни за вођење ратова. Дуго времена је најамничка војска била главно средство којим су се ратови водили.

На трагу наведеног, Кевин ОБрајан (*Kevin O'Brien*) плаћеника дефинише као традиционалног војника који је замењен прихваћеним борцем тек у време Француске револуције када су национални идеали били нераскидиво везани за војну службу (2009, p. 35). Касније, када су државе почеле са увођењем редовних војски, потреба за плаћеницима је постепено опадала. Како Ијан Џеферис (*Ian Jefferies*) примећује, чиста плаћеничка активност се и данас наставља, али се термин плаћеник користи претежно у пежоративном смислу, а стављање плаћеника и приватних војних компанија у исти кош доприноси томе да се често искриви реална слика о приватним војним компанијама (2002, pp. 104-105). Тумачење да свака „приватна сила" није ништа друго него група плаћеника и други аутори сматрају поједностављењем, па чак и заблудом (Adams, 1999; Wither, 2005; Moesgaard, 2013; O'Brien, 2009). До оваквог тренда дошло је вероватно због појаве нове врсте „војника среће" – независних плаћеника (енг. *Freelance Mercenaries*), које је Карлос Зарате (*Juan Carlos Zarate*), тада заменик саветника за националну

[71] О развоју приватних војних компанија и „корпоративним ратницима" видети више у: Singer, Peter W. (2008). *Corporate Warriors: The Rise of the Privatized Military Industry*.Ithaca, NY: Cornell University Press; Kinsey, Christopher. (2006). *Corporate Soldiers and International Security: The Rise of Private Military Companies*. London: Routledge; Moesgaard, Christa. (2013). *Private military and security companies-from mercenaries to intelligence providers*. Danish Institute for International Studies.

[72] О дистинкцији између плаћеника, приватних војски, милиција и војсковођа и приватних безбедносних и приватних војних компанија видети у: O'Brien, Kevin A. (2009). „What should and what should not be regulated?". In S. Chesterman and C. Lehnardt (Eds.), *From Mercenaries to Market: The Rise and Regulation of Private Military Companies* (pp. 29-48). Oxford: Oxford University Press.
О разлици између приватних борбених компанија (енг. *Private Combat Companies*), приватних војних компанија, прокси војних компанија (енг. *Proxy Military Companies* – представљају скуп приватних војних компанија), приватних безбедносних компанија, комерцијалних безбедносних компанија и независних оператора (енг. *Freelance Operators*) видети у: Kinsey, Christopher. (2006). *Corporate Soldiers and International Security: The Rise of Private Military Companies*. London: Routledge.

безбедност за борбу против тероризма САД-а, назвао „дивље гуске“ или *les affreux* („оне од којих се грози“) (Maogoto and Sheehy, 2006, p. 2). Ова врста плаћеника битно се разликује од припадника приватних војних, па и безбедносних компанија у смислу операција, клијената, одговорности и капацитета међународне заједнице да регулише њихове активности. То су лица која нуде војне услуге на тржишту по правилу бирајући клијента који понуди највише новца (Brooks, 2000, p. 130). Ову борбену групу Кристофер Кинсеј (*Christopher Kinsey*) назива независним операторима и примећује да многи независни оператори личе на класичне плаћенике, али да то не оправдава неретко поистовећивање ове две групације (2006, pp. 18-19).

Међународна заједница добила је дефиницију плаћеника као део члана 47. Додатног протокола Женевским конвенцијама од 12. августа 1949. године, који се односи на заштиту жртава међународних оружаних сукоба (Протокол 1) из 1977. године, да би Конвенцијом УН о плаћеницима из 1989. године[73] била проширена. Међутим, на начин на који су тренутно одређене, приватне војне компаније се не могу сматрати плаћеницима, те ни њихове активности нису забрањене.[74]

На крају, вероватно би најбоље било рећи да остају они који сматрају да је „тржиште силе“ ослобађање још једног круга плаћеника, док други тврде да је реч о даљој приватизацији која пушта и шири корене у сферу националне безбедности (Avant, 2005, p. 22). Целокупна приватна војна индустрија континуирано се развија од краја Хладног рата и данас представља бизнис вредан више милијарди долара, што могу поткрепити чињенице да се ове компаније купују и продају на Волстриту (енг. *Wall Street*), а њихове акције котирају на најјачим берзама (McFate, 2014, p. 8).

3.3.3.1. Приватне војне компаније и приватне безбедносне компаније

Како Ким Ричард Носал (*Kim Richard Nossal*) примећује, учестала је употреба термина „приватне војне компаније“. Ипак, неке од приватних војних компанија нуде и услуге обезбеђења, па тако задиру у сферу приватних безбедносних компанија. Са друге стране, и приватне безбедносне компаније некада излазе из оквира свог устаљеног деловања пружајући услуге које су одређене као услуге приватних војних компанија. Из тог разлога, аутор предлаже употребу термина „транснационална безбедносна корпорација“, који наглашава шири елемент безбедности, као и прекогранично пословање (2001). Прављење дистинкције између приватних безбедносних компанија и приватних војних компанија често не резултира јасним закључцима пре свега зато што многе компаније преузимају уговоре и у војном и у комерцијалном сектору (Abrahamsen and Williams, 2007, p. 239). У пракси многе приватне безбедносне компаније спроводе активности које би неки могли сматрати војним, као што су на пример, обука полицијских снага или одржавање војних возила у мировним операцијама. Проблем је што не постоји јасна линија шта постаје „војно“, па је често додељивање овог атрибута субјективно и прозвољно (Kinsey, 2001, p. 17). Многи термини се користе за описивање приватних актера који раде у борбеним зонама, укључујући „приватне војне фирме“,

[73] Пун назив конвенције је Међународна конвенција против регрутовања, употребе, финансирања и обуке плаћеника (енг. *International Convention against the Recruitment, Use, Financing and Training of Mercenaries, 4 December 1989*) ратификована од стране 37 држава и потписана од стране 17 држава. Подаци на дан 16.07.2023. са сајта https://ihl-databases.icrc.org/en/ihl-treaties/conv-mercenaries-1989/state-parties.

[74] Приватне војне компаније могу да потпадну под неке одредбе члана 47 Протокола 1 и Конвенције о плаћеницима, али ако се њихова дефинијиција не уклапа у све одредбе, исто је као да се не уклапа ни у једну одредбу, односно приватне војне компаније ће остати ван домета ове регулативе.
О проблематици дефинисања плаћеника видети више у: Scheimer, Michael. (2009). Separating Private Military Companies from Illegal Mercenaries in International Law: Proposing an International Convention for Legitimate Military and Security Support that Reflects Customary International Law. *American University International Law Review* 24 (3), pp. 609-646.

„приватне безбедносне компаније“, „приватне војне и безбедносне компаније“, „приватну безбедносну индустрију“, па чак и „плаћенике“ (de Nevers, 2009, p. 173). Иако неки аутори бришу дистинкцију између „војног“ и „безбедносног“ фаворизујући употребу термина „приватне безбедносне компаније“ за све приватне компаније у сектору безбедности (Zarate, 1998, p. 76; Holmqvist, 2005, p. 5-6; Kinsey, 2005, p. 270; Krahmann, 2009, p. 25), разумевање и једних и других значајно је из разлога што улазе „под кишобран“ приватне безбедности.

Попут приватних безбедносних и детективских компанија, приватне војне компаније део су индустрије приватне безбедности. Реч је о правним лицима која са циљем стицања профита нуде и пружају војне услуге својим клијентима са којима имају закључене уговоре. Услуге које ове компаније пружају бројне су и прилагођене специфичним потребама клијената. У њих се пре свега убрајају борбена дејства, активности помоћи и подршке, консултантске услуге војног карактера укључујући и војне обуке.

3.4. Корпоративна безбедност – дефинисање појма

Иако би се у први мах корпоративна безбедност повезала са приватним организацијама, она је подједнако важна и за организације јавног карактера преко којих држава извршава своја права и обавезе према другим ентитетима, а у првом реду грађанима. Реч је о пракси имплементираној како у приваним тако и у државним јавним организацијама (Strom et al., 2010; Brooks, 2013; Brooks and Corkill, 2014; Petersen, 2014; Walby and Lippert, 2015a).[75] Корпоративна безбедност дакле може да функционише подједнако и у приватним и у јавним организацијама (Lippert, Walby and Steckle, 2013; Brooks, 2013). Иако се *a priori* везује за корпорације као економске институције, она се успоставља и у институцијама попут универзитета, невладиних организација, политичких партија, цркава (Лалић, Ћеранић и Сикимић, 2019, стр. 60). Корпоративна безбедност је *sine qua non*[76] у данашњем пословном окружењу (Pendić et al., 2019, p. 746). То је концепт аналоган „тотему“ у антрополошком смислу, јер је безбедност за савремене организације као савремени тотем, као *panacea* или лек за све (Borodzicz and Gibson, 2007, p. 181). У том контексту, може остати у основи функција менаџмента (Borodzicz and Gibson, 2007, p. 71). Успостављањем корпоративне безбедности, корпорације су у стању да регулишу сва понашања које се дешавају у њиховим просторима, да одговоре на све прекршаје без обзира да ли их чине корпоративни партнери или њихови запослени (Calder, 1987, pp. 18, 21).

Аутори се слажу око тога да је дефинисање корпоративне безбедности изазов (Brooks, 2010; Williams, 2010; Gerginova, 2016). Како је приметила Гергинова анализирајући дефиниције неких домаћих и страних аутора (Стајић; Cubbage and Brooks; Genser, Deitelhoff and Wolf; Милошевић; Ivandić, Karlović and Ostojić; Marković) „дефиниција овог појма је изузетно тешка, јер праву природу и обим области корпоративне безбедности је тешко утврдити“ (Gerginova, 2016, p. 491). Поред тога, ауторка истиче да постоји одређена подела у мишљењима о томе шта је интерес корпоративне безбедности, а да се притом не уђе у поље приватне безбедности (Gerginova, 2016). Уз то, реч је о комплексном концепту о којем се сазнања још увек развијају (Walby and Lippert, 2014, p.

[75] За додатне студије, а нарочито о корпоративној безбедности у општинама (енг. *Municipal Corporate Security*) видети више у: Walby, Kevin, Lippert, K. Randy, and Gacek, James. (2016). „Securitising 'National Interests': Canadian Federal Government Departments, Corporate Security Creep, and Security Regimes. In: Lippert, R., Walby, K., Warren, I., Palmer, D. (Eds.). *National Security, Surveillance and Terror. Crime Prevention and Security Management* (pp. 155-176). Palgrave Macmillan, Cham.

[76] У преводу са латинског: нешто без чега се не може, нешто неопходно.

2) и постојању дивергенције литературе о корпоративној безбедности (Ludbey, Brooks and Coole, 2017). Да постоји евидентан недостатак радова о теоријско-концептуалним питањима у вези са корпоративном безбедношћу потврђује и група домаћих аутора (Лалић, Ћеранић и Сикимић, 2019, стр. 65).

3.4.1. Корпоративна безбедност као систем

Као што свака држава формира свој систем безбедности, тако и свака организација (треба да) формира свој систем безбедности.

Уколико корпоративну безбедност посматрамо као **СИСТЕМ**, она би била подсистем виших система, и виши систем за сопствене подсистеме. Основ за овај приступ налази се у, већ помињаној, теорији система. Систем корпоративне безбедности јесте отворен систем који покушава да одржи стабилно стање, док на њега утиче унутрашње и спољашње окружење са којим је у континуираној интеракцији (Smith and Brooks, 2012, p. 26).

Уважавајући системски приступ, систем корпоративне безбедности припада вишим системима, најпре систему приватне безбедности, а потом и систему унутрашње и националне безбедности. Систем обезбеђења корпорације представља саставни део система националне безбедности, који се састоји од више подсистема безбедности (Даничић и Стајић, 2008, стр. 19). Према Слободану Марковићу, корпоративна безбедност као подсистем националне безбедности она представља део безбедносне структуре са скупом друштвених циљева који усмеравају пословне активности привредних субјеката и мере њихове друштвене одговорности у складу са стандардима и законом (2007, str. 21). Даље, систем корпоративне безбедности је и део друштвеног система на националном, регионалном и глобалном нивоу. Поред међународног система, припада и систему људске безбедности (Mijalković i Milošević, 2011, str. 481).

И сам систем корпоративне безбедности, са друге стране, састављен је до низа „хетерогених, али функционално повезаних подсистема у оквиру којих су структурирани појединачни, групни и корпоративни интереси, у њиховој узајамној интеракцији и у односу са окружењем“ (Кековић и Димитријевић, 2017, стр. 236).[77] Сходно наведеном, аутори предлажу структурално-функционалну дефиницију корпоративне безбедности по којој „корпоративну безбедност чини целина интеракција које остварују елементи организације међусобно и са окружењем, применом услужних и самозаштитних модалитета безбедности и заштите, штитећи на тај начин корпоративне интересе и циљеве“ (Кековић и Димитријевић, 2017, стр. 239). Кековић истиче значај примене системског приступа у области корпоративне безбедности јер она обухвата „економске, информационе, социјалне, правне и друге аспекте који се налазе у узајамној интеракцији, али и интеракцији са окружењем: националним, регионалним, глобалним“ (Кековић, 2018, стр. 31).

Попут било ког друштвеног (организационог) система, укључујући и систем националне безбедности, систем корпоративне безбедности има одређене елементе и то:

- циљ због којег је систем успостављен – заштита вредности организације (лица, сопствена и поверена имовина и пословање) и остваривање пословног успеха, допринос широј друштвеној заједници;
- снаге и средства потребни за остварење циља – сви ресурси организације самостално или заједно са екстерним снагама (и средствима), а нарочито (интерни и екстерни) субјекти система;

[77] Систем корпоративне безбедности, баш као систем безбедности (Драгишић, 2011, стр. 122), посматра се као подсистем ширих система и систем сачињен од низа подсистема.

- структуру елемената система потребних за остварење појединих активности – подсистеми (организационе целине) који улазе у састав система корпоративне безбедности (нпр, сектор физичког и техничког обезбеђења, сектор унутрашњих истрага, сектор за кризни менаџмент...);
- скуп активности потребних за остварење циља – све системске и функционалне активности које спроводе субјекти система, а које су неопходне за остваривање функције и циља система и
- функцију структурних елемената за остварење циља – заштитна функција организације, која може бити проактивна како и реактивна, и то као најопштија функција система корпоративне безбедности; као и конкретне функције о којима ће касније бити речи.

Систем корпоративне безбедности постоји у динамичном окружењу како организације тако и виших система којима припада. Карактерише га отвореност која омогућава двосмерну интеракцију са окружењем (других система организације или виших система безбедности). Динамичност са адаптабилношћу и регулацијом омогућавају систему корпоративне безбедности опстанак у тим различитим окружењима, прилагођавање на промене како споља тако и изнутра. Спречавају урушавање система дозвољавајући да систем начини промене (да се прилагоди или чак трансформише) ради опстанка. Као и сваки други систем, и систем корпоративне безбедности има своје границе које одређују његово место у организацији и другим системима. Ако се у обзир узме организација у којој је овај систем успостављен, онда је реч о систему који иако има своју хијерархију (нпр. менаџмент и непосредне извршиоце) и сам припада хијерархији система организације или хијерархије виших система безбедности, што је већ представљено.

Систем корпоративне безбедности као крајњи резултат остварује (Стајић и Лукић, 2011, стр. 10-11):

1. теоријски циљ – стицање теоријских знања о елементима који су садржани у појму (система) корпоративне безбедности и
2. практични циљ – имплементација, функционисање, правилно коришћење и развијање оваквог система доприноси остваривању циљева организације у којој је успостављен.

Како је истакнуто, значајан елемент система корпоративне безбедности чине интерни и екстерни субјекти корпоративне безбедности. Интерни субјекти у ширем смислу су руководиоци (менаџери) свих нивоа и сви запослени у правном лицу укључујући и руководиоце свих нивоа, док су у ужем смислу то запослени искључиво на пословима корпоративне безбедности. Екстерни субјекти су сви они субјекати система националне безбедности који би требао да помогну у функционисању система корпоративне безбедности правног лица. Ту спадају: државне институције попут Министарства унутрашњих послова, тужилаштва и судства, органи локалне самоуправе, затим системи корпоративне безбедности других правних лица, научно-истраживачке институције које се баве овом проблематиком и струковна удружења (Мандић и Станојевић, 2020, стр. 50).

3.4.2. Корпоративна безбедност као организација

Уколико корпоративну безбедност посматрамо као организацију, односно организациону целину у организацији као вишем ентитету, онда се за њу може рећи да се „поклапа са основном делатношћу како би подржала стратегију и основне циљеве и тесно сарађивала са својим „партнерима“, односно другим организационим целинама, а у циљу остваривања најбољих резултата“ (Cabric, 2015, str. 19).

Са тренутним нивоем развоја, не бисмо погрешили када бисмо на корпоративну безбедност гледали као на посебну организациону целину. У том случају, рекли бисмо да корпоративна безбедност као посебна организациона целина, чији се запослени баве пословима безбедности, постоји у већим организацијама, док су послови безбедности у мањим организацијама интегрисани у друге организационе целине. Међутим, постоје бројна мишљења која се ефикасно могу аргументовати, а према којима је безбедност интегрисана у организационе целине попут људских ресурса, ревизије или правне службе (Kovacich and Halibozek, 2003).

У било којем решењу организовања послова безбедности кроз организационе целине, активности од којих зависи безбедност организације спроводе запослени као (интерни) субјекти корпоративне безбедности. У првом случају, то су сви запослени у организацији, који се одређују као субјекти у ширем смислу. У другом случају, то су запослени на пословима безбедности, који се одређују као субјекти у ужем смислу (Мандић и Станојевић, 2020, стр. 51).

Истраживање које су спровели Махеш Нала (*Mahesh Nalla*) и Мери Морах (*Merry Morash*) пре више од две деценије укључивало је истраживање односа корпоративних безбедносних јединица са другим одељењима, као и места на којима се налазе у хијерархији организације. Аутори су уочили да је „корпоративна безбедност прешла у више менаџерски режим“ и да је напредовала у хијерархији организације (2002, p. 17). Овакво схватање у сагласности је са ставом да је обезбеђење као безбедносна функција организације једна од кључних менаџерских активности (Fayol, 2016) о чему је било речи у делу рада који се односи на развој корпоративне безбедности.

3.4.3. Корпоративна безбедност као пословна функција

Уколико корпоративну безбедност посматрамо као функцију, она је нешто без чега корпорација не може постојати (Talijan i Ristović, 2012). Као пословна функција, она представља групу послова које обавља правно лице ради остваривања својих циљева (Кековић и Димитријевић, 2018, стр. 237).[78] Има аутора који безбедност посматрају као функцију нижих слојева, која нема стратешки значај, која представља трошак правном лицу (Ludbey et al., 2017). Ипак, широко је распрострањен став да корпоративна безбедност заузима високо место у хијерархијској структури, односно да је инкорпорирана у руководећи (топ) менаџмент или да се налази „уз“ њега (Nalla and Morash, 2002; Кешетовић и Симоновић, 2009; Cubbage and Brooks, 2012; Talijan i Ristović, 2012; Čaleta, 2012; Cabric, 2015; Џигурски, 2018; Мандић, 2020). На тај начин, она је усклађена са корпорацијским смерницама и заштитом добити“ (Cubbage and Brooks, 2012, p. xiii). Уз то, она је блиско повезана са општим менаџментом и осталим функцијама, а нарочито оним које се тичу безбедности, заштите, континуитета пословања и усклађености, и одговорна је за координацију укупне безбедности корпорације (Кековић, 2011; Čaleta, 2012; Cabric, 2015). Можемо дакле закључити да је корпоративна безбедност генерално позиционирана на веома високом месту у хијерархији организације и блиско интегрисана са осталим функцијама организације. Значајан је тренутак препознавања корпоративне безбедности као једне од главних функција пословања која је повезана осталим функцијама правног лица, као и са друштвом у целини у свом пословном окружењу.

[78] На пример, у врло значајној студији идентификован је широки спектар послова корпоративне безбедности, који су сврстани у шест категорија – заштита особља, контрола приступа, заштита имовине, истраге, управљање ризиком и „остало“ (Nalla and Morash, 2002, p. 13).

Тако, према Драгану Тривану (*Dragan Trivan*), корпоративна безбедност јесте „стратешка функција корпорације, која има за циљ остваривање пословног успеха, што подразумева: елиминацију свих ризика и фактора који могу да утичу на остварење пословног успеха; свођење негативних ефеката на најмању могућу меру; способност функционисања у условима криза, њихово превазилажење и нормализацију пословања“ (2012, str. 82). Према наведеној дефиницији, крајњи циљ корпоративне безбедности јесте остваривање пословног успеха, а сама корпоративна безбедност обухвата све оне активности које су усмерене ка реализацији овог циља. Да ли је довољно да као циљ ове стратешке фукције остане остваривање пословног успеха, дискутабилно је. Вредности које се штите корпоративном безбедношћу разнолике су, а по важности, људи су на првом месту. Међутим, како се пословни успех може остварити само преко свих осталих вредности организације, закључује се да се као крајњи циљ заиста може сматрати остваривање пословног успеха.

„Корпоративна безбедност се може одредити као скуп послова којима се од стране институција друштва (државе) обезбеђују лица имовина и пословање корпорација. У ширем смислу, у предмет (садржај) корпоративне безбедности улазе још и безбедносни изазови ризици и претње, те конкретне појаве угружавања безбедности корпорација као и њихови актери“ (Талијан и Талијан, 2010, стр. 14). Денис Чалета (*Denis Čaleta*) додаје да корпоративна безбедност обухвата све активности за идентификовање и имплементирање свих неопходних мера за управљање безбедносним ризицима (2011, p. 40, према Čaleta, 2012, p. 19).

Марко Чабрић иде корак даље у погледу дефинисања корпоративне безбедности истичући да је корпоративна безбедност одговорна за координацију свеукупне безбедности правног лица и „задужена за анализу и квантификацију ризика; измишљање, планирање, постављање и контролу мера безбедности; мерење учинка и успеха безбедносних мера за предвиђање и уочавање трендова, спречавање и заустављање инцидената и разумевање њихове корелације у различитим деловима корпорације и у различитим фазама пословних процеса“ (2015, p. 23). Својом дефиницијом аутор обухвата низ активности које би морале да припадају делокругу корпоративне безбедности у савременом добу.

Николић и Синковски истичу да корпоративна безбедност представља једну од пословних функција и „подразумева безбедност бизниса и групе лица интегрисаних у циљу обављања тог бизниса“. Стога, задатак корпоративне безбедности је да „пословни систем учини стабилним (заштићеним) на путу развоја и у околностима свакодневног увећавања неизвесности и ризика“ (2013, стр. 126, 129).

Изнето схватање корпоративне безбедности као пословне функције није прихваћено код свих аутора. Наиме, Џигурски прави разлику између корпоративне безбедности коју сматра есенцијалном функцијом, безбедности и здравља на раду коју сматра пословном функцијом и физичко-техничког обезбеђења што сматра оперативном функцијом. Поред тога, он пословне функције ставља између есенцијалних функција (виших) и оперативних функција (нижих) у хијерархији „организационих функција“ (2018, стр. 256). Како би се избегли потенцијални проблеми, једно од решења је прихватити да се функције које Џигурски назива пословним схвате као *пословне функције у ужем смислу*, а све функције (организације) које Џигурски назива „организационим“ схвате као *пословне функције у ширем смислу*. С тим у вези, корпоративна безбедност би била пословна функција (у ширем смислу), али са нарочитим значајем, односно смештена на врху лествице организационих функција.

Доста сликовиту дефиницију корпоративне безбедности даје Мијалковић. За њега, корпоративна безбедност или како је још назива, безбедност привредно-енергетских

корпорација обухвата самостално или комбиновано деловање специјализованих служби корпорација и субјеката недржавног и државног сектора безбедности у сферама: безбедносног менаџмента и анализе безбедносних изазова, ризика и претњи; физичког и/или техничког обезбеђења лица, имовине и пословања; безбедности (физичка, техничка и контраобавештајна заштита) интелектуалне својине и права која из ње проистичу, пословних и других тајних података; противпожарне и противдиверзионе заштите; безбедности кадра, материјално-техничких система и пословања у ванредним ситуацијама узрокованих људским, природним и техничко-технолошким факторима и заштите животне средине (2015, стр. 145). Проблем који постоји са наведеном дефиницијом тиче се дела у којем се корпоративна безбедност везује за привредно-енергетске корпорације чиме се занемарују други ентитети (организације) код којих се такође делује у свим наведеним сферама, а са истим циљем – „заштита сопствених интереса и унапређивање личне позиције у домаћем и међународном конкурентном привредном окружењу, и омогућава друштву и држави да задовоље своје потребе“ (Мијалковић, 2015, стр. 145). У вези са тим, овакво тумачење корпоративне безбедности је оправдано усвојити, а без наглашавања индустрије којој припадају (у овом случају привредно-енергетске).

Корпоративна безбедност се често погрешно доживљава као високо прописан задатак са стриктним и нефлексибилним инсистирањем на правилима. У стварности, реч је о широком спектару различитих функција које би могле да сачињавају управљање безбедношћу (познатије као безбедносни менаџмент). У вези са тим, аутори сматрају да постоји јак разлог за укључивање безбедности у области науке о менаџменту (Borodzicz and Gibson, 2007, p. 188; Davidson, 1989; Powell, 2002, p. 34). Као функција управљања, корпоративна безбедност би била интегрисана са свим фазама администрације и операција. Тако би интегрисане функције попут физичког обезбеђења, кадровских пракси, система и процедура ефикасно могле спречити многе губитке стављајући акценат на превентивни приступ (Burnstein, 1978, p. 30).

Препознавањем (корпоративне) безбедности као посебне гране менаџмента, она се подиже на виши ниво чиме се не посматра више само у контексту професионалаца који делају на оперативном нивоу. Један од примера који иде у прилог наведеном јесте чињеница да је за менаџера безбедности од круцијалне важности да познаје анализу трошкова и добити у вези са спречавањем губитака за организацију.[79]

3.4.4. Корпоративна безбедност као својство

На крају, корпоративну безбедност могуће је тумачити и као својство правног лица и у том контексту, она је својство „испољено као стање, процес и/или инструмент заштићености лица, имовине и пословања (објекти заштите) који се штите од свих извора, носиоца и облика угрожавања, а која се постиже људским, материјалним и организационим капацитетима тог лица“ (Мандић, 2020, стр. 169).

Из наведене дефиниције закључује се да је 1) корпоративна безбедност *нужност*, нешто без чега правно лице не постоји (својство); 2) да је она је и један од *циљева* правног лица; као и 3) *средство* за постизање тог циља (стање, процес и/или инструмент).[80]

[79] Magestro, Brandon. (2013). Transitional phase of a security manager: A closer look into the struggles and difficulties experienced during the transition into security management. *Journal of Applied Security Research* 8 (1), pp. 135-150.

[80] Битно је приметити да када безбедност посматрамо као циљ, она је један од циљева, чијим се остваривањем ствара услов за реализацију свих осталих циљева, међу којима је најчешће стицање профита.

Даље, из наведене дефиниције јасно је 1) *шта се штити* – вредности правног лица (лица, сопствена и поверена имовина и пословање); 2) о*д чега* – свих извора, носиоца и облика угрожавања и 3) *на који начин* – употребом свих расположивих ресурса.

Под расположивим ресурсима подразумевају се људски, материјални и организациони ресурси тог правног лица, али и ресурси других правних лица која се изнајмљују/купују с обзиром на то да се обезбеђују сопственим материјалним ресурсима. Овде се не смеју занемарити информациони ресурси, који имају све значајнију улогу како у безбедности, тако и свим осталим областима друштвеног живота. Не треба изгубити из вида и то да су наведени ресурси истовремено и средства за осигурање безбедности и један од објеката заштите правног лица (Марковић, 2021, стр. 13-14).

Питање *од чега* се штите вредности правног лица обухвата изворе, носиоце и облике угрожавања. Изворе угрожавања представљају сви негативни утицаји који угрожавају правно лице и могу бити друштвени, природни и техничко-технолошки. Носиоци угрожавања представљају непосредну конкретизацију извора угрожавања, односно лица и појаве које „врше - извршавају" радњу или процес угрожавања. Деле се на унутрашње, спољашње и комбиноване носиоце, јер угрожавање може да потекне од лица која су запослена у правном лицу, лица која нису запослена у правном лицу и запослених у сарадњи са незапосленима. Под облицима угрожавања правног лица подразумевају се она дела (претње) која наносе штету правном лицу, без обзира на извор, односно носиоца угрожавања (Мандић и Станојевић, 2020, стр. 20).

Дата одређења корпоративне безбедности указују на различите приступе у дефинисању овог концепта. Ради прегледности различитих приступа и аутора који су их користили, састављена је Табела 5.

Табела 5: Приказ начина на који различити аутори схватају корпоративну безбедност (Ауторка)

Корпоративну безбедност могуће је схватити као...	**АУТОРИ**
филозофију	Marković, 2014
систем	Marković, 2007; Даничић и Стајић, 2008; Mijalković і Милошевић, 2011; Кековић и Димитријевић, 2017
организацију	Nalla and Morash, 2002; Borodzicz and Gibson, 2007 (*читава индустрија*)
функцију	Nalla and Morash, 2002; Kovacich and Halibozek, 2003 (*и као процес*) Borodzicz and Gibson, 2007; Brooks, 2011 (*интегрални оквир безбедносних функција*); Талијан и Талијан; 2010; Talijan i Ristović, 2012; Trivan, 2012; Cubbage and Brooks, 2012; Čaleta, 2012; Николић и Синковски, 2013 Cabric, 2015; Мијалковић, 2015; Кековић и Димитријевић, 2018; Цигурски, 2018; Симовић и Манић, 2019
својство	Мандић и Станојевић, 2020

3.5. Корпоративна безбедност и њој сличне гране безбедности

У контексту односа корпоративне и приватне безбедности, у раду се заступа став да су корпоративна безбедност (енг. *Corporative Security*) и приватна безбедност (енг. *Private Security*) два различита концепта. Њихов однос се првенствено може сагледати као однос ужег – корпоративна и ширег појма – приватна безбедност. Реч је о сродним појмовима са значајним заједничким карактеристикама (лат. *genus proximum*), али и специфичностима, које их међусобно разликују (лат. *differentia specificica*) (Лалић, Ћеранић и Сикимић, 2019, стр. 53).

Наведеном иде у прилог подела приватне безбедности на корпоративну безбедност и услужну безбедност. Са једне стране, корпоративна безбедност је пословна функција заштите организације, прилагођена њеним специфичностима, док послове корпоративне безбедности спроводе како сви запослени, тако и она екстерна стручна лица која су ангажована за то. Са друге стране, услужна безбедност подразумева скуп организација које продају и обезбеђују своје безбедносне производе и услуге другим организацијама или приватним (физичким) лицима (Kovacich and Halibozek, 2003, pp. 48-49). Ова подела указује на стуктурне и функционалне разлике. Структурално, ове две врсте безбедности имају различите организације, док функционално, једна има „функцију заштите интереса корпорације и није намењена тржишту“, док друга „продаје услуге безбједности на тржишту у циљу стварања профита“ (Лалић, Ћеранић и Сикимић, 2019, стр. 59). Стога, приватну безбедност чине „оне особе које су запослене или спонзорисане од стране комерцијалног правног лица на основу уговора или `унутар куће`[81] (енг. *in-house*), користећи јавна или приватна средства, да се ангажују у задацима ... где је главна компонента безбедносна или регулаторна функција“ (Sarre and Prenzler, 2009, p. 4).

Ипак, неки аутори приватну безбедност поистовећују са услужном безбедношћу (Shearing and Stenning, 1983; Кековић, 2011; Лабовић, 2015а). Тако, Кековић (2011, стр. 210, 220) сматра да је када се говори о приватној безбедности реч о пружању безбедносних услуга најширем кругу клијената и у том контексту она „постаје широко распрострањена делатност специјализованих привредних субјеката“. Слично томе, Лабовић истиче да „приватна безбедност поред послова приватног обезбеђења лица, имовине и пословања, обухвата и послове приватних војних компанија и многе друге комерцијално засноване послове безбедности (плаћеници, приватизоване казнене установе, различити облици тзв. учешћа грађана у контроли криминалитета, и друго), док се корпоративна безбедност организује и спроводи унутар пословних компанија, а обухвата и послове који се, по правилу, из различитих разлога не поверавају специјализованим субјектима приватне безбедности“ (2015а, стр. 26). Из приложене дефиниције, јасно је да постоји разлика и између приватног обезбеђења и корпоративне безбедности. Појам корпоративне безбедности се суштински разликује од појма „услуга приватног обезбеђења“ (Milošević, 2017, p. 31).

У правцу раздвајања приватне и корпоративне безбедности као две паралелне гране, има аутора (Brooks, 2013; George and Kimber, 2014) који сматрају да корпоративна безбедност није део приватног сектора безбедности, с обзиром на то да приватна безбедност пружа робу и услуге неким трећим лицима, док је корпоративна безбедност уграђена у корпорацију „искоришћавајући по потреби друге елементе индустрије приватне безбедности“ (Brooks and Corkill, 2014, p. 219). Могла би бити занимљива чињеница да су Критичке студије безбедности занемариле у свом „мрежном

[81] Термин унутар куће је буквални превод енглеске кованице *in-house.* У даљем тексту биће коришћен термин интерно.

манифесту“[82] корпоративну безбедност науштрб приватне уговорне безбедности и националне безбедности (Walby, Luscombe and Lippert, 2014, p. 120). То је потврдило став да „корпоративна безбедност није добила исти мултидисциплинарни и теоријски третман као обезбеђење чувара по уговору, јавна полиција или национална и међународна безбедност“ (Lippert, Walby and Steckle, 2013, p. 206).

У литератури се може наићи на поистовећивање корпоративне безбедности са неким другим гранама безбедности. Тако, постоје аутори који корпоративну безбедност користе као еквивалент организационој безбедности (енг. *Organisation Security*) (Brooks, 2010), власничкој безбедности или обезбеђењу имовине (енг. *Proprietary Security*) и безбедности пословања (енг. *Business Security*) (Kovacich and Halibozek, 2003). У првом случају, једино уколико би се корпорација поистоветила са организацијом, могло би се о корпоративној безбедности говорити као о организационој. Власничка безбедност или безбедност пословања, пак, делују као исувише уски појмови да би се сматрали синонимима корпоративне безбедности, а опет, ту је и терминолошко усклађивање појмова које би могло да представља проблем.

Иако је током двадесетог века корпоративна безбедност била повезана са индустријском безбедношћу, која је била усмерена на заштиту пословне тајне, проверу запослених и спречавање саботаже (Russell, 1980 према Walby and Lippert, 2014, p. 3), данас је корпоративна безбедност много више од тога. Индустријска безбедност садржински обухвата све послове безбедности и заштите у индустрији попут управљања људским ресурсима, заштитом животне средине, заштитом од пожара, послова безбедности и здравља на раду, пословима физичко-техничке заштите (Бошковић, 2017). Међутим, индустрија је део свих корпорација, па би поистовећивање индустријске и корпоративне безбедности значило знатно ограничавање делокруга корпоративне безбедности и то на индустријске системе, објекте и постројења.

Слично, има аутора који поистовећују приватну и корпоративну безбедност. Бавећи се појмом приватне безбедности, Стајић наводи да је „приватна (корпоративна) безбедност планска, организована и на закону заснована самостална или заједничка делатност и функција организација, приватних и(ли) професионалних агенција, усмерених на сопствену заштиту или заштиту других, као и заштиту одговарајућих лица, простора, објеката, пословања или делатности, а који нису покривени ексклузивном заштитом државних органа” (2008, стр. 383). Анализирајући елементе приложене дефиниције она пре одговара ономе што је одређено као приватна безбедност.

Поред већ изнетих ставова, Слободан Марковић тежи ка томе да се направи разлика између „корпоративне безбедности као друштвеног односа и корпорацијске безбедности која се односи на корпорацију као конкретно удружење без обзира на то да ли је оно у сектору производње или услуга“ (2014, str. 20). Према оваквом тумачењу, сви до сада изнети ставови о корпоративној безбедност више одговарају појму „корпорацијска безбедност“. С обзиром на специфичан – филозофски приступ који аутор, чији је навод управо наведен, заузима у разумевању концепта корпоративне безбедности, у раду се ипак корпоративна безбедност схвата у ширем контексту, за који се може рећи да обухвата и друштвени однос и корпорацију као удружење, односно организацију.

[82] О томе видети више у: Collective, C. A. S. E. (2006). Critical approaches to security in Europe: A networked manifesto. *Security dialogue* 37 (4), pp. 443-487.

3.6. Функције корпоративне безбедности

Прву студију о процени функција и циљева корпоративне безбедности спровели су Нала и Мораш утврдивши да корпоративна безбедност преузима активности који се обично поистовећују са приватним обезбеђењем (нпр. физичко обезбеђење, безбедност запослених, безбедност имовине, истраге), док остале активности које се сматрају безбедносним су „брига“ других организационих целина које их реализују самостално или у сарадњи са корпоративном безбедношћу (Nalla and Morash, 2002, p. 16). Овакав став данас међутим не налази утемељење како у пракси, тако ни у теорији. Наиме, корпоративна безбедност „обухвата самостално или комбиновано деловање специјализованих служби корпорација и субјеката недржавног и државног сектора безбедности у следећим сферама: физичког и/или техничког обезбеђења лица, имовине и пословања, безбедности (физичка, техничка и контраобавештајна заштита) интелектуалне својине и права која из ње проистичу, пословних и других тајних података, противпожарне и противдиверзионе заштите; безбедноста кадрова, материјално-техничких система и пословања у редовним и ванредним ситуацијама узрокованим људским, природним и техничко-технолошким факторима; заштите животне средине и других вредности и интереса субјеката“ (Мијалковић и Бошковић, 2010, стр. 292).

Ради бољег разумевања концепта корпоративне безбедности, односно шта се то под истом заиста подразумева, у делу рада који следи биће представљени елементи који је чине. Приликом сагледавања елемената (функција) и уједно послова корпоративне безбедности потребно је уважити „циљеве заштите и штићене вредности који су комплементарни са другим циљевима и интересима у јавној и приватној сфери“ (Кековић и Димитријевић, 2017, стр. 236, 238). Ти елементи ће се бити сагледани уз уважавање две ставке:

1. корпоративна безбедност јесте пословна функција и као таква се састоји од (пот)функција и
2. корпоративна безбедност јесте организациони систем и као такав се састоји од (под)система.

Према Чабрићу постоји десет основних елемената корпоративне безбедности:

1. „физичка и техничка безбедност лица, процеса, производа и имовине;
2. заштита репутације компаније и брендова;
3. безбедност информација;
4. управљање безбедношћу;
5. превенција и откривање криминала;
6. борба против превара;
7. истраге;
8. нефинансијско управљање ризиком;
9. управљање континуитетом пословања и опоравак од катастрофе и
10. управљање кризама“ (2015, p. 23).

Џигурски у основне елементе корпоративне безбедности сврстава:

1. „безбедност људи;
2. безбедност материјалних и нематеријалних ресурса;
3. информатичка безбедност;
4. детекција и спречавање криминалитета;
5. управљање ризицима;
6. планирање континуитета пословања;
7. управљање кризама и
8. животна средина, безбедност и здравље на раду“ (2015, стр. 257).

Код неких класификација се не помиње појам елемената, већ појам функција. Једна од таквих класификација издваја једанаест основних функција заштите корпоративних ресурса:

1. „административна безбедност - политике и процедуре;
2. физичка безбедност - заштита објеката и друге имовине;
3. лична безбедност - заштита лица;
4. свест о безбедносној едукацији и програм тренинга – едукација запослених;
5. заштита од пожара - заштита људи и имовине;
6. деловање у ванредним ситуацијама - припрема за најгоре;
7. истраге - истрага непоштовања закона и програм спречавања злочина;
8. државна (владина) безбедност - услуга и подршка по уговорима;
9. информациона безбедност - заштита информација у свим окружењима;
10. заштита руководства - заштита руководећег менаџмента и
11. безбедност догађаја - обезбеђивање безбедности људи и имовине на догађајима“ (Kovacich and Halibozek, 2003, p. 161).

Сличну класификацију функција нуди Триван уважавајући доктрину и праксу земаља са развијеном тржишном економијом и стабилном демократијом. Функције обухватају:

- „административну безбедност (енг. *Administrative Security*) - процедуре и политику у области информатичке заштите;
- физичку и техничку безбедност (енг. *Out-Source/Proprietary*) - машина, постројења и објеката;
- безбедност својине и спољних партнерстава (енг. *Personnel Security*);
- личну безбедност (енг. *Protective Security*) - заштиту лица и заштиту на раду;
- заштиту од пожара (енг. *Fire Security*);
- деловање у ванредним ситуацијама (енг. *Contingency Planning*);
- информациону безбедност (енг. *Information Security*);
- безбедност менаџера (енг. *Executive Security*);
- безбедност на различитим пословним догађајима (енг. *Event Security*);
- безбедност уговорених послова са државним структурама;
- истраге (енг. *Investigations*) - програм заштите од криминалитета и
- програме едукације и развоја безбедносне културе запослених (енг. *Security Education Awareness and Training Program*)“ (Trivan, 2012, str. 87-88).

Узимајући у обзир класификацију елемената/функција корпоративне безбедности других аутора, као и специфичности домаћег окружења Мандић прави разлику између следећих функција:

1. „безбедност на радном месту – безбедност запослених;
2. физичка заштита;
3. техничка заштита;
4. физичко-техничка заштита – контрола приступа;
5. прикупљање, провера, заштита и безбедност података и информација;
6. надзор и контрола у функцији проактивног;
7. унутрашње истраге;
8. безбедност и здравље на раду и заштита животне средине;
9. противпожарна заштита;
10. процена, контрола и управљање ризиком;
11. управљање кризама (кризни менаџмент) и
12. по потреби“ (Мандић и Станојевић, 2020, стр. 27).

Често цитирани аутор, Дејвид Брукс (*David Brooks*) понудио је интегрисан оквир корпоративне безбедности који обухвата два нивоа знања која су неопходна за потребе корпоративне безбедности, односно два нивоа области корпоративне безбедности:

- Ниво 1 (основне категорије): управљање безбедносним ризицима, управљање континуитетом пословања (планирање континуитета, управљање кризама и управљање катастрофама), технологија, физичка безбедност, особље и индустрија и
- Ниво 2 (сродне или подржавајуће категорије): истраге, право, криминологија, управљање објектима, заштита од пожара и лична сигурност и заштита података (2010, p. 236).

Посматрајући корпоративну безбедност као организациони систем, аутори праве разлику између информационе, економске, социјалне и правне безбедности иинформационо-аналитичког обезбеђења (Нинковић и Синковски, 2013, стр. 130) или нешто општије, „и друге припадајуће области безбедности“ (Кековић, 2018).

На основу изнетих подела можемо рећи да у погледу одређивања садржине концепта корпоративне безбедности постоје два правца, а у зависности од тога да ли се корпоративна безбедност посматра као функција или систем. Значајно у вези са тим јесте да се они међусобно не искључују, већ сагледавају овај концепт из различитих углова, и свакако, иако пружају различит степен разраде садржаја ниједна од њих није погрешна.

3.7. Корпоративна безбедност у служби друштвено одговорног пословања

Тешко је рећи да ли друштвено одговорно пословање[83] „ради“ за безбедност или послови корпоративне безбедности „раде“ за друштвено одговорно пословање. Полазећи од тога да је корпоративна безбедност функција која треба да обезбеди постојање свих осталих функција организације, да обезбеди услове опстанка, функционисања и понашања организације онда се чини да управо она „ради“ за друштвено одговорно пословање. Својим (пот)функцијама корпоративна безбедност доприноси организацији да одговорно поступа према широј друштвеној заједници у економском, социјалном и еколошком контексту, а пре свега на добровољној основи.

Корпоративна безбедност се неретко посматра као једна од пословних функција, уколико је дефинишемо као групу послова које обавља правно лице ради остваривања својих циљева. Кековић сматра да тако схваћена корпоративна безбедност подразумева и одређено „друштвено одговорно пословање“– пословање у складу са етичким нормама и на друштвено прихватљив начин. Тако схваћена, корпоративна безбедност обухвата нову форму безбедносне културе – „како заштити друге од себе“ (Кековић, 2018, стр. 18), поред традиционалне бриге – како заштитити себе од других и како заштитити себе од себе. Добар пример друштвено одговорног пословања јесте усвајање и ефикасна примена стандарда из области попут безбедности и здравља на раду или заштитите животне средине. Усвајањем и применом ових и бројних других стандарда, уз наравно поштовање свих законских прописа, доприноси се не само друштвено одговорном пословању, већ и унапређењу репутације, као једне од виталних вредности правног лица.

[83] Израз који је прихваћен и који се користи од стране бројних аутора јесте „Corporate Social Responsibility“ што у буквалном преводу на српски језик значи „корпоративна друштвена одговорност“, с тим да се често користе преводи као „друштвена одговорност“ или „друштвено одговорно пословање“. У даљем раду, користиће се израз „друштвено одговорно пословање“.

Уз то, феномен друштвено одговорног пословања могуће је посматрати и у контексту јачања отпорности критичне инфраструктуре (Ridley, 2011), а имајући у виду значај који ова инфраструктура има за националну безбедност, отпорност представља спрегу која јача однос националне безбедности и друштвено одговорног пословања.

3.7.1. Појам друштвено одговорног пословања

Историја постојања идеје, а потом и појма и концепта друштвено одговорног пословања развија се већ деценијама. Постоји став да је „идеја да пословање има друштвене обавезе била евидентна барем још у деветнаестом веку" (Smith, 2003, p. 52), а да се идеја о друштвеној одговорности први пут формално појавила у праву Немачке 1937. године, усвајањем Закона о акционарским друштвима чиме је први пут држава формално проглашена за једног од заинтересованих субјеката пословања компаније (Rajnović, 2016, p. 1) или у списима историчара Вилијама Лојтенбурга (*William Leuchtenburg*) раних тридесетих година прошлог века. Модерну еру друштвено одговорног пословања обележио је рад Хауарда Р. Боуена (*Howard R. Bowen*) педесетих, а шездесетих година прошлог века је о овој теми почело да се говори и из научне перспективе, да би након важних друштвених покрета у истом периоду уследила еволуирајућа усавршавања и примене (Carroll, 1979, p. 497).

Када је реч о одређењу друштвено одговорног пословања, постоји велики број дефиниција.[84] Већина дефиниций друштвено одговорно пословање описује као концепт у коме компаније интегришу друштвене и еколошке проблеме у своје пословање иу интеракцију са заинтересованим странама и то на добровољној основи (Commission of the European Communities, 2001). Међутим, упркос бројним дефиницијама, један од проблема на који су наишли они који су се бавили њиховом анализом јесте то да оне (дефиниције) „описују феномен, али не дају никакво упутство о томе како се носити са изазовима унутар овог феномена. Стога, изазов за пословање није толико да дефинише друштвено одговорног пословање, колико да разуме како је друштвено одговорног пословање друштвено конструисано у специфичном контексту и како то узети у обзир када се развијају пословне стратегије" (Dahlsrud, 2003, p. 11). Јер, реч је о поступању које се „може исплатити: односно може бити добар посао за све и ићи руку под руку са добрим корпоративним управљањем" (Claessens, 2003, p. 23).

Уколико се следи терминолошко одређење „Corporate Social Responsibility" реч је о одговорности коју корпорација има према друштву. Како је корпорација једна врста организације и како се друштво може схватити како на локалном, тако и на националном и глобалном нивоу, па и у симбиози са државом, следи да се може говорити и о одговорности коју организација има како према друштву на локалном нивоу (непосредно), тако и према држави на националном нивоу и међународној заједници на глобалном нивоу (посредно). На овај начин, концепт друштвено одговорног пословања представља спону између организације са једне стране, и државе и међународне заједнице са друге стране.

[84] Број дефиниција толики је да је вероватно и немогуће одредити га тачно. О дефиницијама видети више у: Dahlsrud, Alexander. (2008). How corporate social responsibility is defined: an analysis of 37 definitions. *Corporate social responsibility and environmental management* 15 (1), pp. 1-13; Hamidu, Ahmad, Haron, Md and Amran, Azlan. (2015). Corporate social responsibility: A review on definitions, core characteristics and theoretical perspectives. *Mediterranean Journal of Social Sciences* 6 (4), pp. 83-95; Činčalová, Simona and Prokop, Martin. (2019). How is Corporate Social Responsibility Meant: Analysis of 100 Definitions. *Hradec Economic Days* 9 (1), pp. 112–120; Ridley, Gail. (2011). National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience. *Journal of Business Ethics* 103 (1), pp. 111-125.

Арчи Керол (*Archie Carroll*) издваја економске, правне, етичке и дискреционе (волонтерске) категорије пословања које дефиниција друштвене одговорности мора да садржи како би одговорила на читав низ обавеза које пословање има према друштву (1979, p. 499). Концепт друштвено одговорног пословања треба и мора да обухвати неколико димензија, и то економску (социо-економска и финансијска), друштвену (социјална), еколошку (животна средина), заинтересоване субјекте, добровољну (волонтеризам) (Dahlsrud, 2008, p. 4), којима други аутори додају још и филантропску, легалну и интеграцијску (Činčalová and Prokop, 2019, p. 115). Како је на глобалном нивоу расла пажња за еколошка питања постепено су одговорност за животну средину и одрживост интегрисани у теорију друштвено одговорног пословања, па је фокус постављен на одрживи развој у овој области.[85] Група аутора као шест главних димензија издваја волонтеризам, интернационализацију или управљање екстерналијама (факторима који утичу на права различитих заинтересованих страна, а о којима се не води директно рачуна у процесу доношења одлука), орјентацију ка заинтересованим странама, усклађивање друштвених и економских одговорности, праксе и вредности (праксе и стандарди који се прихватају као филозофија или сет вредности) и димензију „изван филантропије" (превазилажење филантропије и могућност да инструментално и сратешки задовољава очекивања заинтересованих страна и циљеве организације) (Hamidu et al., 2015). На крају, вероватно најсвеобухватнији приступ одређењу димензија друштвено одговорног пословања даје Шафикур Рахман (*Shafiqur Rahman*) издвајајући чак десет главних димензија: обавезе према друштву, укључивање заинтересованих страна, побољшање квалитета живота, економски развој, етичност пословања, поштовање закона, добровољност, људска права, заштита животне средине, транспарентност и одговорност (2011, pp. 172-173).

Из свега до сада изнетог, реч је о коцепту који се развија, најблаже речено, већ седам деценија и који је постаокарактеристика и саставни део политике сваке организације, или бар оне која је препознала значај и потребу за имплементацијом овог концепта. Реч је о концепту који се може схватити и као саморегулација коју уводе организације како би поправиле или, чешће, унапредиле неке сегменте пословања попут радне снаге, питања људских права, заштите животне средине. Значај друштвено одговорног пословања огледа се у тежњи ка остваривању не само економских циљева, већ и социјалних и еколошких, чиме омогућава самој организацији да остварује циљеве у овим сферама. Организација не само да ефикасно послује и остварује профит, већ и одговорно послује према свом окружењу, живом и неживом, односно како према заинтересованим странама, тако и према природи. На неки начин, концепт друштвено одговорног пословања заснива се на интересима организације и законским и другим прописима, али истовремено их и превазилази.

3.7.2. Допринос корпоративне безбедности друштвено одговорном пословању

Поставља се питање на који начин представити допринос корпоративне безбедности друштвено одговорном пословању. Као једно од могућих решења јесте користити елементне корпоративне безбедности, са једне стране и елемете или димензије друштвено одговорног пословања, са друге стране.

На основу свега изнетог о елементима корпоративне безбедности могуће је рећи да она обухвата следеће области: заштита лица, заштита имовине (укључујући заштиту

[85] О повезаности концепта друштвено одговорног пословања, корпоративне одрживости и одрживог развоја видети више у: Јовановић, Милица. (2017). Корпоративна друштвена одговорност као детерминанта одрживости. *Economics of Sustainable Development*1 (1), pp. 93-107.

информационих система и информација) и заштита пословања (укључујући заштиту репутације и угледа), односно безбедност запослених укључујући безбедност и здравље на раду и спречавање насиља на радном месту и безбедност личних података; физичка и техничка заштита, заштита од пожара, заштита животне средине, бављење ризицима, кризама и катастрофама, спровођење истрага.

Све ове области корпоративне безбедности своје тежиште налазе у законима и подзаконским актима, а потом и у стандардима и интерној регулативи која ближе одређује субјекте, средства и начине остваривања циљева постављених пред корпоративну безбедност. Дакле, корпоративна безбедност има правну димензију. Како она функционише у служби организације у оквиру које је успостављена, следи да правна димензија корпоративне безбедности доприноси правној димензији друштвено одговорног пословања. Тако је и са осталим димензијама друштвено одговорног пословања – социјалном, еколошком и економском димензијом.

Социјална димензија друштвено одговорног пословања, могла би у првом реду да обухвати бригу о заинтересованим странама укључујући поштовање и промовисање људских права. Ако би се брига о заинтересованим странама у које спадају како запослени, тако и партнери и клијенти, односно сва физичка и правна лица која су на неки начин повезана са организацијом посматрали као једно од начела друштвено одговорног пословања, лако можемо рећи да је она и једно од начела корпоративне безбедности. Уз то, сама брига о физичким лицима као заинтересованим странама нужно значи и поштовање права која та лица уживају као људска бића.

Функције корпоративне безбедности су тако организоване да у сваком тренутку заинтересованим странама пружају заштиту у различитим сферама уз обавезно поштовање свих права које заинтересовани субјекти уживају, а нарочито поштовање људских права. Тако, све функције корпоративне безбедности су усмерене на заштиту запослених од различитих облика угрожавања здравља и живота, у сваком тренутку, односно како у редовним условима (свакодневно), тако и у ванредним условима (када наступи криза или катастрофа). Заштита запослених тако не подразумева само заштиту у погледу безбедности и здравља на раду, заштите од пожара и других техничких акцидената, насиља и других облика девијантног понашања, већ значи и заштиту њихових личних података. Партнерима и клијентима као физичким лицима, такође се пружа сваки облик заштите у циљу њихове безбедности када се налазе на локацијама и објектима организације са којом послује, али по потреби и ван локације када се ради са њиховим личним подацима. Када се партнери и клијенти посматрају као правна лица, заштита се такође пружа, а пре свега у виду заштите података и информација који се размењују и поверене имовине уколико је има. Додатно, заинтересовани субјекти не морају бити само физичка и правна лица, већ то може бити и заједница у којој организација послује, где се у првом плану обично налази филантропија и волонтирање, као још два елемента социјалне димензије или чак посебна, еколошка димензија.

Филантропске и волонтерске активности налазе се изван редовног пословања организације и не доприносе директно економској сфери пословања, с тим да могу позитивно деловати на репутацију и углед, што би индиректно ипак допринело и економској сфери пословања. Како филантропија представља давања у виду новца или у виду робе, услуга, па чак и простора или имовине организације, и волонтирање давања у смислу времена, знања и вештина запослених онда би организација била та која даје за заједницу, док су запослени у сектору корпоративне безбедности ти који ће своје време, знање и вештине дати заједници. Социјалном димензијом, организација показује да разуме потребе како својих запослених, партнера и клијената, тако и шире заједнице и друштва у којем ради, а како томе доприноси и корпоративна безбедност, па би било неоправдано занемарити њен утицај.

Даље, потребно је са аспекта еколошке димензије сагледати допринос корпоративне безбедности друштвено одговорном пословању, а за коју је већ наведено да се налази у првом плану када је реч о односу организације за заједницом или окружењем на чијем простору послује. Како еколошка димензија обухвата бригу о животној средини, њоју првом реду одговара заштита животне средине, али и друге функције корпоративне безбедности попут заштите од пожара, бављења ризицима, кризама и катастрофама или спровођења истрага које итекако могу допринети овој димензији. Са друге стране, еколошка димензија не обухвата само заштиту животне средине, већ свеобухватну бригу о њој, укључујући иновацију и модернизацију процеса и производа или употребу чистих технологија. Корпоративна безбедност јесте укључена у еколошку димензију друштвено одговорног пословања, али није једина функција организације која доприноси овој димензији.

Иако се може говорити засебно о свакој димензији друштвено одговорног пословања, све четири димензије су повезане и могуће их је разумети кроз њихову међусобну повезаност преко које остварују утицај једна на другу. Када је реч о социјалној и еколошкој димензији, оне су ипак међусобно испреплетане, тако да би било врло ризично рећи да активности социјалне димензије доприносе искључиво социјалним циљевима или да активности еколошке димензије доприносе искључиво еколошким циљевима. Такође, за неке активности би се могло рећи да преплићу социјалну и еколошку димензију те тако доприносе како социјалним, тако и еколошким циљевима. Као пример наведеног, могуће је узети систем ХСЕ (енг. *HSE – Health, Safety, Environment*) који повезује управљање ризицима у областима здравља, заштите и животне средине. Овај систем могао би имати нешто другачије форме попут ХССЕ (енг. *HSSE – Health, Safety, Security and Environment*) или ХССЕQ (енг. *HSSEQ – Health, Safety, Security, Environment and Quality*) (Мандић и Станојевић, 2020, стр. 432). Овај систем, и уједно функција представљају добар пример доприноса корпоративне безбедности и њених функција друштвено одговорном пословању.

На крају, када је реч о економској димензији, првенствено треба имати у виду да се социјалном и еколошком димензијом друштвено одговорног пословања доприноси самој економској димензији, што потврђује њихову међусобну испреплетаност. Када је реч о овој димензији, пре је реч о посредном доприносу него директном. Корпоративна безбедност кроз проактивне и реактивне мере остварује заштиту свих вредности организације чиме доприноси остварењу или чак увећању профита. На тај начин, корпоративна безбедност има утицај на финансијску и економску сферу пословања.

Корпоративну безбедност, као и било коју другу функцију организације треба да карактерише етичност у виду скупа вредности које се поштују у односима са заинтересованим странама, транспарентност онолико колико то дозвољава природа активности ове функције, као и побољшање квалитета живота кроз законе, стандарде и интерну регулативу. Како ове карактеристике одговарају карактеристикама друштвено одговорног пословања, могуће је корпоративну безбедност посматрати као припадајући део шире структуре под називом друштвено одговорно пословање, а тиме и елемент који доприноси механизму којем припада.

Корпоративна безбедност, са једне стране, као део приватне безбедности доприноси целокупној безбедности државе и друштва, док са друге стране, као систем и функција организације доприноси њеним циљевима. Како је један од циљева организације друштвено одговорно пословање, корпоративна безбедност управо доприноси таквом пословању, посредно утичући на окружење које је шире од организације. На тај начин, корпоративна безбедност директно или путем друштвено одговорног пословања чини ефикаснијим целокупан систем националне безбедности и уопште, повећава степен безбедности заједнице.

3.8. Корпоративна безбедност у Републици Србији – правни оквир организације и функционисања корпоративне безбедности

Уопште, да би се говорило о постојању корпоративне безбедности неопходно је да она буде утемељена у легалним оквирима. Из тог разлога, сагледавање њеног постојања у правним лицима, треба и мора да почне од нормативног оквира. У зависности од обима те анализе, она може обухватити потом и међународне стандарде и добру праксу, али и интерну регулативу усвојену на нивоу правног лица. С обзиром на предмет ове врсте интерне регулативе, она се у највећој мери неретко оставља „изван јавности" означена као пословна или друга тајна. Стандарди нису обавезујући, осим уколико се закон не позове на стандард што може бити дискутабилно и уопште под питањем да ли то треба учинити. За разлику од ове две категорије, чија анализа и неће бити предмет рада, са нормативним оквиром је другачије. Отворен приступ овој категорији извора даје могућност његове анализе у мери у којој се то жели или је потребно. У тексту који следи дат је ограничен приказ нормативног оквира за који се сматра да служи као основ за успостављање организације и функција корпоративне безбедности у правним лицима. Анализа која следи није исцрпна, те оставља простор за много подробније бављење законском регулативом и пратећим актима како на нивоу корпоративне безбедности, тако и на нивоу појединачних послова који су јој припадајући.

Велики техничко-технолошки системи (уједно и критична инфраструктура), привредна друштва и друга правна лица препозната су као део извршног дела система националне безбедности. Поред надлежних органа државне управе, послове унутрашње безбедности обављају и правна и физичка лица која врше послове приватног обезбеђења (Стратегија националне безбедности Републике Србије, 2019, 5.1.2.). Са аспекта корпоративне безбедности, то су правна лица која се баве самозаштитном делатношћу, као и физичка лица која имају неку од лиценци која се издаје за вршење послова приватног обезбеђења. Уз то, органи државне управе и институције надлежне за спољне послове, правосуђе, здравство, демографију, људска и мањинска права, економију, образовање и научну делатност, привреду, енергетику, телекомуникације, саобраћај и транспорт, инфраструктуру, заштиту животне средине, културу, органи аутономних покрајина и јединица локалне самоуправе јесу други субјекти значајни за националну безбедност (Стратегија националне безбедности Републике Србије, 2019, 5.1.2.).

Сви наведени субјекти обављајући послове из својих делатности за које су надлежни доприносе функционисању државе и пружању основних потреба становништву те је могуће подвести их под националну критичну инфраструктуру. Иако се нигде у највишем стратешком акту наше државе не спомиње корпоративна безбедност, из наведених одредаба она се може наслутити. Сви набројани субјекти обезбеђујући основне производе и услуге доприносе стању националне безбедности. Додатно, ниво безбедности ових субјеката утиче на ниво безбедности државе, па су системи безбедности ових субјеката у неку руку одговорни и за систем безбедности државе. У том контексту, на државном стратешком нивоу постоји простор за бављењем корпоративном безбедношћу и њеним укључивањем у систем националне безбедности.

Државни органи, органи државне управе, органи аутономних покрајина, органи јединица локалне самоуправе, привредна друштва и друга правна лица, који у складу са законом, извршавају задатке које имају у систему одбране спадају у извршни део система одбране. Како одговорност за припрему за одбрану и одбрану лежи на националном нивоу, тако су и ови субјекти одговорни за припрему и одбрану према значају и капацитетима које имају. Не само да треба континуирано да изграђују способности за супротстављање свим облицима угрожавања, већ и да обезбеде успешно функционисање како у миру, тако и у ванредном стању и рату, односно да обезбеде

услове за непрекидно снабдевање основним животним добрима и функционисање служби од јавног интереса, обезбеде потребан ниво робних резерви и ратних материјалних резерви, као и извршавање војне, радне и материјалне обавезе.[86] Уз све наведене обавезе, иако су носиоци заштите и спасавања јединице цивилне заштите и ватрогасно-спасилачке јединице, горе наведени субјекти учествују и у извршавању задатака заштите и спасавања (Стратегија одбране Републике Србије, 2019, 6.3.). Поред наведених обавеза које проистичу из Стратегије одбране, министарства из области одбране, у оквиру свог делокруга, извршавају законе из области одбране, прописе за рад у ратном и ванредном стању, општа акта Народне скупштине и Владе, задатке утврђене Планом одбране Републике Србије и одговарају за поступање правних лица која су у њиховој надлежности (Закон о одбрани, члан 24). План одбране, поред националног, доноси се за ова министарства као и за државне органе, органе аутономних покрајина, органе јединица локалне самоуправе, привредна друштва и друга правна лица од значаја за одбрану (Закон о одбрани, члан 81). Како се међутим рад бави заштитом критичне инфраструктуре у мирнодопским условима, даљих разматрања о безбедности и заштити критичне инфраструктуре у ванредном и ратном стању неће бити.

3.8.1. Физичка и техничка заштита

На прву помисао шта то значи или обухвата безбедност правног лица издвојиле би се физичка и техничка заштита. Физичка и техничка заштита јесу две основне функције корпоративне безбедности, али свакако не једине, на шта ће касније бити и указано.

Физичка заштита односи се на физичко обезбеђење, односно обезбеђење које се пружа личним присуством и непосредном активношћу службеника обезбеђења. Са друге стране, техничка заштита се односи на обезбеђење које се врши техничким средствима и уређајима. С обзиром на то да службеници обезбеђења обављају послове из свог делокруга рада користећи техничка средства, могуће је говорити о физичко-техничкој заштити.

У области физичке и техничке заштите издвајају се следећи нормативни акти:

- Закон о приватном обезбеђењу, Сл. гласник РС, бр. 104/2013, 42/2015, 87/2018
  - Правилник о начину вршења послова техничке заштите и коришћења техничких средстава, Сл. гласник РС, бр. 91/2019
  - Правилник о начину примене овлашћења службеника обезбеђења, Сл. гласник РС, бр. 59/2019;
  - Правилник о боји и саставним деловима униформе службеника обезбеђења, Сл. гласник РС, бр. 49/2019
  - Правилник о садржини, изгледу и начину употребе легитимације службеника приватног обезбеђења, Сл. гласник РС, бр. 3/2016, 30/2019
  - Уредба о минималним техничким условима код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама, Сл. гласник РС, бр. 9/2021
- Закон о оружју и муницији, Сл. гласник РС, бр. 20/2015, 10/2019, 20/2020, 14/2022
  - Правилник о евиденцијама које воде правна лица и предузетници, Сл. гласник РС, бр. 3/2016
  - Правилник о поступку издавања, изгледу и садржини образаца и исправа о оружју предвиђених Законом о оружју и муницији, Сл. гласник РС, бр. 16/2016

[86] Конкретне обавезе које треба да испуне превасходно се односе на живот и рад грађана и задовољење потреба снага одбране у ванредном стању и у рату. Међутим, када се ове обавезе извршавају у контексту припреме за ванредно и ратно стање, онда се способности за супротстављање свим облицима угрожавања изграђују и за мирнодопске услове.

- Правилник о просторно-техничким условима за безбедно смештање и чување оружја и муниције, Сл. гласник РС, бр. 9/2016, 106/2016, 50/2018
- Закон о порезима на употребу, држање и ношење добара, Сл. гласник РС, бр. 26/2001, 80/2002, 43/2004, 31/2009, 101/2010, 24/2011, 68/2014, 112/2015, 86/2019, 118/2021, 92/2023

Закон о приватном обезбеђењу, Сл. гласник РС, бр. 104/2013, 42/2015, 87/2018 кровни је нормативни документ којим се уређује област физичке и техничке заштите. Одредбе овог закона примењују се како на службенике обезбеђења, тако и на правна лица која користе услуге приватног обезбеђења, односно оне који организују самозаштитну делатност.

Самозаштитна делатност јесте унутрашњи облик организовања обезбеђења лица, имовине и пословања за сопствене потребе (Закон о приватном обезбеђењу, члан 2).[87] Схваћена на овакав начин, самозаштитна делатност најближа је организацији и функцијама корпоративне безбедности, с тим да је много ужа делатност од делатности корпоративне безбедности. Закон предвиђа да самозаштитна делатност обавезно има организовану планску, организациону и контролну функцију када се обезбеђује заштита обавезно обезбеђених објеката (Закон о приватном обезбеђењу, члан 5). На основу ове одредбе, правна лица којима припадају објекти од посебног значаја за одбрану могу да ангажују друге за физичку заштиту али имају обавезу планирања, организације и контроле. Проблем са наведеном одредбом тиче се чињенице да је уредба којом се одређују ови објекти стављена ван снаге, о чему ће бити речи у раду. Закон предвиђа да се за ову врсту послова издаје посебна лиценца и то Лиценца за вршење послова самозаштитне делатности и Лиценца за вршење послова обезбеђења транспорта и преноса новца и вредносних пошиљки у обављању самозаштитне делатности (Закон о приватном обезбеђењу, чланови 7 и 8), ако су испуњени предвиђени услови (члан 45).

Правно лице које користи услуге приватног обезбеђења дужно је да за вршење послова приватног обезбеђења ангажује правно лице, предузетника или физичко лице искључиво са лиценцом за вршење послова приватног обезбеђења (Закон о приватном обезбеђењу, члан 8); има закључен писани уговор са правним лицем или предузетником за приватно обезбеђење које је ангажовало да му пружа те услуге (Закон о приватном обезбеђењу, члан 20); на видљивом месту истакне обавештење да је објекат или простор који се користи за јавну употребу, заштићен видео обезбеђењем или ако архивиране снимке не чува најмање 30 дана или ако их, на захтев, не стави на увид овлашћеном полицијском службенику (Закон о приватном обезбеђењу, члан 32)[88]; осигура одржавање и сервисирање техничких средстава у складу са овим законом и уговором (Закон о приватном обезбеђењу, члан 35). И ова правна лица су дужна да воде одговарајуће евиденције (Закон о приватном обезбеђењу, члан 67).

Основа коришћења услуга приватног обезбеђења јесте израда акта о процени ризика у заштити лица, имовине и пословања. Процена ризика у заштити лица, имовине и пословања врши се по захтевима и на начин прописан важећим српским стандардом у

[87] Оваквим одређењем, самозаштитна функција је сведена само на унутрашњу службу физичког обезбеђења. У раду се брани став по којем се терминолошки и појмовно погрешно користи појам самозаштите, јер би самозаштита требало да буде једна од полазних основа функционисања система обезбеђења правних лица и као таква да обухвати све запослене као интерне субјекте обезбеђења (Стајић и Радивојевић, 2015, стр. 176).

[88] Употреба термина овлашћени полицијски службеник је упитна. Наиме, нигде се у Закону који уређује рад полиције и запослених лица у полицији не спомиње овај термин. У употреби је термин полицијски службеник, као и овлашћено службено лице, па се поставља питање одакле термин овлашћени полицијски службеник осим уколико се термин „овлашћени“ не наводи као придев уз термин „полицијски службеник“. У наредном тексту, задржаће се употреба овог термина уважавајући терминологију коју је користио Законодавац.

области приватног обезбеђења (Закон о приватном обезбеђењу, члан 20). Реч је о стандарду *Безбедност и отпорност друштва – Процена ризика – Захтеви и упутство за оцењивање усаглашености – СРПС А.Л2.003:2025.* На основу ове процене, израђује се план обезбеђења, односно план поступања са ризицима и то према методологији стандарда *Безбедност и отпорност друштва – Процена ризика – Део 5: Упутство за израду плана обезбеђења – СРПС ТР А.Л2.003-5:2020.* Ипак, из наведеног, уочава се да је стандард постављен изнад закона, те је упитна оправданост оваквог одлучивања.

Службеник обезбеђења дужан је да послове приватног обезбеђења лица, имовине и пословања врши на начин којим се не омета рад државних органа и нарушава спокојство грађана (Закон о приватном обезбеђењу, члан 19); пружа услуге приватног обезбеђења само по уговору (Закон о приватном обезбеђењу, члан 20); носи униформу и оружје на законом прописан начин (Закон о приватном обезбеђењу, чланови 22, 25, 26 и 60); поступи по наређењу полицијског службеника према одредбама закона (Закон о приватном обезбеђењу, члан 27); интервенише у складу са писаним процедурама (Закон о приватном обезбеђењу, члан 44); приликом вршења послова обезбеђења и примене овлашћења код себе има легитимацију, или је да на увид овлашћеном полицијском службенику или грађанину према коме примењује овлашћење, на њихов захтев и врати легитимацију по престанку радног односа (Закон о приватном обезбеђењу, члан 63); као тајну, у складу са законом и другим прописима којима се уређује тајност података, чува све податке за које сазна у вршењу послова (Закон о приватном обезбеђењу, члан 69). Службеник обезбеђења дужан је врши радње за које је овлашћен законом, подзаконским актима и планом обезбеђења (Закон о приватном обезбеђењу, чланови 46-57).

Законом о приватном обезбеђењу уређује питање сарадње између Министарства унутрашњих послова и субјеката из области приватног обезбеђења. Са аспекта корпоративне безбедности, биће издвојене одређене активности: Министарство унутрашњих послова врши безбедносну проверу (лица која треба да раде на пословима приватног обезбеђења) којом се утврђује постојање или непостојање безбедносне сметње (Закон о приватном обезбеђењу, члан 3); спроводи обуку и стручни испит физичких лица за вршење послова приватног обезбеђења (Закон о приватном обезбеђењу, чланови 13 и 14); прима захтеве за издавање лиценци и издаје лиценце за вршење послова приватног обезбеђења (Закон о приватном обезбеђењу, члан 15); поступа по жалби на решење о захтеву за издавање лиценце и решење о одузимању лиценце (Закон о приватном обезбеђењу, члан 17) и даје одобрење за набавку оружја (Закон о приватном обезбеђењу, члан 24). Месно надлежна полицијска управа прима обавештење о закључењу, анексу или раскиду уговора за физичку заштиту лица која се врши са оружјем и за пружање услуга видео надзора са архивирањем снимка (Закон о приватном обезбеђењу, члан 20); прима захтев за издавање легитимације службенику обезбеђења (Закон о приватном обезбеђењу, члан 63), као и обавештење о употреби средстава принуде од службеника обезбеђења и извештај о употреби средстава принуде са мишљењем од одговорног лица у правном лицу (Закон о приватном обезбеђењу, члан 56). Полиција прима обавештење о вршењу кривичних дела или прекршаја са елементима насиља у штићеном објекту, штићеном простору или простору који је видљив из штићеног простора или објекта или на правцу кретања од оператера у Контролном центру (Закон о приватном обезбеђењу, члан 44); прима привремено одузете предмете уз потврду о привременом одузимању предмета (Закон о приватном обезбеђењу, члан 49), као и обавештење о привременом задржавању лица од службеника обезбеђења (Закон о приватном обезбеђењу, члан 50).

Министарство унутрашњих послова врши надзор приватног обезбеђења – испуњености услова и начина обављања делатности, примену овлашћења и вођење евиденција и спровођење прописа о држању и ношењу оружја приватног обезбеђења (Закон о

приватном обезбеђењу, члан 70). Овлашћени полицијски службеник проверава услове и начин обављања делатности, примену овлашћења, вођење евиденција, начин чувања и ношења ватреног оружја, и, по потреби, спроводи и друге радње којима се остварује непосредан и ненајављен увид у вршење послова приватног обезбеђења, разматра примедбе на записник о обављеном надзору и, према потреби, понавља радње на које се примедбе односе, односно мења или одустаје од предложене мере, може да у току надзора, уз потврду, привремено одузме пословне књиге, евиденције, другу документацију, видео снимке или друге исправе, до окончања поступка надзора (Закон о приватном обезбеђењу, члан 71). Овлашћени полицијски службеници Министарства могу лице које поседује лиценцу која се за обављање послова приватног обезбеђења издаје физичком лицу, да упути на лекарски преглед, ако се оправдано посумња да више не испуњава психофизичке услове за вршење послова (Закон о приватном обезбеђењу, члан 73)[89]; да захтева стављање архивираних снимака на увид (Закон о приватном обезбеђењу, члан 32) и да изда наређење службенику обезбеђења (Закон о приватном обезбеђењу, члан 27).[90]

Министар утврђује ближи начин вршења послова техничке заштите и коришћења техничких средстава (ч Закон о приватном обезбеђењу, лан 33); ближи начин примене овлашћења утврђених овим законом (Закон о приватном обезбеђењу, члан 57); боју и саставне делове униформе коју носе службеници обезбеђења (Закон о приватном обезбеђењу, члан 58); ближу садржину, изглед и начин употребе легитимације службеника приватног обезбеђења (Закон о приватном обезбеђењу, члан 64). У вези са последње наведеним, донети су следећи подзаконски акти чије одредбе треба да узму у обзир правна лица која користе услуге приватног обезбеђења или организују самозаштитну делатност: *Правилник о начину вршења послова техничке заштите и коришћења техничких средстава, Сл. гласник РС, бр. 91/2019; Правилник о начину примене овлашћења службеника обезбеђења, Сл. гласник РС, бр. 59/2019; Правилник о боји и саставним деловима униформе службеника обезбеђења, Сл. гласник РС, бр. 49/2019; Правилник о садржини, изгледу и начину употребе легитимације службеника приватног обезбеђења, Сл. гласник РС, бр. 3/2016, 30/2019*.

Посебно се издваја *Уредба о минималним техничким условима код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама, Сл. гласник РС, бр. 9/2021,* којом се утврђују минимални технички услови код обавезне уградње система техничке заштите у банкама, њиховим пословницама, платним институцијама, пословницама јавног поштанског оператора и другим финансијским организацијама.

Службеници обезбеђења могу да раде са оружјем уколико је то предвиђено планом обезбеђења. У том случају, издваја се и *Закон о оружју и муницији, Сл. гласник РС, бр. 20/2015, 10/2019, 20/2020, 14/2022*. Међутим, и правна лица која обављају самозаштитну делатност могу уз одобрење надлежног органа, односно уз пријаву надлежном органу, набављати оружје и основне делове оружја (Закон о оружју и муницији, члан 40). Правна лица дужна су да оружје и муницију чувају у складу са одредбама овог Закона и да о њему воде прописану евиденцију, као и да се придржавају других релевантних одредаба (Закон о оружју и муницији, члан 40). Правна лица дужна су да воде евиденције о оружју (врста, марка, модел, калибар, фабрички број оружја) и муницији, као и евиденције о запосленим лицима (име, презиме, јединствени матични број грађана, број личне карте односно идентификационог документа, пребивалиште, адреса и уверење о здравственој способности). *Правилник о евиденцијама које воде правна лица и предузетници, Сл.*

[89] Поставља се питање да ли је уопште овлашћени полицијски службеник компетентан да „оправдано" процени психофизичко стање службеника обезбеђења за обављање послова.

[90] Самим тим што Законодавац користи реч „наређење", ограничавају се напори да се приватно обезбеђење начини партнером полицији у систему националне безбедности.

гласник РС, бр. 3/2016, прописује да правна лица који набављају оружје, основне делове за оружје и муницију у складу са делатношћу којом се баве, воде евиденције: набављеног оружја и основних делова за оружје, набављене муниције, потрошене муниције, запослених лица (Правилник, 3/2016, члан 7). *Правилником о поступку издавања, изгледу и садржини образаца и исправа о оружју предвиђених Законом о оружју и муницији, Сл. гласник РС, бр. 16/2016* прописани су изглед и начин издавања Одобрења за набављање оружја за правна лица и предузетнике (Правилник, 16/2016, члан 9), као и изглед и садржина образаца на којим се издаје оружани лист за правна лица и предузетнике (Правилник, 16/2016, члан 13). Чување оружја и муниције, као и питање изношења оружја регулисано је *Правилником о просторно-техничким условима за безбедно смештање и чување оружја и муниције, Сл. гласник РС, бр. 9/2016, 106/2016, 50/2018*. Правна лица дужна су да обезбеде просторно-техничке услове за безбедан смештај и чување (закључани и одвојени у металним орманима, сефовима, касама или трезорима који се не могу лако отворити и који су опремљени сигурносним механичким системом за закључавање) оружја и муниције и то у објекту који је зидан од чврстог материјала и који се налази у седишту правног лица (Правилник, 50/2018, члан 10а). Наведени Закон о оружју и муницији, нужно је повезан и са *Законом о порезима на употребу, држање и ношење добара, Сл. гласник РС, бр. 26/2001, 80/2002, 43/2004, 31/2009, 101/2010, 24/2011, 68/2014, 112/2015, 86/2019, 118/2021, 92/2023,* посебно одредбе које се односе на порез на регистровано оружје (чланови 21-26а).

3.8.2. Безбедност података и информација

Подаци и информације јесу ресурс и уједно вредност сваког правног лица. Због значаја које имају за правно лице, заштита података и информација је један од највиших интереса правног лица и уједно један од главних задатака корпоративне безбедности. Безбедност података и информација као функција корпоративне безбедности обухвата пре свега правни аспект, који ће на овом месту да буде представљен и то у односу на две групе података и информација:

1) податке и информације које штите пословање правног лица (пословна тајна) са подацима од интереса за Републику Србију (тајни податак) и
2) податке и информације које штите лица (подаци о личности).

У области безбедности података и информација издвајају се следећи нормативни акти:

- Закон о заштити пословне тајне, Сл. гласник РС, бр. 53/2021
- Закон о тајности података, Сл. гласник РС, бр. 104/2009
  - Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима, Сл. гласник РС, бр. 54/2010
  - Уредба о обрасцима безбедносних упитника, Сл. гласник РС, бр. 30/2010
  - Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима, Сл. гласник РС, бр. 89/2010
  - Уредба о посебним мерама надзора над поступањем са тајним подацима, Сл. гласник РС, бр. 90/2011
  - Уредба о начину и поступку означавања тајности података, односно докумената, Сл. гласник РС, бр. 8/2011
  - Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа, Сл. гласник РС, бр. 63/2013
  - Уредба о посебним мерама физичко-техничке заштите тајних података, Сл. гласник РС, бр. 97/2011

- Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима, Сл. гласник РС, бр. 53/2011
- Закон о слободном приступу информацијама од јавног значаја, Сл. гласник РС, бр. 120/2004, 54/2007, 104/2009, 36/2010,105/2021
- Упутство за израду и објављивање информатора о раду органа јавне власти, Сл. гласник РС, бр. 10/2022
- Закон о заштити података о личности, Сл. гласник РС, бр. 87/2018
- Одлука о утврђивању Стандардних уговорних клаузула, Сл. гласник РС, бр. 5/2020
- Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности, Сл. гласник РС, бр. 40/2019
- Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности, Сл. гласник РС, бр. 45/2019, 112/2020
- Закон о информационој безбедности, Сл. гласник РС, бр. 6/2016, 94/2017, 77/2019
- Уредба о утврђивању Листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја, Сл. гласник РС, бр. 94/2019
- Правилник о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја, Сл. гласник РС, бр. 9/2020
- Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, Сл. гласник РС, бр. 94/2016
- Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, Сл. гласник РС, бр. 94/2016
- Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, Сл. гласник РС, бр. 11/2020
- Уредба о криптобезбедности и заштити од компромитујућег електромагнетног зрачења, Сл. гласник РС, бр. 57/2019, којом се уређују ближи услови за криптографска
- Уредба о обезбеђивању и заштити информационих система државних органа, Сл. гласник РС, бр. 41/1990
- Упутство за израду и усвајање пројеката информационих система органа управе, Сл. гласник РС, бр. 49/1989

Од значаја су и следећи закони, који се на овом месту неће посебно анализирати:

- Закон о привредним друштвима, Сл. гласник РС, 36/2011, 99/2011, 83/2014, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021, 19/2025 у члану 72 одређује појам пословне тајне
- Кривични законик, Сл. гласник РС, 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 у члану 240 одређује одавање пословне тајне

Пре анализе наведених аката, треба уздвојити следеће. Закон о заштити пословне тајне и Закон о привредним друштвима регулише област заштите информација у привредним ентитетима, док Закон о тајности података регулише област заштите информација у државним институцијама, док Кривични законик дефинише која се дела из ових области сматрају кривичним, односно за која су дела предвиђене кривичне санкције.

Правна заштита пословне тајне од незаконитог прибављања, коришћења и откривања регулисана је *Законом о заштити пословне тајне, Сл. гласник РС, бр. 53/2021.* Пословна тајна

представља информације које нису у целини или у погледу структуре и скупа њихових саставних делова опште познате или лако доступне лицима која у оквиру својих активности уобичајено долазе у контакт са таквом врстом информација, имају комерцијалну вредност и штите се одређеним мерама: израда интерног акта о руковању пословном тајном и кругу лица и њиховим правима и обавезама приликом руковања пословном тајном, мере физичке или електронске заштите приступа и руковања пословном тајном, означавање докумената ознаком „пословна тајна" или сличном ознаком, ограничавање приступа просторијама и датотекама у којима се налазе информације које се сматрају пословном тајном или закључивање уговора о поверљивости, односно неоткривању поверљивих информација са лицима која потенцијално могу да дођу у посед пословне тајне, укључујући запослене, пословне партнере, спољне сараднике и консултанте, односно потписивање изјава о поверљивости или неоткривању поверљивих информација од стране наведених лица (Закон о заштити пословне тајне, члан 2). На овом месту, подвлачи се да је правно лице под чијом је законитом контролом пословна тајна држалац пословне тајне (Закон о заштити пословне тајне, члан 2).

Област заштите тајних података који су од интереса за националну и јавну безбедност, одбрану, унутрашње и спољне послове Републике Србије уређена је *Законом о тајности података, Сл. гласник РС, бр. 104/2009.* Правно лице са седиштем у Републици Србији, коме је издат одговарајући сертификат од стране надлежног органа сматра се корисником тајног податка. Уз то, правно лице које оснива државни орган или се финансира у целини, односно у претежном делу из буџета, државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења могу такође да поступају са тајним подацима (Закон о тајности података, члан 2).

Правно лице као корисник тајног податка, има право приступа тајним подацима који су неопходни за обављање послова према сертификату који има (Закон о тајности података, члан 42). Закон прописује и услове за издавање сертификата правном лицу (Закон о тајности података, члан 49), начин подношења захтева (Закон о тајности података, члан 51) и садржину захтева (Закон о тајности података, члан 52). Садржина, облик и начин достављања сертификата за приступ тајним подацима, као и повезане обавезе лица која поступају са тајним подацима прописани су *Уредбом о садржини, облику и начину достављања сертификата за приступ тајним подацима, Сл. гласник РС, бр. 54/2010*. Закон предвиђа и попуњавање основног безбедносног упитника за правна лица (Закон о тајности података, члан 59) и посебног безбедносног упитника (Закон о тајности података, члан 60), док је образац ових упитника прописан *Уредбом о обрасцима безбедносних упитника, Сл. гласник РС, бр. 30/2010*. Органи јавне власти воде евиденције решења о сертификатима степена тајности „ПОВЕРЉИВО", „СТРОГО ПОВЕРЉИВО" и „ДРЖАВНА ТАЈНА", за лица која у органу јавне власти обављају функцију или су запослена, односно за лица која обављају послове. Садржај евиденција решења о сертификату и евиденција о изјавама, као и друга релевантна питања у области вођења ових евиденција прописани су у *Уредби о садржини, облику и начину вођења евиденција за приступ тајним подацима, Сл. гласник РС, бр. 89/2010*. Питање унутрашње контроле у органу јавне власти регулисано је посебном *Уредбом о посебним мерама надзора над поступањем са тајним подацима, Сл. гласник РС, бр. 90/2011*. Посебним уредбама прописани су ближи критеријуми за одређивање степена тајности „ПОВЕРЉИВО" и „ИНТЕРНО" у органима јавне власти, Министарству одбране, Министарству унутрашњих послова, Канцеларији Савета за националну безбедност и заштиту тајних података и Безбедносно-информативној агенцији, као и за одређивање степена тајности „ДРЖАВНА ТАЈНА" и „СТРОГО ПОВЕРЉИВО". Међутим, без обзира на степен тајности, приликом означавања тајности, овлашћена лица су у обавези да се придржавају одредби *Уредбе о начину и поступку означавања тајности података, односно докумената, Сл. гласник РС,*

бр. 8/2011. Овлашћено лице може тајне податке доставити другим правним или физичким лицима уколико правно или физичко лице испуњава организационе и техничке услове за чување тајних података.

Посебне мере заштите тајних података, које се односе на начин и поступак утврђивања испуњености организационих и техничких услова за чување тајних података достављених правном или физичком лицу по основу уговорног односа прописане су посебном *Уредбом о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа, Сл. гласник РС, бр. 63/2013*. Организациони услови односе се нарочито на организацију процеса рада, заштиту приступа тајним подацима, заштиту од неовлашћеног коришћења тајних података, одређивање одговорног лица задуженог за спровођење мера заштите, као и утврђивање поступка у случају ванредних и хитних околности, док се технички услови односе нарочито на физичко-техничку заштиту простора, односно просторија у којима се чувају тајни подаци, противпожарну заштиту, заштиту тајних података приликом преношења и достављања изван просторија у којој се чувају, транспорт тајних података, обезбеђивање и заштиту информационо-телекомуникационим средстава којима се врши преношење и достављање тајних података и спровођење прописаних мера крипто-заштите (Уредба, бр. 63/2013, члан 2). *Уредба о посебним мерама физичко-техничке заштите тајних података, Сл. гласник РС, бр. 97/2011*, прописује посебне мере физичко-техничке заштите тајних података које се односе на просторије где се ови подаци чувају, простор око просторија, одређивање административне и безбедносне зоне, одговарајуће безбедносно техничке опреме, као и мере обезбеђења безбедносних зона. На крају, с обзиром на све већи значај који имају информационо-телекомуникационе технологије, и њихову све већу присутност у свим сферама живота и рада, издваја се и *Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима, Сл. гласник РС, бр. 53/2011.* Последње две уредбе обезбеђују имплементацију мера физичко-техничке заштите тајног податка, укључујући и уградњу и постављање техничких средстава заштите, утврђивање безбедносне зоне и заштиту ван безбедносне зоне, као и мера заштите информационо-телекомуникационих система.

За органе јавне власти, у овом сегменту, издваја се и *Закон о слободном приступу информацијама од јавног значаја, Сл. гласник РС, бр. 120/2004, 54/2007, 104/2009, 36/2010,105/2021.* Реч је о органу Републике Србије, органу аутономне покрајине, органу општине, града, градске општине и града Београда, јавном предузећу, установи, организацији, привредном друштву и другом правном лицу које је настало под условима прописаним одредбама закона (Закон о слободном приступу информацијама од јавног значаја, члан 3). Сви органи јавне власти дужни су да јавно објављују и јавности учине доступним све информације о свом раду које се сматрају информацијама од јавног значаја, а у сврху омогућавања остварења интереса јавности да зна исте (Закон о слободном приступу информацијама од јавног значаја, члан 1). Информација од јавног значаја јесте све оно о чему јавност има оправдан интерес да зна (Закон о слободном приступу информацијама од јавног значаја, члан 2). То су, на пример, увек информације о угрожавању, односно заштити здравља становништва и животне средине (Закон о слободном приступу информацијама од јавног значаја, члан 4). Одређен скуп информација од јавног значаја објављује се у Информатору о раду, за који органи јавне власти имају право и обавезу објављивања. Ближе смернице за израду и објављивање овог документа дате су у *Упутству за израду и објављивање информатора о раду органа јавне власти, Сл. гласник РС, бр. 10/2022.* Издваја се одредба по којој орган власти може тражиоцу ограничити остваривање права на приступ информацијама од јавног значаја ако би тиме повредио право на приватност, право на

заштиту података о личности, право на углед или неко друго право лица (Закон о слободном приступу информацијама од јавног значаја, члан 14).

Заштита података о личности регулисана је посебним *Законом о заштити података о личности, Сл. гласник РС, бр. 87/2018*, с тим да се ова питања регулишу и другим законима у зависности од области обраде података и делатности правног лица. Тако се у области обраде и слободног приступа информацијама од јавног значаја регулише и горе наведеним законом или у области рада и запошљавања Законом о раду (биће речи у делу текста који обрађује Закон о раду). У сваком случају, закон обавезује на прописивање и посебних мера заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини (Закон о заштити података о личности, члан 91). Правно лице може бити руковалац (правно лице које одређује сврху и начин обраде података о личности), обрађивач (правно лице које обрађује податке о личности у име Руковаоца), прималац или чак надлежни орган уколико испуњава услове према закону (Закон о заштити података о личности, члан 4). Обрада података о личности мора бити у складу са законом (Закон о заштити података о личности, члан 12) и она се најчешће спроводи на основу пристанка лица на које се подаци о личности односе (нпр. припремање, закључивање и испуњење уговора приликом запошљавања), обавезе извршења уговора закљученог са лицем на које се подаци односе или за предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора или обавезе у циљу поштовања правних обавеза руковаоца (нпр. у вези са запосленима и радно ангажованим лицима). Обавезе руковаоца јесу примена свих начела обраде података, поступање по захтевима (Закон о заштити података о личности, чланови 21 и 22), обавештење о обради (Закон о заштити података о личности, чланови 23 и 24), као и остваривање права лица (Закон о заштити података о личности, чланови 26-40). Поједини руковаоци имају посебне обавезе и то уговорни однос са обрађивачем (Закон о заштити података о личности, члан 45), вођење евиденција о радњама обраде (Закон о заштити података о личности, члан 47), бележење радњи обраде надлежних органа (Закон о заштити података о личности, члан 48), обавештење о повреди заштите података (Закон о заштити података о личности, чланови 52 и 53), процена утицаја на заштиту података (Закон о заштити података о личности, чланови 54-55), одређивање лица за заштиту података (Закон о заштити података о личности, чланови 56-58) и израда Кодекса поступања (Закон о заштити података о личности, члан 59).

Правни однос између руковаоца и обрађивача одређен је законом и посебно, *Одлуком о утврђивању Стандардних уговорних клаузула, Сл. гласник РС, бр. 5/2020.* Под овим условима одређеним законом, руковалац и обрађивач података о личности дужни су да одреде лице за заштиту података о личности, да објаве контакт податке лица за заштиту података о личности и доставе их Поверенику (Закон о заштити података о личности, члан 56). Закон је прописао положај и обавезе овог лица (Закон о заштити података о личности, чланови 57 и 58). Руковалац је дужан да о повреди података о личности која може да произведе ризик по права и слободе физичких лица одмах обавести Повереника, односно лице на које се подаци односе (Закон о заштити података о личности, чланови 52 и 53). У вези са првим случајем, донет је *Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности, Сл. гласник РС, бр. 40/2019.* Руковалац је дужан да пре него што започне са обрадом података о личности, за које постоји вероватноћа да ће проузроковати висок ризик за права и слободе физичких лица, изврши процену утицаја предвиђених радњи обраде. Врсте ових радњи наведене су у *Одлуци о листи врста радњи обраде података о личности за које се мора*

извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности, Сл. гласник РС, бр. 45/2019, 112/2020.

У области информационе безбедности тренутно је актуелан *Закон о информационој безбедности, Сл. гласник РС, бр. 6/2016, 94/2017, 77/2019*, с тим да је израђен Нацрт новог закона о информационој безбедности. На овом месту, биће представљене неке од одредби важећег Закона, и биће указано на уредбе које су тренутно важеће. Правно лице, попут органа власти или организационе јединице органа власти које користи ИКТ систем у оквиру обављања своје делатности јесте оператор система (Закон о информационој безбедности, члан 2). Закон одређује операторе информационо-комуникационих система (ИКТ система) од посебног значаја, прописује њихове обавезе и евиденције које су дужни да воде (Закон о информационој безбедности, члан 6), као и мере заштите ових система (Закон о информационој безбедности, члан 7). Оператори се одређују према областима делатности и у сврху тога усвојена је *Уредба о утврђивању Листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја, Сл. гласник РС, бр. 94/2019. Правилник о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја, Сл. гласник РС, бр. 9/2020* прописује шта све поменуте евиденције треба да садрже. Мере заштите информационо-комуникационих система од посебног значаја посебно се уређују *Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, Сл. гласник РС, бр. 94/2016.* Оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система (Закон о информационој безбедности, члан 8). У вези са садржајем овог акта, усвојена је *Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, Сл. гласник РС, бр. 94/2016*. Оператори ИКТ система од посебног значаја дужни су да обавештавају о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедност (Закон о информационој безбедности, члан 11), а који су утврђени чланом 11а, као и статистичке податке о свим инцидентима у ИКТ систему (Закон о информационој безбедности, члан 11б). Поступак обавештавања о инцидентима, листу, врсте и значај инцидената према нивоу опасности, поступање и размену информација прописани су ближе *Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, Сл. гласник РС, бр. 11/2020.* Органи власти, укључујући и правна лица са јавним овлашћењима дужна су да имају своје центре за превенцију безбедносних ризика у ИКТ системима (ЦЕРТ) (Закон о информационој безбедности, члан 18).

Закон уређује и област криптобезбедности и заштите од компромитујућег електромагнетног зрачења. У овом сегменту, усвојена је и *Уредба о криптобезбедности и заштити од компромитујућег електромагнетног зрачења, Сл. гласник РС, бр. 57/2019,* којом се уређују ближи услови за криптографска решења, криптографске производе, вођење регистара из области криптобезбедности, проверу компромитујућег електромагнетног зрачења и пружање услуга уз накнаду правним и физичким лицима изван система јавне власти у области криптобезбедности и заштите од компромитујућег електромагнетног зрачења. Од подзаконских аката издвајају се још и *Уредба о обезбеђивању и заштити информационих система државних органа, Сл. гласник РС, бр. 41/1990* и *Упутство за израду и усвајање пројеката информационих система органа управе, Сл. гласник РС, бр. 49/1989*.

3.8.3. Људски ресурси и безбедност запослених

Људски ресурси се на овом месту анализирају двојако: 1) као посебна организациона целина сваког правног лица која је одговорна за управљање и подршку радној снази и 2) као функција корпоративне безбедности која као таква недвосмислено утиче на ниво безбедности правног лица.

3.8.3.1. Људски ресурси као организациона целина правног лица

Управљање људским ресурсима у било ком правном лицу неизоставни је део пословања правног лица. Запослени у сектору људских ресурса спроводе планирање, регрутовање и селекцију кандидата, праћење рада запослених, њихово усавршавање, осмишљавање система награђивања и санкционисања, као и послове отпуштања запослених. Из наведеног, уочава се да у правном лицу постоји посебна организациона целина која се бави пословима у области људских ресурса. Ипак, делатност сектора људских ресурса важна је са аспекта корпоративне безбедности, јер многа радна места само на први поглед делују безбедносно ирелевантна, док то никако није случај.

Значајна активност у раду сектора људских ресурса, коју на овом месту треба подвући, јесте такозвана безбедносно радна провера (радне и личне прошлости кандидата) која треба да спречи „запошљавање неодговарајућих кандидата који могу представљати потенцијални ризик по рад и вредности правног лица“ (Мандић и Станојевић, 2020, стр. 195). Ову проверу не треба мешати са безбедносном провером којом се утврђује постојање или непостојање безбедносне сметње, коју у складу са Законом о полицији врши Министарство унутрашњих послова. Безбедносној провери у овом смислу подлежу кандидати за пријем у радни однос у Министарство, кандидати за пријем у радни однос у другим државним органима, кандидати за обављање послова детективске делатности или службеника обезбеђења, и у другим случајевима утврђеним посебним законом (Закон о полицији, члан 102), као што је провера кандидата за издавање знака идентификације у области ваздухопловства (Закон о ваздушном саобраћају, члан 231а).

Да би службеници приватног обезбеђења добили лиценцу за вршење послова приватног обезбеђења, поред осталих прописаних услова морају да прођу безбедносну проверу којом се утврђује да ли постоје безбедносне сметње (Закон о приватном обезбеђењу, чланови 3, 12). Безбедносна провера дакле врши се за службенике обезбеђења, у процесу издавања лиценце. Безбедносно-оперативна провера се врши за физичка лица за набављање и држање оружја (Закон о оружју и муницији, члан 11). Министарство унутрашњих послова је надлежно за спровођење провере.

Интересантно је да вршење безбедносне провере није предвиђено за власнике правних лица за приватно обезбеђење. На овај начин, селективно се врши процена ризикујући да се лиценцира правно лице чији је власник упитне криминалне прошлости или садашњости, односно да корисник услуга изнајмљује и плаћа исте индиректно „дајући новац“ за потенцијалне нелегалне послове.

Закон о ваздушном саобраћају, Сл. гласник РС, бр. 73/2010, 57/2011, 93/2012, 45/2015, 66/2015, 83/2018, 9/2020, 62/2023, предвиђа спровођење безбедносне провере за лица којима се издаје знак идентификације, за ваздухопловне инспекторе и проверивача, лица која обављају контролу обезбеђивања, инструкторе у области обезбеђивања, одговорне руководиоце за обезбеђивање у ваздухопловству, валидаторе обезбеђивања у ваздухопловству, контролоре летења, чланове посаде ваздухоплова, као и за лица која имају приступ безбедносно осетљивим информацијама од значаја за обезбеђивање у ваздухопловству (Закон о ваздушном саобраћају, члан 231а). У овом случају, обавеза подношења захтева за вршење ове провере у надлежности је издаваоца знака

идентификације, Директората или послодавца. Министарство унутрашњих послова је и у овом случају надлежно за спровођење провере.

Безбедносном провером се утврђује да ли постоје безбедносне сметње због којих неко лице не може да врши послове за које је ангажован или треба да буде ангажован. Ипак, овај закон нешто другачије одређује безбедносне сметње него што је то учињено у Закону о приватном обезбеђењу у члану 3. У вези са тим, оправдано би било да се из Закона о ваздушном саобраћају преузму још неки услови постојања безбедносне сметње попут закључивања споразума о признању кривичног дела са надлежним органом за дела за које се гони по службеној дужности или ако је лице члан или учествује у активностима или на било који начин подржава организације чије су активности или циљеви забрањени (Закон о ваздушном саобраћају, члан 231б).

3.8.3.2. Људски ресурси и безбедност запослених као функција корпоративне безбедности

На овом месту се као посебна функција корпоративне безбедности издваја функција људских ресурса и уз њу безбедност запослених по питању њихових права на рад и у вези са радом из следећег разлога. Најпре, сектор људских ресурса обавља у свом свакодневном раду послове делегиране од стране система корпоративне безбедности, и то у три области: регрутовање и селекција кадрова – запошљавање нових лица, престанак радног односа запосленог по било ком основу и праћење рада запослених (Мандић и Станојевић, 2020, стр. 53). Додатно, придржавајући се у свом раду законских и подзаконских прописа, сектор људских ресурса директно утиче на безбедност свих запослених.

У области људских ресурса и безбедности запослених издвајају се следећи нормативни акти који индиректно, али позитивно утичу на стање корпоративне безбедности у правном лицу:

- Закон о раду, Сл. гласник РС, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017, 113/2017, 95/2018
- Закон о централном регистру обавезног социјалног осигурања, Сл. гласник РС, бр. 95/2018, 91/2019
- Закон о доприносима за обавезно социјално осигурање, Сл. гласник РС, бр. 84/2004, 61/2005, 62/2006, 5/2009, 52/2011, 101/2011, 47/2013, 108/2013, 57/2014, 68/2014, 112/2015, 113/2017, 95/2018, 86/2019, 153/2020, 44/2021, 118/2021, 138/2022, 92/2023
- Закон о здравственом осигурању, Сл. гласник РС, бр. 25/2019, 92/2023
- Закон о запошљавању и осигурању за случај незапослености, Сл. гласник РС, бр. 36/2009, 30/2010, 88/2010, 38/2015, 113/2017, 113/2017, 49/2021
- Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, Сл. гласник РС, 91/2015, 50/2018
- Закон о запошљавању странаца, Сл. гласник РС, бр. 128/2014, 113/2017, 50/2018, 31/2019, 62/2023
- Закон о евиденцијама у области рада, Сл. гласник РС, бр. 46/1996, РС 101/2005, РС 36/2009
- Закон о државним и другим празницима у Републици Србији, Сл. гласник РС, бр. 43/2001, 101/2007, 92/2011
- Закон о професионалној рехабилитацији и запошљавању особа са инвалидитетом, Сл. гласник РС, бр. 36/2009, 32/2013
- Правилник о начину праћења извршавања обавезе запошљавања особа са инвалидитетом и начину доказивања извршења те обавезе, Сл. гласник РС, бр. 101/2016

- Правилник о ближим условима, критеријумима и стандардима за спровођење мера и активности професионалне рехабилитације, Сл. гласник РС, бр. 112/2009
- Правилник о ближем начину, трошковима и критеријумима за процену радне способности и могућности запослења или одржања запослења особа са инвалидитетом, Сл. гласник РС, бр. 36/2010, 97/2013
- Закон о забрани дискриминације, Сл. гласник РС, бр. 22/2009, 52/2021
- Закон о спречавању дискриминације особа са инвалидитетом, Сл. гласник РС, бр. 33/2006, 13/2016
- Закон о родној равноправности, Сл. гласник РС, бр. 52/2021
- Правилник о вођењу евиденције и извештавању о остваривању родне равноправности, Сл. гласник РС, бр. 67/2022
- Правилник о садржају и начину достављања Плана мера за отклањање или ублажавање неравномерне заступљености полова и годишњег извештаја о његовом спровођењу, Сл. гласник РС, бр. 89/2010
- Закон о заштити узбуњивача, Сл. гласник РС, бр. 128/2014
- Правилник о начину унутрашњег узбуњивања, начину одређивања овлашћеног лица код послодавца, као и другим питањима од значаја за унутрашње узбуњивање код послодавца који има више од десет запослених, Сл. гласник РС, бр. 49/2015, 44/2018
- Закон о облигационим односима, Сл. гласник, бр. 29/1978, 39/1985, 45/1989, 57/1989, 31/1993, РС 18/2020
- Закон о агенцијском запошљавању, Сл. гласник РС, бр. 86/2019
- Закон о волонтирању, Сл. гласник РС, бр. 36/2010
- Закон о мирном решавању радних спорова, Сл. гласник РС, бр. 125/2004, 104/2009, 50/2018
- Закон о штрајку, Сл. лист СРЈ, бр. 29/96 и Сл. гласник РС, бр. 101/2005, 103/2012

Додатно, посебно се издваја и следећи закон, који за разлику од претходно наведених има директна утицај на корпоративну безбедност:

- Закон о спречавању злостављања на раду, Сл. гласник РС, бр. 36/2010
- Правилник о правилима понашања послодаваца и запослених у вези са превенцијом и заштитом од злостављања на раду, Сл. гласник РС, бр. 62/2010

Права, обавезе и одговорности из радног односа, односно по основу рада, уређују се *Законом о раду, Сл. гласник РС, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017, 113/2017, 95/2018* и другим законима, као и колективним уговором и уговором о раду или правилником о раду, односно уговором о раду. Послодавац је дужан да запосленом за обављени рад исплати зараду, у складу са законом, општим актом и уговором о раду, запосленом обезбеди услове рада и организује рад ради безбедности и заштите живота и здравља на раду, у складу са законом и другим прописима, запосленом пружи обавештење о условима рада, организацији рада, правилима у вези са испуњавањем уговорних и других обавеза из радног односа и правима и обавезама које произлазе из прописа о раду и прописа о безбедности и заштити живота и здравља на раду, запосленом обезбеди обављање послова утврђених уговором о раду и затражи мишљење синдиката у случајевима утврђеним законом, а код послодавца код кога није образован синдикат од представника кога одреде запослени (Закон о раду, члан 16).

Како цео закон нормативно уређује права и обавезе које правно лице у својству послодавца има у области рада, уместо преопширног бављења овим законом, кратак осврт биће направљен на начин на који овај закон уређује питања заштите података о личности, на шта је у претходном тексту указано, а потом ће бити наведени други релевантни закони и подзаконски акти значајни за ову област анализе. Кандидат је дужан да, приликом заснивања радног односа, послодавцу достави исправе и друге

доказе о испуњености услова за рад на пословима за које заснива радни однос (Закон о раду, члан 26). Исти члан прописује да послодавац нема право да тражи одређене групе података (о породичном, односно брачном статусу и планирању породице). Заштита личних података (овде се не говори о подацима о личности) подразумева право запосленог да оствари увид у документе који садрже личне податке и да захтева брисање података који нису од непосредног значаја за послове које обавља, као и исправљање нетачних података, право на ограничавање достављања ових података трећем лицу и овлашћења за прикупљање, обрађивање, коришћење и достављање ових података (Закон о раду, члан 83).[91]

Заснивање радног односа подразумева и закључивање уговора о раду или другог уговора у складу са Законом, који је послодавац у обавези да у оригиналу или копију држи у седишту или другој пословној просторији послодавца или на другом месту, у зависности од тога где запослени или радно ангажовано лице ради. Такође, послодавац је дужан да на основу уговора о раду или другог уговора о обављању послова закљученог у складу са овим Законом поднесе јединствену пријаву на обавезно социјално осигурање (Закон о раду, члан 35).

У складу са *Законом о централном регистру обавезног социјалног осигурања, Сл. гласник РС, бр. 95/2018, 91/2019,* послодавац је дужан да поднесе јединствену пријаву у електронском облику на централни регистар, најкасније пре ступања запосленог и другог радно ангажованог лица на рад, односно у року од три радна дана од дана почетка обављања делатности, односно од дана престанка запослења, престанка обављања послова или обављања делатности, односно од дана настале промене у току осигурања.

Питања социјалног осигурања регулисана су посебним законима. Прописима о обавезном социјалном осигурању, односно *Законом о доприносима за обавезно социјално осигурање, Сл. гласник РС, бр. 84/2004, 61/2005, 62/2006, 5/2009, 52/2011, 101/2011, 47/2013, 108/2013, 57/2014, 68/2014, 112/2015, 113/2017, 95/2018, 86/2019, 153/2020, 44/2021, 118/2021, 138/2022, 92/2023,* послодавац у својству правног лица јесте обвезник доприноса за запослене као осигуранике (члан 6). Закон уређује питања основице доприноса, стопе доприноса, начин обрачунавања и плаћања доприноса, као и друга питања од значаја за утврђивање и плаћање доприноса.

У складу са *Законом о здравственом осигурању, Сл. гласник РС, бр. 25/2019, 92/2023,* послодавац у својству правног лица дужан је да достави филијали податке који су од значаја за утвђивање чињеница важних за стицање и остваривање права из обавезног здравственог осигурања, као и омогући матичној филијали увид у евиденцију и документацију (Закон о здравственом осигурању, члан 42), достави филијали захтев за исплату накнаде зараде са свим потребним доказима (Закон о здравственом осигурању, члан 102), уплати износ накнаде плаћених трошкова на рачун осигураног лица (Закон о здравственом осигурању, члан 127), као и да Републичком фонду достави податке од значаја за поступак накнаде штете (Закон о здравственом осигурању, члан 227).

Закон о запошљавању и осигурању за случај незапослености, Сл. гласник РС, бр. 36/2009, 30/2010, 88/2010, 38/2015, 113/2017, 113/2017, 49/2021, прописује права и обавезе послодавца у области запошљавања и осигурања за случај незапослености (Закон о запошљавању и осигурању за случај незапослености, чланови 34 и 35). У складу са законом, послодавац може да оствари право на субенције за запошљавање (Закон о запошљавању и осигурању за случај незапослености, члан 50), може да тражи додатно образовање и обуку чије трошкове сам сноси (Закон о запошљавању и осигурању за

[91] Видети више у: Рељановић, Марио. (2020). „Заштита података о личности у радном односу". У С. Андоновић, Д. Прља и А. Дилигенски (Ур.). *Заштита података о личности у Србији* (стр. 61-92). Београд: Институт за упоредно право.

случај незапослености, члан 52) и подноси пријаву потребе за запошљавањем у земљи (Закон о запошљавању и осигурању за случај незапослености, члан 93).

Одредбе Закона о раду примењују се и на запослене који су упућени на рад у иностранство од стране послодавца, као и на запослене стране држављане и лица без држављанства који раде код послодавца на територији Републике Србије (Закон о раду, члан 2). Међутим, ове области уређене су и посебним законима. *Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, Сл. гласник РС, 91/2015, 50/2018*, прописује услове под којима послодавац може да упути запосленог на привремени рад у иностранство (Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, чланови 7, 8 и 9). Послодавац је у обавези да најпре са запосленим закључи анекс уговора о раду (Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, члан 11), изврши промену основа осигурања (Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, члан 12), да обезбеди здравствено, пензијско и инвалидско осигурање и осигурање за случај незапослености (Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, члан 14); безбедност и здравље на раду (Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, члан 15); смештај, исхрану и превоз за долазак и одлазак са рада (Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, члан 16); зараду (Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, члан 17) и припрему за упућивање на привремени рад (Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити, члан 18).

Услед дефицита домаће радне снаге, све чешће послодавци запошљавају странце за рад у правним лицима. С тим у вези, са аспекта корпоративне безбедности, а посебно оне која се успоставља у секторима критичне инфраструктуре, од значаја је *Закон о запошљавању странаца, Сл. гласник РС, бр. 128/2014, 113/2017, 50/2018, 31/2019, 62/2023*, одредбе које се односе на обавезе послодаваца у овој овој области. Послодавац има право да (привремено) запосли странца само под условима прописаним законом (Закон о запошљавању странаца, члан 3). Са странцем се закључује уговор о раду и послодавац је у обавези да сву документацију у вези са запошљавањем чува (Закон о запошљавању странаца, члан 9). Послодавац је дужан да запосленом исплати сва новчана потраживања (Закон о запошљавању странаца, члан 15) и спроводи процену за запошљавање према одредбама закона (Закон о запошљавању странаца, члан 16). Закон предвиђа и остваривање права и обавеза из акта између послодавца и страног послодавца о упућивању на привремени рад (Закон о запошљавању странаца, члан 19).

Послодавац је дужан да води дневну евиденцију о прековременом раду запослених (Закон о запошљавању странаца, члан 55), као и месечну евиденцију о заради и накнади зараде (Закон о запошљавању странаца, члан 122). У вези са вођењем евиденција, од значаја је посебан *Закон о евиденцијама у области рада, Сл. гласник РС, бр. 46/1996, РС 101/2005, РС 36/2009.* Према наведеном закону, правна лица у својству послодавца воде евиденције о запосленим лицима, зарадама запослених лица, запосленима на раду у иностранству, запосленим странцима и корисницима права инвалидског осигурања (Закон о евиденцијама у области рада, чланови 2 и 3). У вези са вођењем евиденција, такође је од значаја питање заштите података о личности.

Као подршка члану 70 Закона о раду у вези празника као нерадних дана, од значаја је посебан *Закон о државним и другим празницима у Републици Србији, Сл. гласник РС, бр. 43/2001, 101/2007, 92/2011.*

Заштита особа са инвалидитетом и запосленог са здравственим сметњама регулисана је како Законом о раду (Закон о раду, члан 101), тако и *Законом о професионалној рехабилитацији и запошљавању особа са инвалидитетом, Сл. гласник РС, бр. 36/2009, 32/2013.* Сваки послодавац који има најмање 20 запослених у обавези је да има у радном односу одређени број особа са инвалидитетом (Закон о професионалној рехабилитацији и запошљавању особа са инвалидитетом, члан 24). Закон прописује одређену накнаду коју послодавац мора да плати услед неизвршавања ове обавезе (Закон о професионалној рехабилитацији и запошљавању особа са инвалидитетом, члан 26), односно повластице које послодавац остварује уколико испуни одређене активности (Закон о професионалној рехабилитацији и запошљавању особа са инвалидитетом, чланови 27, 31 и 32). Више о извршавању обавезе запошљавања особа са инвалидитетом прописано је *Правилником о начину праћења извршавања обавезе запошљавања особа са инвалидитетом и начину доказивања извршења те обавезе, Сл. гласник РС, бр. 101/2016*, посебно чланови 5, 6, 7, 11, 13, 14 и 15. Када код особе са инвалидитетом настане повреда на раду или професионална болест у време када је особа у радном односу код послодавца, трошкове професионалне рехабилитације особе са инвалидитетом сноси послодавац (Закон о професионалној рехабилитацији и запошљавању особа са инвалидитетом, члан 19). Ближи услови, критеријуми и стандарди за спровођење мера и активности професионалне рехабилитације одређени су посебним *Правилником о ближим условима, критеријумима и стандардима за спровођење мера и активности професионалне рехабилитације, Сл. гласник РС, бр. 112/2009*. Послодавац може да сноси и трошкове процене радне способности и могућности запослења или одржања запослења запосленог лица у складу са чланом 17 *Правилника о ближем начину, трошковима и критеријумима за процену радне способности и могућности запослења или одржања запослења особа са инвалидитетом, Сл. гласник РС, бр. 36/2010, 97/2013.*

Закон о раду прописује и забрану дискриминације у области рада (Закон о раду, члан 18). Дискриминација у области рада забрањена је и посебним *Законом о забрани дискриминације, Сл. гласник РС, бр. 22/2009, 52/2021.* Под дискриминацијом сматра се нарушавање једнаких могућности за заснивање радног односа или уживање под једнаким условима свих права у области рада. Заштиту од дискриминације ужива лице у радном односу или било које друго лице које по било ком основу учествује у раду (Закон о забрани дискриминације, члан 16). Закон предвиђа обавезу послодавца да предузму одговарајуће мере ако је то потребно у конкретном случају у циљу обезбеђивања приступа, разумно прилагођеног радног места, учешћа, стручног усавршавања и напредовања у послу запослених који се налазе у неравноправном положају у односу на друге запослене, а нарочито особа са инвалидитетом, припадника националних мањина, жена, мушкараца, особа другачије сексуалне оријентације, родног идентитета, старијих особа и других, осим ако би ове мере представљале несразмеран терет за послодавца (Закон о забрани дискриминације, члан 14). Када је реч о дискриминацији особа са инвалидитетом, посебни *Закон о спречавању дискриминације особа са инвалидитетом, Сл. гласник РС, бр. 33/2006, 13/2016*, прописује одредбе које се односе на дискриминацију у вези са запошљавањем и радним односом ове категорије лица (чланови 21-26).

Посебно се уређује област забране дискриминације на основу пола, полних карактеристика, односно рода. *Законом о родној равноправности, Сл. гласник РС, бр. 52/2021*, регулисане су обавезе послодаваца у погледу интегрисања родне перспективе у области у којој делују (Закон о родној равноправности, члан 2). Послодавац је у обавези да одређује и спроводи посебне мере за остваривање и унапређивање родне равноправности (Закон о родној равноправности, члан 10). У свим областима у којима се спроводе ове мере, послодавац је дужан да прикупља и евидентира све информације и статистичке податке (Закон о родној равноправности, члан 65), који морају бити, осим збирно, разврстани и

исказани по полу и старосној доби (Закон о родној равноправности, члан 12). Послодавни су дужни да посебне мере пропишу у Плану и програму (Закон о родној равноправности, члан 16), да редовно извештавају надлежно Министарство о реализованим активностима из Акционог плана, као и о реализованим активностима из Плана и програма (Закон о родној равноправности, чланови 17 и 18, члан 66). Изглед образаца на којима послодавци евидентирају податке разврстане по полу, као и садржина и начин достављања извештаја о остваривању родне равноправности послодаваца ближе су прописани *Правилником о вођењу евиденције и извештавању о остваривању родне равноправности, Сл. гласник РС, бр. 67/2022*. Садржај и начин достављања плана мера за отклањање или ублажавање неравномерне заступљености полова и годишњег извештаја о његовом спровођењу ближе су прописани *Правилником о садржају и начину достављања Плана мера за отклањање или ублажавање неравномерне заступљености полова и годишњег извештаја о његовом спровођењу, Сл. гласник РС, бр. 89/2010.* Послодавац је дужан да запосленима, односно другим радно ангажованим лицима обезбеди једнаке могућности у вези са остваривањем права из радног односа и по основу рада (Закон о родној равноправности, члан 29), као и да пријави сваки вид насиља заснован на полу, односно роду и насиља према женама у приватној и јавној сфери (Закон о родној равноправности, члан 53). Закон прописује и забрањено поступање послодавца (Закон о родној равноправности, чланови 30-34). Посебне обавезе послодавца прописују се и за области образовања, васпитања, науке и технолошког развоја (Закон о родној равноправности, члан 37), одбране и безбедности (Закон о родној равноправности, члан 39).

Негативне појаве са којима се запослени могу суочити, а по којима послодавци морају реаговати јесу кршење прописа, кршење људских права, вршење јавног овлашћења противно сврси због које је поверено. Откривање, односно пријављивање ових појава према *Закону о заштити узбуњивача, Сл. гласник РС, бр. 128/2014,* назива се узбуњивање, а физичко лице или запослени који врши узбуњивање узбуњивач. У складу са законом, правно лице као послодавац дужно је да донесе општи акт о поступку унутрашњег узбуњивања и исти истакне на видном месту (Закон о заштити узбуњивача, члан 16), предузме мере ради отклањања утврђених неправилности, заштити узбуњивача и одреди лице овлашћено за пријем информације и вођење поступка у вези са узбуњивањем или (Закон о заштити узбуњивача, члан 14) и спроведе друге радње у складу са овим Законом (Закон о заштити узбуњивача, члан 15). Начин унутрашњег узбуњивања, начин одређивања овлашћеног лица код послодавца, као и друга питања од значаја за унутрашње узбуњивање код послодавца који има више од десет запослених уређена су посебним *Правилником о начину унутрашњег узбуњивања, начину одређивања овлашћеног лица код послодавца, као и другим питањима од значаја за унутрашње узбуњивање код послодавца који има више од десет запослених, Сл. гласник РС, бр. 49/2015, 44/2018*. Послодавац је дужан да запослене упозна како са забраном вршења злостављања, тако и са правима из Закона о заштити узбуњивача.

Од значаја је и *Закон о облигационим односима, Сл. гласник, бр. 29/1978, 39/1985, 45/1989, 57/1989, 31/1993, РС 18/2020,* посебно одредбе које се односе на одговорност предузећа и других правних лица према трећим лицима. За штету коју запослени у раду или у вези са радом проузрокује трећем лицу одговара предузеће (или друго правно лице) у коме је запослени радио у тренутку проузроковања штете, осим ако докаже да је запослени у датим околностима поступао онако како је требало (Закон о облигационим односима, чланови 140 и 141). Правно лице одговара за штету коју његов орган проузрокује трећем лицу у вршењу или у вези са вршењем својих функција (Закон о облигационим односима, члан 142).

Онда када правно лице у својству послодавца користи услуге агенција за запошљавање, онда је од значаја *Закон о агенцијском запошљавању, Сл. гласник РС, бр. 86/2019*. Да би се

услуге уступања на привремени рад послодавцу кориснику користиле, неопходно је закључивање уговора о уступању запослених између агенције за привремено запошљавање и послодавца (Закон о агенцијском запошљавању, члан 11 и повезани). Закон предвиђа обавезе послодавца који користи ову врсту услуга (Закон о агенцијском запошљавању, чланови 25 и 26) укључујући обавезе из области безбедности и здравља на раду (Закон о агенцијском запошљавању, члан 27), поступања у случају повреде на раду и професионалног обољења (Закон о агенцијском запошљавању, члан 28), вођења евиденције о уступљеним запосленима и обезбеђивање заштите личних података (Закон о агенцијском запошљавању, члан 29), гарантовање права рада (Закон о агенцијском запошљавању, члан 30), накнаде штете (Закон о агенцијском запошљавању, чланови 32 и 33).

Када правно лице организује волонтирање за опште добро, односно добро другог лица на пословима ван своје делатности, те не стиче добит обављањем волонтерских услуга и активности или волонтирање не замењује рад запослених и других радно ангажованих лица у правном лицу онда правно лице може да буде организатор волонтирања. Тада, правно лице поступа и према одредбама *Закона о волонтирању, Сл. гласник РС, бр. 36/2010*.

Како је правно лице у својству послодавца један од страна у колективном или индивидуалном радном спору, издваја се и *Закон о мирном решавању радних спорова, Сл. гласник РС, бр. 125/2004, 104/2009, 50/2018*.

Закон о штрајку, Сл. лист СРЈ, бр. 29/96 и Сл. гласник РС, бр. 101/2005, 103/2012, уређује питања из области организовања штрајка, као прекида рада који запослени организују ради заштите својих професионалних и економских интереса по основу рада (Закон о штрајку, члан 1). Према овом закону, правно лице у својству послодавца не сме да прими нова лица која би заменила учеснике у штрајку, када то закон не предвиђа или спречи запослене да учествују у штрајку или употреби мере принуде ради окончања штрајка или ако предвиди повољнију зараду или друге повољније услове рада за запослене који не учествују у штрајку (Закон о штрајку, члан 15). Посебно је значајна одредба која се односи на организовање штрајка у правним лицима која обављају делатност од јавног интереса (у области електропривреде, водопривреде, саобраћаја, информисања (радио и телевизија), ПТТ услуга, комуналних делатности, производње основних прехрамбених производа, здравствене и ветеринарске заштите, просвете, друштвене бриге о деци и социјалне заштите) или делатности чији би прекид рада због природе посла могао да угрози живот и здравље људи или да нанесе штету великих размера (Закон о штрајку, члан 9). Тада је обавеза послодавца да обезбеди минимум процеса рада утврђен општим актом или пропише тај минимум процеса рада (Закон о штрајку, члан 10).

Злостављање на раду још једна је од појава којој запослени може да буде изложен на свом радном месту или у вези са радом, која угрожава његова права. Злостављање као један од облика угрожавања у правном лицу, интересантан је са аспекта корпоративне безбедности у циљу откривања, истраге, санкционисања и на крају, елиминисања из радног окружења правног лица. У вези са тим, издваја се *Закон о спречавању злостављања на раду, Сл. гласник РС, бр. 36/2010* који јасно обавезује правно лице у својству послодавца да запосленог, пре ступања на рад, писменим путем обавести о забрани вршења злостављања и правима, обавезама и одговорностима запосленог и послодавца у вези са забраном злостављања, као и да у циљу препознавања, превенције и спречавања злостављања, спроводи мере обавештавања и оспособљавања запослених и њихових представника да препознају узроке, облике и последице вршења злостављања (Закон о спречавању злостављања на раду, члан 7). Уз то, послодавац је дужан да запосленог заштити од злостављања и одговара и надокнади штету проузроковану злостављањем (Закон о спречавању злостављања на раду, чланови 8 и 9).

Када дође до пријаве злостављања, послодавац поступа по пријави и тада он може да предложи посредовање као начин разрешења спорног односа (Закон о спречавању злостављања на раду, члан 15 и повезани), односно он предузима одређене мере за спречавање злостављања (Закон о спречавању злостављања на раду, чланови 23 и 24). Детаљније, правила понашања послодаваца у вези са превенцијом и заштитом од злостављања на раду укључујући и сексуално узнемиравање прописана су посебним *Правилником о правилима понашања послодаваца и запослених у вези са превенцијом и заштитом од злостављања на раду, Сл. гласник РС, бр. 62/2010*.

3.8.4. Безбедност и здравље на раду

Безбедност и здравље на раду представља неизоставну функцију корпоративне безбедности. Значај ове функције огледа се пре свега у спровођењу и унапређивању безбедности и здравља на раду, и то у сваком сегменту рада правног лица и у односу на свако лице које учествује у радним процесима, као и лице које се затекне у радној околини правног лица. Безбедност и здравље на раду треба да омогуће:

1) спровођење и унапређење безбедности и здравља на раду и
2) спречавање повреда на раду, професионалних обољења и обољења у вези са радом.

У области безбедности и здрављу на раду издвајају се у основи следећи нормативни акти:

- Закон о безбедности и здрављу на раду, Сл. гласник РС, бр. 35/2023
- Закон о заштити становништва од изложености дуванском диму, Сл. гласник РС, бр. 30/2010

Права, обавезе и одговорности послодаваца (државни органи, органи аутономних покрајина, органи јединица локалне самоуправе, привредна друштва, друга правна лица) у области безбедноста и здравља на раду остварују се у складу са *Законом о безбедности и здрављу на раду, Сл. гласник РС, бр. 35/2023,* и морају бити прописана и интерним актима - колективним уговором, правилником о безбедности и здрављу на раду или правилником о раду, односно уговором о раду (члан 3).

Послодавац је дужан да обезбеди и спроводи превентивне мере безбедности и здравља на раду, као и да запосленом обезбеди безбедност и здравље у свим активностима и на свим нивоима организовања рада и радног процеса (Закон о безбедности и здрављу на раду, члан 9). У вези са тим, послодавац је дужан да обезбеди да само они запослени којима су издата одговарајућа упутства и дозволе за рад имају приступ зонама повећаног ризика (Закон о безбедности и здрављу на раду, члан 10) и да у склопу превентивних мера обезбеди пружање информација и обуке запослених (Закон о безбедности и здрављу на раду, члан 12). Послодавац не сме да запосленом одреди да обавља послове на радном месту и у радној средини на којима нису спроведене мере безбедности и здравља на раду. То значи да је послодавац дужан да општим актом утврди права, обавезе и одговорности у области безбедности и здравља на раду (Закон о безбедности и здрављу на раду, члан 14); актом у писаној форми именује саветника, односно сарадника за безбедност и здравље на раду, донесе програм и не изврши обуку запосленог за безбедан и здрав рад, обезбеди коришћење личне заштитне опреме, обезбеди одржавање у исправном стању средстава за рад и личне заштитне опреме, обезбеди прописане лекарске прегледе запослених, обучи одговарајући број запослених за пружање прве помоћи и обезбеди пружање прве помоћи, заустави сваку врсту рада који представља озбиљну, неизбежну и непосредну опасност за живот или здравље запослених (Закон о безбедности и здрављу на раду, члан 15).

За сва радна места у радној средини, послодавац треба да донесе акт о процени ризика у писаној форми, обезбеди да мере утврђене овим актом буду интегрисане у све активности и на свим нивоима, измени акт о процени ризика када за то постоје разлози предвиђени законом (Закон о безбедности и здрављу на раду, члан 16); одреди посебне здравствене услове које морају испуњавати запослени на радним местима са повећаним ризиком (Закон о безбедности и здрављу на раду, члан 17); обавести све запослене о опасностима и штетностима (Закон о безбедности и здрављу на раду, чланови 15 и 19); упозори на опасности или штетности и видно обележи и истакне ознаке за безбедност и/или здравље на раду (Закон о безбедности и здрављу на раду, члан 37). Послодавац је дужан да извести надлежну инспекцију рада о почетку рада, раду одвојене јединице или свакој промени технолошког поступка, уколико се тим променама мењају услови рада (Закон о безбедности и здрављу на раду, члан 20) или кад запослени одбије да ради (Закон о безбедности и здрављу на раду, члан 39); пре отпочињања обављања одређене делатности добије решење о испуњености услова за почетак рада (Закон о безбедности и здрављу на раду, члан 21) и испуни обавезе које има према закону када изводи радове на градилишту, односно радилишту, хитне радове или под другим околностима (Закон о безбедности и здрављу на раду, чланови 22, 23, 24, 25 и 27). Послодавац је дужан да запосленом обезбеди средства и опрему за пружање прве помоћи (Закон о безбедности и здрављу на раду, члан 18); обезбеди личну заштитну опрему у исправном стању и спроведе обуку за њено правилно коришћење (Закон о безбедности и здрављу на раду, члан 28), као и да обезбеди упутство за њихову употребу и одржавање, као и упутства за безбедан рад по прописима о безбедности и здрављу на раду за употребу опреме за рад (Закон о безбедности и здрављу на раду, члан 29); изради и достави безбедносни лист под условима прописаним законом (Закон о безбедности и здрављу на раду, члан 30), сачини посебан програм о поступном отклањању недостатака који су утврђени актом о процени ризика, односно утврди рокове за реализацију програма (Закон о безбедности и здрављу на раду, члан 32). Послодавац је дужан да организује послове безбедности и здравља на раду, те да уреди обавезе и одговорности у вези са свакодневним праћењем и контролом примене мера безбедности и здравља на раду (Закон о безбедности и здрављу на раду, члан 46).

Послодавац је дужан да обезбеди под одређеним околностима претходни, односно периодични лекарски преглед, запосленог који није прошао преглед премести на друго радно место које одговара његовим здравственим способностима (Закон о безбедности и здрављу на раду, члан 56), као и да запослене осигура за случај повреда на раду и професионалних болести, ради обезбеђивања накнаде штете (Закон о безбедности и здрављу на раду, члан 67). Такође, он треба да организује додатну обуку за радно место где се догодила тешка, смртна или колективна повреда на раду, запосленог упозна о обављању радног процеса на безбедан начин, када радни процес захтева додатну обуку за безбедан и здрав рад или обавести о резултатима процене ризика одређене категорије запослених под условима када то предвиђа закон (Закон о безбедности и здрављу на раду, члан 36). Послодавац је дужан да под условима предвиђеним законом има саветника за безбедност и здравље на раду, односно сарадника за безбедност и здравље на раду који испуњава услове прописане овим законом, те му обезбеди континуирано усавршавање знања (Закон о безбедности и здрављу на раду, чланови 48, 49 и 53). Такође, он има одређене обавезе и према запосленима, представнику запослених и/или Одбору за безбедност и здравље на раду (Закон о безбедности и здрављу на раду, чланови 57-60), као и у вези вођења евиденција (Закон о безбедности и здрављу на раду, чланови 62 и 63). Послодавац је дужан да, у за то предвиђеном року, пријави надлежној инспекцији рада и надлежном органу за унутрашње послове сваку смртну, колективну или тешку повреду на раду, као и опасну појаву која би могла да угрози безбедност и здравље запослених, као и лаку повреду на раду због које запослени

није способан за рад више од три дана (Закон о безбедности и здрављу на раду, члан 64), достави извештај о повреди на раду и професионалној болести који се догоде на радном месту (Закон о безбедности и здрављу на раду, члан 65). Дужан је да поступи како закон одређује и приликом вршења надзора од стране инспектора (Закон о безбедности и здрављу на раду, чланови 94 и 95), отклони утврђене недостатке и неправилности чије отклањање је решењем наредио инспектор рада и о томе обавести надлежну инспекцију (Закон о безбедности и здрављу на раду, члан 99).

Подзаконска регулатива која је тренутно важећа, донета је на основу тренутно важећег Закона о безбедности и здрављу на раду , али и раније важећег Закона о безбедности и здрављу на раду. У вези са тим, у овој области неће се повезивати одредбе закона са подзаконским актима, већ ће бити наведени они чија је примена незаобилазна за регулисање организовања и функционисања безбедности и здрављу на раду у правном лицу. Реч је о следећим подзаконским актима: *Правилник о превентивним мерама за безбедан и здрав рад за спречавање појаве и ширења епидемије заразне болести, Сл. гласник РС, бр. 94/2020; Правилник о програму усавршавања знања и другим питањима у вези са усавршавањем знања лица за безбедност и здравље на раду, Сл. гласник РС, бр. 108/2017; Правилник о начину пружања прве помоћи, врсти средстава и опреме који морају бити обезбеђени на радном месту, начину и роковима оспособљавања запослених за пружање прве помоћи, Сл. гласник РС, бр. 109/2016; Правилник о превентивним мерама за безбедан и здрав рад при коришћењу опреме за рад, Сл. гласник РС, бр. 23/2009, 123/2012, 102/2015, 101/2018, 130/2021; Правилник о превентивним мерама за безбедан и здрав рад при коришћењу средстава и опреме за личну заштиту на раду, Сл. гласник РС, бр. 92/2008, 101/2018; Правилник о превентивним мерама за безбедан и здрав рад на радном месту, Сл. гласник РС, бр. 21/2009, 1/2019; Правилник о претходним и периодичним лекарским прегледима запослених на радним местима са повећаним ризиком, Сл. гласник РС, бр. 120/2007, 93/2008, 53/2017; Правилник о обезбеђивању ознака за безбедност и/или здравље на раду, Сл. гласник РС, бр. 95/2010, 108/2017; Правилник о начину вођења и роковима чувања евиденција у области безбедности и здравља на раду, Сл. гласник РС, бр. 5/2025; Правилник о садржају и начину издавања обрасца извештаја о повреди на раду и професионалном обољењу, Сл. гласник РС, бр. 72/2006, 84/2006, 4/2016, 106/2018, 14/2019; Правилник о начину и поступку процене ризика на радном месту и у радној средини, Сл. гласник РС, бр. 76/2024; Правилник о поступку утврђивања испуњености прописаних услова у области безбедности и здравља на раду, Сл. гласник РС, бр. 60/2006; Правилник о висини трошкова поступка утврђивања испуњености прописаних услова у области безбедности и здравља на раду, Сл. гласник РС, бр. 111/2013*. Овде се списак подзаконских аката у овој области не завршава, те је неопходно за ширу слику консултовати базе које обухватају све акте.

Правилницима су одређене и мере за безбедан и здрав рад запослене жене за време трудноће, породиље и запослене која дојди дете, рад младих, као и превентивне мере за безбедан и здрав рад при излагању вештачким оптичким зрачењима, буци, карциногенима или мутагенима, вибрацијама, биолошким штетностима, хемијским материјама, при ручном преношењу терета, при коришћењу опреме за рад са екраном.

Послодавац је у обавези да се придржава и одредаба по којем може, под условима предвиђеним законом, да одреди посебну просторију искључиво за пушење у којој се не може обављати делатност послодавца и на којој је обавезан да истакне знак да је пушење у тој просторији дозвољено (Закон о заштити становништва од изложености дуванском диму, члан 3). Ближи услови за истицање знака, као и друга питања од значаја за послодавца, прописана су *Правилником о облику и садржају знака забране пушења и знака да је пушење дозвољено у одређеном простору, начину истицања тих знакова, обрасцу извештаја о повреди забране пушења, врсти потребних доказа о пушењу и начину на који*

се они прикупљају и на који се утврђује присуство дуванског дима у простору у коме је пушење забрањено, као и о обрасцу за наплату новчане казне на лицу места, Сл. гласник РС, бр. 73/2010, 89/2017.

3.8.5. Заштита животне средине

Област заштите животне средине од изузетне је важности када се узму у обзир последице које су велике катастрофе оставиле на животну средину кроз историју. Одговарајући однос према окружењу и заштита животне средине представљају оно што је познато као одговорно понашање правног лица према свом ужем и ширем окружењу. Овом функцијом, корпоративна безбедност делује проактивно на могуће испољавање ризика из домена еколошких инцидената.

У области заштите животне средине издвајају се следећи нормативни акти:

- Закон о заштити животне средине, Сл. гласник РС, бр. 135/2004, 36/2009, 36/2009, 72/2009, 43/2011, 14/2016, 76/2018, 95/2018
  - Правилник о Листи опасних материја и њиховим количинама и критеријумима за одређивање врсте документа које израђује оператер севесо постројења, односно комплекса, Сл. гласник РС, бр. 41/2010-7, 51/2015-13, 50/2018
  - Правилник о садржини политике превенције удеса и садржини и методологији израде Извештаја о безбедности и Плана заштите од удеса, Сл. гласник РС, бр. 41/2010
  - Правилник о садржини обавештења о новом севесо постројењу односно комплексу, постојећем севесо постројењу, односно комплексу и о трајном престанку рада севесо постројења, односно комплекса, Сл. гласник РС, бр. 41/2010
  - Уредба о садржини и начину вођења информационог система заштите животне средине, методологији, структури, заједничким основама, категоријама и нивоима сакупљања података, као и о садржини информација о којима се редовно и обавезно обавештава јавност, Сл. гласник РС, бр. 112/2009
  - Правилник о методологији за израду националног и локалног регистра извора загађивања, као и методологији за врсте, начине и рокове прикупљања података, Сл. гласник РС, бр. 91/2010, 10/2013, 98/2016, 72/2023
- Закон о процени утицаја на животну средину, Сл. гласник РС, бр. 135/2004, 36/2009
- Закон о интегрисаном спречавању и контроли загађивања животне средине, Сл. гласник РС, бр. 135/2004, 25/2015, 109/2021
- Закон о заштити природе, Сл. гласник РС, бр. 36/2009, 88/2010, 91/2010, 14/2016, 95/2018, 71/2021
- Закон о заштити ваздуха, Сл. гласник РС, бр. 36/2009, 10/2013, 26/2021
- Закон о заштити од буке у животној средини, Сл. гласник РС, бр. 96/2021

Закон о заштити животне средине, Сл. гласник РС, бр. 135/2004, 36/2009, 36/2009, 72/2009, 43/2011, 14/2016, 76/2018, 95/2018 уређује интегрални систем заштите животне средине у којем су правна лица једна од категорија субјеката заштите. Реч је о правним лицима која у обављању привредне и друге делатности користе природне вредности, угрожавају или загађују животну средину (Закон о заштити животне средине, члан 4). Посебно, Закон се примењује на оператера (севесо постројења[92]) као правног лица које, у складу са прописима, управља постројењем или га контролише или је овлашћен за доношење економских одлука у области техничког функционисања постројења и на чије име се издаје интегрисана дозвола (Закон о заштити животне средине, члан 3). Закон

[92] Детаљан списак севесо постројења могуће је пронаћи у: МУП РС. (2019). *Процена ризика од катастрофа у Републици Србији*. Министарство унутрашњих послова Републике Србије, стр. 71-73.

одређује обавезе оператера у погледу поседовања потребне документације, а у зависности од количине опасних материја (Закон о заштити животне средине, члан 58). С тим у вези, од значаја је *Правилник о Листи опасних материја и њиховим количинама и критеријумима за одређивање врсте документа које израђује оператер севесо постројења, односно комплекса, Сл. гласник РС, бр. 41/2010, 51/2015, 50/2018.* Оператер се обавезује на доношење одређених докумената и то: Политике превенције удеса, Извештаја о безбедности, Плана заштите од удеса и одређених Обавештења (Закон о заштити животне средине, чланови 58а, 59, 60 и повезани). Садржина ових докумената одређена је посебним документима и то: *Правилником о садржини политике превенције удеса и садржини и методологији израде Извештаја о безбедности и Плана заштите од удеса, Сл. гласник РС, бр. 41/2010* и *Правилником о садржини обавештења о новом севесо постројењу односно комплексу, постојећем севесо постројењу, односно комплексу и о трајном престанку рада севесо постројења, односно комплекса, Сл. гласник РС, бр. 41/2010*. У случају удеса, оператер је дужан да о околностима везаним за хемијски удес, присутним опасним материјама, расположивим подацима за процену последица хемијског удеса за људе и животну средину и о предузетим хитним мерама одмах обавести надлежне одрган и предузме друге прописане мере (Закон о заштити животне средине, члан 60ј).

Закон предвиђа успостављање и вођење информационог система заштите животне средине (Закон о заштити животне средине, члан 74), у вези са чим су правна лица чије активности имају утицај на животну средину дужна да достављају релевантне податке и информације за систем. Ова обавеза потврђена је *Уредбом о садржини и начину вођења информационог система заштите животне средине, методологији, структури, заједничким основама, категоријама и нивоима сакупљања података, као и о садржини информација о којима се редовно и обавезно обавештава јавност, Сл. гласник РС, бр. 112/2009.* Исто тако, предвиђено је и вођење националних и локалних регистара извора загађивања животне средине (Закон о заштити животне средине, члан 75), у вези са чим правна лица која представљају изворе загађивања различитих делатности достављају податке. Ова обавеза потврђена је *Правилником о методологији за израду националног и локалног регистра извора загађивања, као и методологији за врсте, начине и рокове прикупљања података, Сл. гласник РС, бр. 91/2010, 10/2013, 98/2016, 72/2023.*

Закон о процени утицаја на животну средину, Сл. гласник РС, бр. 135/2004, 36/2009, примењује се на правна лица која намеравају да врше изградњу или реконструкцију објекта или друге интервенције у природи и природном окружењу, те као носиоци пројекта подносе захтев за добијање дозволе или одобрења (Закон о процени утицаја на животну средину, члан 2). У вези са проценом утицаја, вреди поменути и Процену утицаја пројеката на животну средину (Закон о заштити животне средине, члан 36). Процена утицаја врши се за пројекте из области индустрије, рударства, енергетике, саобраћаја, туризма, пољопривреде, шумарства, водопривреде, управљања отпадом и комуналних делатности, као и за пројекте који се планирају на заштићеном природном добру и у заштићеној околини непокретног културног добра. Све од наведеног представља критичну инфраструктуру, док је добар део наведених области од критичног значаја за функционисање државе.

Додатно, *Закон о интегрисаном спречавању и контроли загађивања животне средине, Сл. гласник РС, бр. 135/2004, 25/2015, 109/2021*, прописује обавезе које правно лице – оператер има у области спречавања и контроле загађивања животне средине (Закон о интегрисаном спречавању и контроли загађивања животне средине, чланови 8 и 17), као и привредне прекршаје и преступе (Закон о интегрисаном спречавању и контроли загађивања животне средине, чланови 29 и 30).

Закон о заштити природе, Сл. гласник РС, бр. 36/2009, 88/2010, 91/2010, 14/2016, 95/2018, 71/2021, примењује се на правна лица која у обављању привредних и других делатности користе природне ресурсе и заштићена природна добра. Уједно ова група лица спада у субјекте заштите природе (Закон о заштити природе, члан 6), те се као таква морају придржавати одредби Закона.

Закон о заштити ваздуха, Сл. гласник РС, бр. 36/2009, 10/2013, 26/2021, примењује се на правна лица која у обављању делатности утичу или могу утицати на квалитет ваздуха и која су дужна да: обезбеде техничке мере за спречавање или смањивање емисија у ваздух, планирају трошкове заштите ваздуха од загађивања у оквиру инвестиционих и производних трошкова, прате утицај своје делатности на квалитет ваздуха и обезбеде друге мере заштите (Закон о заштити ваздуха, члан 4). Закон предвиђа да у циљу предузимања мера за смањење загађења ваздуха, примене одређених техничко-технолошких решења и планирања трошкова смањења емисија оператери донесу План оператера за смањење емисија из стационарних постројења (Закон о заштити ваздуха, чланови 26 и 39). Оператери су дужни да извршавају обавезе (Закон о заштити ваздуха, члан 58) у складу са Законом укључујући спровођење мера превенције и санације (Закон о заштити ваздуха, члан 55). Благовремено и без накнаде дужни су да достављају податке из своје надлежности, као и друге податке који су потребни за вођење информационог система о квалитету ваздуха Агенцији у циљу израде планова и извештаја (Закон о заштити ваздуха, члан 68). Дужни су да омогуће поступак инспекцијског надзора (Закон о заштити ваздуха, члан 77). Закон прописује и казне за привредне прекршаје и преступе из ове области (Закон о заштити ваздуха, чланови 79 и 81).

Закон о заштити од буке у животној средини, Сл. гласник РС, бр. 96/2021, примењује се на правна лица која у обављању привредне делатности емитују буку и друга правна лица (Закон о заштити од буке у животној средини, члан 5). Прва група лица усваја стратешке карте буке и доставља надлежном органу јединице локалне самоуправе и Агенцији за заштиту животне средине (Закон о заштити од буке у животној средини, члан 21). Друга друга лица одговорна је за сваку активност којом се проузрокује изложеност буци изнад граничних вредности, те су у том случају дужна да обезбеде: учешће у трошковима заштите од буке у животној средини у оквиру инвестиционих, текућих и производних трошкова, праћење утицаја своје делатности на буку и спровођење одговарајућих мера заштите од буке, односно звучне заштите (Закон о заштити од буке у животној средини, члан 10), укључујући утврђивање испуњености услова и мера заштите (Закон о заштити од буке у животној средини, члан 18). Правна лица одговорна су и за непредузимање прописаних мера заштите од буке у животној средини (Закон о заштити од буке у животној средини, члан 36).

Поред наведених законских аката, правна лица су дужна да се у обављању своје делатности придржавају и *Закона о водама, Сл. гласник РС, бр. 30/2010, 93/2012, 101/2016, 95/2018, 95/2018; Закона о шумама, Сл. гласник РС, бр. 30/2010, 93/2012, 89/2015, 95/2018; Закона о заштити земљишта, Сл. гласник РС, бр. 112/2015; Закона о радијационој и нуклеарној сигурности и безбедности; Сл. гласник РС, бр. 95/2018, 10/2019, Закона о заштити од нејонизујућих зрачења, Сл. гласник РС, бр. 36/2009; Закона о хемикалијама, Сл. гласник РС, бр. 36/2009, 88/2010, 92/2011, 93/2012, 25/2015; Закона о управљању отпадом, Сл. гласник РС, бр. 36/2009, 88/2010, 14/2016, 95/2018, 35/2023* и других закона са подзаконским актима донетим у области заштите животне средине.

3.8.6. Управљање ризиком од катастрофа и ванредним ситуацијама

Функција управљања ризиком од катастрофа и ванредним ситуацијама веома је блиска функцији заштите животне средине, у тој мери да ју је могуће и подвести под њу. Ипак, на овом месту ће се разматрати као засебна функција корпоративне безбедности. Ова функција се превасходно односи на обавезе и одговорности правног лица у односу на

смањење ризика и управљање ризиком од катастрофа и управљање ванредним ситуацијама када исте буду проглашене од стране надлежног органа.

У области управљања ризиком од катастрофа и ванредним ситуацијама издвајају се следећи нормативни акти:

- Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, Сл. гласник РС, бр. 87/2018
- Упутство о Методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања, Сл. гласник РС, бр. 80/2019
- Уредба о садржају, начину израде и обавезама субјеката у вези са израдом процене ризика од катастрофа и планова заштите и спасавања, Сл. гласник РС, бр. 102/2020
- Правилник о начину израде и садржају Плана заштите од удеса, Сл. гласник РС, бр. 41/2019
- Правилник о врсти и количини опасних супстанци на основу којих се сачињава План заштите од удеса, Сл. гласник РС, бр. 34/2019
- Правилник о садржини, начину успостављања и одржавања регистра ризика од катастрофа, Сл. гласник РС, бр. 78/2019
- Уредба о обавезама субјеката система смањења ризика од катастрофа и управљања ванредним ситуацијама у поступку израде Регистра ризика од катастрофа, начину израде Регистра ризика од катастрофа и уносу података, Сл. гласник РС, бр. 122/2020
- Одлука о одређивању субјеката од посебног значаја за заштиту и спасавање у Републици Србији, Сл. гласник РС, бр. 69/2019
- Уредба о обавезним средствима и опреми за личну, узајамну и колективну заштиту од елементарних непогода и других несрећа, Сл. гласник РС, бр. 3/2011, 37/2015
- Правилник о садржају и начину вођења евиденције о припадницима органа, јединица, служби и другим учесницима и о средствима и опреми у цивилној заштити, Сл. гласник РС, бр. 91/2013

У области ванредних ситуација, као кровни закон издваја се *Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, Сл. гласник РС, бр. 87/2018*. Органи државне управе, органи аутономне покрајине и јединице локалне самоуправе, јавне службе, привредна друштва и друга правна лица чија је делатност од значаја за смањење ризика и управљање ванредним ситуацијама одређени су као субјекти система смањења ризика од катастрофа и управљања ванредним ситуацијама (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 13).

Закон предвиђа за одређене субјекте израду посебних аката у овој области и то Процену ризика, планове и Регистар ризика од катастрофа (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, чланови 15-22). Процена ризика од катастрофа, као и план заштите и спасавања израђују се према *Упутству о Методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања, Сл. гласник РС, бр. 80/2019* и *Уредби о садржају, начину израде и обавезама субјеката у вези са израдом процене ризика од катастрофа и планова заштите и спасавања, Сл. гласник РС, бр. 102/2020.* Република Србија, аутономна покрајина, јединица локалне самоуправе, субјекти од посебног значаја за заштиту и спасавање и привредна друштва и друга правна лица која испуњавају услове прописане Законом, дужна су да имају Процену ризика од катастрофа (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 15). Сви субјекти који имају обавезу израде процене ризика од катастрофа дужни су да имају и План заштите и спасавања (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 17). Сва наведена документа израђују сва привредна друштва,

односно друга правна лица која имају овлашћење за израду тих докумената (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, чланови 19-20).

У вези са наведеним, донети су *Правилник о начину израде и садржају Плана заштите од удеса, Сл. гласник РС, бр. 41/2019* и *Правилник о врсти и количини опасних супстанци на основу којих се сачињава План заштите од удеса, Сл. гласник РС, бр. 34/2019*. План заштите од удеса дужна су да имају привредна друштва и друга правна лица која обављају активности у којима је присутна или може бити присутна једна или више опасних супстанци у прописаним количинама (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, чланови 64-66). На основу Плана заштите од удеса и службених евиденција води се Регистар привредних друштава и правних лица која рукују опасним супстанцама (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 67). Начин вођења овог регистра уређен је посебним *Правилником, Сл. гласник РС, бр. 34/2019*. Сва правна лица која су уједно и субјекти система смањења ризика од катастрофа и управљања ванредним ситуацијама дужни су да Министарству достављају ажурне податке потребне за израду Регистра ризика (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 22). Одредба је потврђена и *Правилником о садржини, начину успостављања и одржавања регистра ризика од катастрофа, Сл. гласник РС, бр. 78/2019*, члан 9. Обавезе ових субјеката према овом регистру прописане су *Уредбом о обавезама субјеката система смањења ризика од катастрофа и управљања ванредним ситуацијама у поступку израде Регистра ризика од катастрофа, начину израде Регистра ризика од катастрофа и уносу података, Сл. гласник РС, бр. 122/2020.*

Значајна одредба Закона односи се на субјекте од посебног значаја за заштиту и спасавање које представљају привредна друштва и друга правна лица која се баве делатношћу из области: телекомуникација, рударства и енергетике, транспорта, метеорологије, хидрологије, сеизмологије, заштите од јонизујућег зрачења и нуклеарне сигурности, заштите животне средине, водопривреде, шумарства и пољопривреде, здравства, збрињавања лица, ветерине, комуналне делатности, грађевинарства, угоститељства, и други који располажу ресурсима за смањење ризика од катастрофа (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 31). Конкретније, ова привредна друштва и друга правна лица ближе су одређена *Одлуком о одређивању субјеката од посебног значаја за заштиту и спасавање у Републици Србији, Сл. гласник РС, бр. 69/2019.* Субјекти од посебног значаја имају и посебне обавезе у складу са Законом. Иначе, свако привредно друштво и друго правно лице дужно је да, у оквиру своје делатности предузима све мере превенције и смањења ризика, као и да се одазове захтеву надлежног штаба и узме учешће у спровођењу мера заштите и спасавања, и даје податке који се траже (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 30). Државни органи, органи аутономне покрајине и органи јединице локалне самоуправе, привредна друштва и друга правна лица обезбеђују и држе у исправном стању потребна средства и опрему за личну и узајамну заштиту и врше обуку запослених (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 55). У вези са овим средствима и опреми тренутно су на снази одредбе *Уредбе о обавезним средствима и опреми за личну, узајамну и колективну заштиту од елементарних непогода и других несрећа, Сл. гласник РС, бр. 3/2011, 37/2015.*

Закон предвиђа посебне обавезе за субјекте из одређених грана делатности (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 32), као и за субјекте – електропривредна, водопривредна и друга привредна друштва која користе хидроакумулације створене изградњом високих брана, депонија јаловине и пепелишта, привредна друштва и друга правна лица која врше производњу, складиштење и промет опасних материја (Закон о смањењу ризика од катастрофа и управљању ванредним

ситуацијама, члан 97), као и радио-дифузне и телевизијске станице и оператери мобилне телефоније (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, чланови 98 и 100). Поред одредби Закона које се односе на евиденције (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, чланови 105-110) усвојен је и *Правилник о садржају и начину вођења евиденције о припадницима органа, јединица, служби и другим учесницима и о средствима и опреми у цивилној заштити, Сл. гласник РС, бр. 91/2013,* посебно чланови 4 и 9.

3.8.7. Заштита од пожара

Заштита од пожара као функција корпоративне безбедности делује у два правца: проактивно у циљу елиминисања услова за настанак пожара и реактивно у циљу смањења и елиминације последица када до пожара дође. Заштита од пожара један је од услова заштите људских живота, имовине и животне средине. Попут претходно објашњених функција корпоративне безбедности, и ова област је законски веома добро уређена. У области заштите од пожара издвајају се следећи нормативни акти:

- Закон о заштити од пожара, Сл. гласник РС, бр. 111/2009, 20/2015, 87/2018, 87/2018, 87/2018
  - Уредба о разврставању објекта, делатности и земљишта у категорије угрожености од пожара, Сл. гласник РС, бр. 76/2010
  - Правилник о организовању заштите од пожара према категорији угрожености од пожара, Сл. гласник РС, бр. 6/2021
  - Правилник о начину израде и садржају Плана заштите од пожара аутономне покрајине, јединице локалне самоуправе и субјеката разврстаних у прву и другу категорију, Сл. гласник РС, бр. 73/2010
- Закон о запаљивим и горивим течностима и запаљивим гасовима, Сл. гласник РС, бр. 54/2015
- Закон о планирању и изградњи, Сл. гласник РС, бр. 72/2009, 81/2009, 64/2010, 24/2011, 121/2012, 42/2013, 50/2013, 98/2013, 132/2014, 145/2014, 83/2018, 31/2019, 37/2019, 9/2020, 52/2021, 62/2023

Закон о заштити од пожара, Сл. гласник РС, бр. 111/2009, 20/2015, 87/2018, 87/2018, 87/2018, уређује обавезе правних лица у области заштите од пожара, као једних од субјеката система заштите од пожара (Закон о заштити од пожара, члан 3). Она су дужна да да примењују мере заштите од пожара и експлозија, да обезбеде примену планова заштите од пожара и других аката и одговорни су за сваку активност којом мењају или могу променити стање и услове заштите од пожара, као и да ангажовањем расположивих људских и материјалних ресурса учествују у гашењу пожара и спасавању људи и имовине угрожених пожаром, ако то могу да учине без опасности за себе или другога (Закон о заштити од пожара, члан 6).

Како правна лица располажу различитим објектима, значајна одредба Закона односи се на категоризацију објеката према угрожености (Закон о заштити од пожара, чланови 23 и 24). У вези са наведеним, издваја се *Уредба о разврставању објекта, делатности и земљишта у категорије угрожености од пожара, Сл. гласник РС, бр. 76/2010* и посебно члан 9 Уредбе који се односи на обавезу правних лица. За субјекте разврстане у прву и другу категорију угрожености од пожара од значаја су *Правилник о организовању заштите од пожара према категорији угрожености од пожара, Сл. гласник РС, бр. 6/2021* и *Правилник о начину израде и садржају Плана заштите од пожара аутономне покрајине, јединице локалне самоуправе и субјеката разврстаних у прву и другу категорију, Сл. гласник РС, бр. 73/2010.* Поред Плана заштите од пожара, субјекти у првој и другој

категорији угрожености од пожара морају имати и План евакуације и упутства за поступање у случају пожара (Закон о заштити од пожара, члан 27а). Одређена правна лица из ових категорија, као и субјекти у трећој категорији доносе Правила заштите од пожара (Закон о заштити од пожара, члан 28). Од посебног су значаја одредбе Закона које се односе на обуку запослених у области заштите од пожара. Запослени су дужни да присуствују обуци и провери знања из области заштите од пожара и да се у раду придржавају прописаних упутстава, упозорења, забрана, мера заштите од пожара, као и да у случају пожара приступе гашењу пожара (Закон о заштити од пожара, члан 54).

Сва правна лица дужна су да поред поседовања прописане документације и области заштите од пожара, одржавају у исправном и функционалном стању и обезбеде контролисање инсталација и уређаја за аутоматско откривање и дојаву пожара, гашење пожара, детекцију експлозивних и запаљивих гасова, инсталација у зонама опасности од експлозије, инсталација за одвођење дима и топлоте, инсталација хидрантске мреже за гашење пожара, као и мобилних уређаја за гашење пожара (Закон о заштити од пожара, чланови 43 и 44). Правно лице мора водити рачуна о смештају запаљивог материјала и то на удаљености од најмање најмање 6 m од објекта или дела објекта, ако техничким прописима није другачије одређено (Закон о заштити од пожара, члан 48). За одређене врсте инсталација или објеката, делатност која се у објекту обавља и опасност од пожара и експлозија за људе и имовину, донети су правилници о техничким нормативима за заштиту од пожара и то: стамбених и пословних објеката и објеката јавне намене, угоститељских објеката, индустријских објеката, високих објеката, спољних зидова зграда, инсталације хидрантске мреже за гашење пожара, као и техничким нормативима за стабилне инсталације за детекцију експлозивних гасова и пара, за стабилне инсталације за дојаву пожара, за уређаје за аутоматско затварање врата или клапни отпорних према пожару, за системе за вентилацију или климатизацију (Закон о заштити од пожара, члан 44а).

Повезан са матичним Законом у области заштите од пожара јесте *Закон о запаљивим и горивим течностима и запаљивим гасовима, Сл. гласник РС, бр. 54/2015*. Закон се примењује на сва правна лица која рукују или користе запаљиве и горива течности и запаљиве гасове, као и обављају послове складиштења, држања и промета запаљивих и горивих течности или запаљивих гасова. Прописани су услови у погледу примене мера заштите од пожара и експлозија приликом постављања, изградње, реконструкције, доградње и санације (Закон о запаљивим и горивим течностима и запаљивим гасовима, глава 2) и приликом коришћења постројења и објеката за производњу, прераду, дораду, претакање, складиштење, држање и промет запаљивих и горивих течности и запаљивих гасова, ради спречавања настајања и ширења пожара и експлозија и гашења пожара (Закон о запаљивим и горивим течностима и запаљивим гасовима, глава 3).

У контексту уређивања и коришћења грађевинског земљишта и изградњи објеката чему правна лица могу да приступе, а у вези је са наведеним законима у области заштите животне средине, заштити од пожара или чак безбедности и здрављу на раду издваја се *Закон о планирању и изградњи, Сл. гласник РС, бр. 72/2009, 81/2009, 64/2010, 24/2011, 121/2012, 42/2013, 50/2013, 98/2013, 132/2014, 145/2014, 83/2018, 31/2019, 37/2019, 9/2020, 52/2021, 62/2023.*

3.8.8. Остали нормативни прописи од значаја за безбедност и функционисање организације

Поред свих закона и подзаконских аката који су наведени у тексту који је претходио, постоје закони који нису директно повезани са функцијама корпоративне безбедности,

али имају утицаја и значајни су за функционисање организације и заштиту њених вредности. Реч је о следећим законима:

- Закон о привредним друштвима, Сл. гласник РС, бр. 36/2011, 99/2011, 83/2014, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021, 19/2025
- Закон о јавним предузећима, Сл. гласник РС, бр. 15/2016, 88/2019
- Закон о јавним набавкама, Сл. гласник РС, бр. 91/2019, 92/2023
- Закон о јавно-приватном партнерству и концесијама, Сл. гласник РС, бр. 88/2011, 15/2016, 104/16
- Закон о заштити конкуренције, Сл. гласник РС, бр. 51/2009, 95/2013
- Закон о општем управном поступку, Сл. гласник РС, бр. 18/2016, 95/2018, 2/2023
- Кривични законик, Сл. гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019
- Закон о одговорности правних лица за кривична дела, Сл. гласник РС, бр. 97/2008
- Законик о кривичном поступку, Сл. гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021, 62/2021
- Закон о прекршајима, Сл. гласник РС, бр. 65/2013, 13/2016, 98/2016, 91/2019
- Закон о привредним преступима, Сл. гласник, бр. 4/1977, 36/1977, 14/1985, 10/1986-, 74/1987, 57/1989, 3/1990, СРЈ 27/1992, 16/1993, 31/1993, 41/1993, 50/1993, 24/1994, 28/1996, 64/2001, РС 101/2005

Закон о привредним друштвима, Сл. гласник РС, бр. 36/2011, 99/2011, 83/2014, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021, 19/2025 уређује правни положај привредних друштава а нарочито њихово оснивање, управљање, статусне промене, промене правне форме, престанак и друга питања од значаја за њихов положај.

Закон о јавним предузећима, Сл. гласник РС, бр. 15/2016, 88/2019 уређује правни положај – оснивање, пословање, управљање, имовину, јавних предузећа и других облика организовања који обављају делатност од општег интереса. Реч је о делатностима у области: рударства и енергетике, саобраћаја, електронских комуникација, издавања службеног гласила Републике Србије и издавања уџбеника, нуклеарних објеката, наоружања и војне опреме, коришћења, управљања, заштите, уређивања и унапређивања добара од општег интереса и добара у општој употреби (воде, путеви, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја и др.), управљања отпадом. Наведене делатности највећим делом обухватају области од критичне важности за функционисање државе и друштва, што даје на снази овом пропису.

За пословање одређених правних лица, у зависности од делатности, од значаја су и закони који би могли да се подведу под област економске заштите правног лица. У том контексту, од значаја је *Закон о јавним набавкама, Сл. гласник РС, бр. 91/2019, 92/2023*. Правно лице се појављује као наручилац јавне набавке без обзира да ли је реч о јавном наручиоцу или секторском наручиоцу (Закон о јавним набавкама, чланови 2-4). Овим Законом се уређују правила поступака јавних набавки које спроводе наручиоци, а ради закључења уговора о јавној набавци добара, услуга или радова или оквирног споразума. Наручилац у складу са овим Законом дужан је да спроводи поступак јавних набавки када набавља добра, услуге или радове, осим када Законом није другачије одређено (Закон о јавним набавкама, члан 51). О томе је дужан да закључи уговор (Закон о јавним набавкама, члан 151), да извршава обавезе које произилазе из уговора (Закон о јавним набавкама, члан 154) и врши измене закљученог уговора само на начин прописан Законом (Закон о јавним набавкама, чланови 155-161). Дужан је да се придржава начела јавне набавке (Закон о јавним набавкама, чланови 5-10), одређује предмет јавне набавке (Закон о јавним набавкама, чланови 29-35), поштује рокове за подношење понуда или

пријава за све врсте поступака (Закон о јавним набавкама, чланови 52-63), спроводи припрему за спровођење поступка јавне набавке, односно донесе годишњи план јавних набавки (Закон о јавним набавкама, члан 88), обезбеди заштиту интегритета поступка (Закон о јавним набавкама, члан 90), образује комисију за јавну набавку под одређеним условима (Закон о јавним набавкама, члан 92), објављује огласе о јавној набавци (Закон о јавним набавкама, члан 105). Када постоји неки од прописаних основа за искључење неког привредног субјекта из поступка јавне набавке, наручилац је дужан да то и уради (Закон о јавним набавкама, члан 111 и повезани). Наручилац је дужан да пре доношења одлуке у поступку јавне набавке утврди доказе о испуњености критеријума за квалитативни избор привредног субјекта (Закон о јавним набавкама, чланови 119 и повезани, 125). Након пријема и отварања понуда, врши се преглед, стручна оцена и рангирање понуда на основу услова и захтева из документације о набавци и сачињава извештај о поступку јавне набавке, као и доносе одређене одлуке у складу са одредбама Закона (Закон о јавним набавкама, чланови 139-148). Наручилац је дужан да у прописаном року достави тражене податке и обавештења који су од значаја за спровођења мониторинга Канцеларији за јавне набавке (Закон о јавним набавкама, члан 180), да евидентира податке о вредности и врсти јавних набавки, у прописаном року исте објави на Порталу јавних набавки, достави податке о појединачном поступку јавне набавке или закљученом уговору Канцеларији за јавне набавке (Закон о јавним набавкама, чланови 152а и 181), поступи у складу са одлуком Републичке комисије (Закон о јавним набавкама, члан 226), достави извештај о спровођењу одлуке Републичке комисије (Закон о јавним набавкама, члан 230). Значај Закона огледа се и у одредбама које прописују Предмет јавне набавке у области одбране и безбедности (Закон о јавним набавкама, члан 164), као и у секторским делатностима: гас и топлотна енергија, електрична енергија, водопривреда, услуге превоза, луке и аеродроми, поштанске услуге, вађење нафте и гаса и истраживање или вађење угља или других чврстих горива (Закон о јавним набавкама, чланови 165-172) које су од критичног значаја за функционисање државе. На основу спроведеног истраживања, као велики недостатак Закона подвлачи се учестала пракса да се приликом избора најчешће примењује критеријум „најниже понуђене цене". Тада се изабере „најјефтинији" понуђач, док је квалитет услуге упитан, јер ниска цена понуде никако не гарантује квалитет те понуде.[93]

Закон о јавно-приватном партнерству и концесијама, Сл. гласник РС, бр. 88/2011, 15/2016, 104/2016 издваја се на овом месту претежно у областима права и обавеза јавних и приватних партнера и заштите права учесника у поступцима доделе јавних уговора. Посебно се издваја и члан 11, односно одредба која предвиђа да предмет концесије могу бити добра у областима попут енергетике, транспорта и здравства које су одређене као области од посебног значаја (критичне инфраструктуре).

Закон о заштити конкуренције, Сл. гласник РС, бр. 51/2009, 95/2013 примењује се на правна лица која непосредно или посредно, стално, повремено или једнократно учествују у промету робе, односно услуга, независно од њиховог правног статуса, облика својине или држављанства, односно државне припадности. Реч је о следећим правним лицима: домаћа и страна привредна друштва и предузетници; државни органи, органи територијалне аутономије и локалне самоуправе; друга правна лица и облици удруживања учесника на тржишту (синдикати, удружења, спортске организације, установе, задруге, носиоци права интелектуалне својине и др.), као и јавна предузећа, привредна друштва, предузетнике и друге учеснике на тржишту, који

[93] Више о овом проблему видети у: Transparentnost Srbija i Centar za primenjene evropske studije. (2022). *GLAVNI PROBLEMI JAVNIH NABAVKI U SRBIJI: U kontekstu novih zakonskih rešenja i evropskih integracija*. Beograd: Transparentnost Srbija i Centar za primenjene evropske studije.

обављају делатности од општег интереса, односно којима је актом надлежног државног органа додељен фискални монопол.

Закон о општем управном поступку, Сл. гласник РС, бр. 18/2016, 95/2018, 2/2023 примењује се на државне органе и организације, органе и организације покрајинске аутономије и органе и организације јединица локалне самоуправе, установе, јавна предузећа, посебне органе преко којих се остварује регулаторна функција и правна лица којима су поверена јавна овлашћења када поступају у управним стварима.

Кривични законик, Сл. гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 издваја се јер регулише област кривичних дела чије је разумевање од значаја за корпоративну безбедност, посебно у делу заштите правног лица од извршења кривичних дела која могу да угрозе било које вредности правног лица. Одговорност правних лица за кривична дела, као и санкције правних лица за кривична дела уређују се посебним законом. Реч је о *Закону о одговорности правних лица за кривична дела, Сл. гласник РС, бр. 97/2008.* Овај закон уређује услове одговорности правних лица за кривична дела (кривична дела из посебног дела Кривичног законика и других закона), кривичне санкције које се могу изрећи правним лицима и правила поступка у којем се одлучује о одговорности правних лица, изрицању кривичних санкција, доношењу одлуке о рехабилитацији, престанку мере безбедности или правне последице осуде и извршењу судских одлука.

У складу са чланом 298 *Законика о кривичном поступку, Сл. гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021, 62/2021,* правно лице је дужно да на захтев јавног тужиоца пружи помоћ за предузимање доказне радње која не трпи одлагање.

Закон о прекршајима, Сл. гласник РС, бр. 65/2013, 13/2016, 98/2016, 91/2019 прописује одговорност за прекршај за правно лице (члан 27) и одговорно лице у правном лицу (члан 29). *Закон о привредним преступима, Сл. гласник, бр. 4/1977, 36/1977, 14/1985, 10/1986-, 74/1987, 57/1989, 3/1990, СРЈ 27/1992, 16/1993, 31/1993, 41/1993, 50/1993, 24/1994, 28/1996, 64/2001, РС 101/2005* прописује одговорност за привредни преступ за правно лице и одговорно лице у правном лицу.

Ово поглавље требало је да послужи за систематичан приказ нормативних аката који директно или индиректно постављају основу за успостављање и функционисање корпоративне безбедности. У случају да правно лице обавља делатност која је посебним законима уређена, онда је потребно узети у разматрање и законе којима је та делатност уређена, те их применити са аспекта корпоративне безбедности. Небавећи се детаљном анализом наведених закона и подзаконских аката (правилници, уредбе и одредбе, одлуке) циљ је био указати на нормативни оквир који омогућава и усмерава законитост у раду корпоративне безбедности са једне стране, и израду интерних аката правног лица из области корпоративне безбедности, са друге стране.

Поред нормативног оквира који је дат на овом месту, детаљнија анализа би требало да обухвати и велики број директива Европске Уније и важећих домаћих (СРПС) и међународних стандарда. Тада би приказ правног оквира организовања и функционисања корпоративне безбедности био обухватнији и потпунији.

4. КРИТИЧНА ИНФРАСТРУКТУРА И ЊЕНА ЗАШТИТА

„Суштински можемо имати два основна разога због чега обрађујемо тему критичне инфраструктуре, први би био функционално-економски, а други безбједносни“
(Damjanović i Ristić, 2022, str. 171).

Једно од кључних питања функционисања државе, њене заштите и њене националне безбедности јесте критична инфраструктура. Данас је критична инфраструктура општи појам који се односи на збир мрежа и система које је направио човек и који пружа добра и услуге јавности, па се као такав третира као кључни за безбедност државе и њених грађана. Свет који је постао индустријализованији, развијенији и глобализованији понудио је са једне стране бољу заштиту критичне инфраструктуре, док ју је са друге стране учинио подложном бројним поремећајима од природних катастрофа, преко криза попут ратова и немира, па све до тероризма који намерно циља инфраструктуру у циљу повреде, ометања и застрашивања грађана. У ери након 11. септембра, забринутост од терористичких напада је појачана. Појачани су и напори у заштити критичне инфраструктуре као оне индустрије за које би очекивани људски и економски губици били највећи (Farmer et al., 2004, p. 2). Зато, добар део, ако не и целокупна безбедност и економија једне државе заснивају се на способности државе да надгледа и штити критичну инфраструктуру, односно брзо санира последице и обезбеди континуирано функционисање и пружање услуга. Временом, држава је престала да буде једина одговорна за заштиту критичне инфраструктуре. Приватизација и глобализација створиле су нешто другачији систем заштите критичне инфраструктуре у којем одговорности за заштиту сада деле јавни и приватни сектор безбедности, како држава са својим органима и службама, тако и специјализовани субјекти приватне безбедности. Заправо, целокупан приватни сектор (неограничавајући се на безбедносни део) једна је од кључних карика у заштити безбедности од низа претњи.

Све инфраструктуре категоризоване као критичне од посебног су интереса за државу и њено друштво. Не би било погрешно рећи да је реч о темељу сваке државе, јер њихово нефункционисање или ограничено функционисање може створити озбиљне проблеме по могућност државе да задовољи све своје функције и потребе. Критична инфраструктура данас је важан сегмент националне безбедности, а њена заштита је сврстана међу приоритете сваке државе и приоритетно питање националне безбедности. Како је велики део (националне) критичне инфраструктуре у власништву организација (корпорација) приватног сектора, намеће се неискључива потреба да и ови субјекти буду ангажовани у заштити критичне инфраструктуре. Из наведеног проистиче да су организације (корпорације) неизоставни субјекат заштите критичне инфраструктуре и тиме националне безбедности. Уз то, услед комплексности савремених претњи, као и недостатка ресурса, држава више није у могућности да заштиту обезбеди сама. Тада на сцену ступају приватни субјекти безбедности и са њима корпоративна безбедност.

Држава има кључну улогу у систему заштите критичне инфраструктуре. По правилу, један од највећих интереса државе јесте да обезбеди несметано функционисање критичне инфраструктуре и тиме несметано функционисање заједнице, и то без обзира на власничку структуру критичног инфраструктурног објекта или система. Како је немогуће развити функционални систем заштите критичне инфраструктуре ако заинтересовани субјекти нису свесни његове критичности за виталне друштвене функције, тако је неопходно подизање свести и правилно разумевање значаја критичне инфраструктуре у оквиру стратешког управљања државом и њеним институцијама (RECIPE, 2015, p. 7).

Могуће је извести закључак да је део критичне инфраструктуре у државном власништву, а део у приватном власништву (домаће или стране организације) намеће потребу вишестраног приступа државе и оператори (организације која је одговорна за критичну инфраструктуру). Са једне стране, држава, односно надлежни органи ће дефинисати смернице на основу којих ће оператори израдити своје програме заштите, док са друге стране, оператори ће развити програме заштите који ће бити одобрени, прихваћени и усаглашени са програмима других субјеката система националне безбедности који су укључени у заштиту критичне инфраструктуре. С тим у вези, неопходна је континуирана сарадња ових двеју страна, а нарочито онда када се интереси оператора не поклапају у потпуности са интересима државе.

За сагледавање доприноса корпоративне безбедности стању националне безбедности у овој дисертацији одабран је аспект критичне инфраструктуре и њене заштите. Да би се постигао наведени циљ, поглавље које предстоји подељено је у два дела. Први део се бави теоријским увидима у одређење, идентификацију и карактеристике критичне инфраструктуре, угрожавање и аспекте њене заштите. Други део има за циљ да представи начин на који се критична инфраструктура одређује, идентификује и штити у Републици Србији, држави која је изабрана за ово истраживање.

4.1. Појмовно одређење критичне инфраструктуре и њене заштите

Национална безбедност, економски просперитет и благостање (као референтни објекти сваке националне државе) зависе од скупа различитих и уједно веома међузависних инфраструктура. Реч је о „опреми, зградама и конструкцијама, инсталацијама и услугама које се третирају као целина и као такве чине кохезивне системе неопходне за несметано функционисање државе“ (Żaboklicka, 2020, p. 71). Група аутора упозорава да је критична инфраструктура много више од „архитектуре која подржава операције“, јер архитектура сама по себи „не храни људе, не производи електричну енергију, не пречишћава воду или транспортује робу“ (Radvanovsky and McDougall, 2024, p. 3). Критичне инфраструктуре „производе кључни асортиман робе и пружају оне врсте услуга без којих нема опстанка, стабилности и развоја друштва као таквог“ (Бошковић, 2017, стр. 72). Како међутим ништа од наведеног не би постојало или могло да функционише без човека, прихватљивији је став по којем критична инфраструктура обухвата материјална физичка средства (нпр. зграде, објекти, имања, животиње, производи), нематеријална физичка средства (нпр. информације), људске ресурсе (запослени и екстерна релевантна физичка лица) и сајбер средства (хардвер, софтвер, подаци и мреже неопходне за функционисање) (DCSINT, 2006, стр. I-1). Примери ових инфраструктура од суштинског значаја укључују мреже и системе који обезбеђују електричну енергију, снадбевање нафтом и природним гасом, телекомуникационе и информационе мреже, транспортне мреже, водоводне системе, банкарски и финансијски сектор. Критичне инфраструктуре су од суштинског значаја за јавну добробит, те би њихов неуспех или поремећај потенцијално могао имати негативан утицај на здравље, сигурност, безбедност, економско и социјално благостање грађана или ефективно функционисање владе, као и исцрпљујући утицај на одбрану и националну безбедност (US President's Commission on Critical Infrastructure Protection, 1997; Rinaldi, 2004; Кешетовић, 2008; El Kalam et al., 2009; Murray and Grubesic, 2012; Komazec i Janković, 2023).[94]

[94] У скорашњем истраживању спроведеном на територијинама суседне државе Црне Горе, највећи број испитаника истакао је да критична инфраструктура има веома велики или велики значај за функционисање државе и друштва (Marjanović, 2020, str. 181).

До данас, развијен је немали број дефиниција међу којима ниједна која испуњава критеријум универзалности, нити она за коју се може рећи да је општеприхваћена. Иако је свака дефиниција применљива, бар у оној дисциплини у оквиру које је усвојена, ниједна није прихваћена као меродавна у „дисциплини критичне инфраструктуре“ (Jaradat and Keating, 2014, p. 88). Дефиниције се разликују у зависности од времена настанка и извора. Оне могу настатати у академским, стручним или институционалним оквирима. Са једне стране, разликоваће се дефиниције између различитих дисциплина у академско-стручном оквиру, док са друге стране, постојаће разлике и у институциналном дефинисању како на националном, тако и на наднационалном нивоу. Објашњење за последње наведено налази се у разликама националних или чак наднационалних политика које се темеље на свакако различитим безбедносним изазовима, ризицима и претњама, и са њима повезаним историјом, географским подручјем, политичким, економским, друштвеним и културолошким факторима. Бавећи се анализом ових концепата у националним документима, документима међународних организација, приручницима и другим студијама, уочава се да се основни приступи, односно основне дефиниције ових концепата значајно разликују од земље до земље, као и у различитим периодима (Pursiainen, 2009, p. 722; Гачић и Шећеров, 2012). Ипак, група аутора је на основу анализе политичких, правних, стручних и теоријских одређења критичне инфраструктуре утврдила је „да су основни елементи за дефинисање критичне инфраструктуре управо материјална основа (путеви, железнице, постројења, техничко – технолошки системи и средства...) и инструментални карактер такве основе у смислу да се њеним постојањем или нормалним функционисањем доприноси задовољењу потреба друштва, државе и појединца“ (Стајић, Мирковић и Радивојевић, 2020, стр. 956-957).

Анализирајући неке од дефиниција ових концепата Метју Еган (*Matthew Jude Egan*) примећује да колико год да су дефиниције широке, чини се да „и најшире критичне инфраструктуре имају тенденцију да се шире“ (2007, p. 5). Овакав став поткрепљен је чињеницом да се са једне стране развијају нови елементи који се оцењују као критични, док се са друге стране постојећи елементи препознају као критични, јер су се или развили као такви или су као такви оцењени новим системима оцењивања. Да ли се злоупотребом елементи могу дефинисати као критични иако то нису? Сасвим сигурно. У литератури је могуће пронаћи и бојазан став како је одмах након напада 11. септембра идентификовано све од пешачких мостова до високих зграда као критична инфраструктура која захтева заштиту (Prieto, 2003, p. 517). Ракић закључује да велики број стручњака указује на „опасност идентификовања свих инфраструктура као критичних услед нејасних граница између критичне и некритичне инфраструктуре“ (2015, стр. 56).[95] Изгледа да је веома тешко, ако не и немогуће одредити колико широко и дубоко треба да идемо у овој идентификацији, јер „ако је све критично, онда ништа није критично“ (RECIPE, 2015, p. 65).

Критична инфраструктура и њена заштита нису нови феномени. Одавно је познато да су основне ствари за живот попут хране и воде увек неопходне, а када су угрожене потребно их је заштити. Тако, у средњем веку владајући слојеви морали да на пример, „прикупе усеве, уведу стада унутар зидина замка и заштите бунаре“ (Jones, 2007, стр. 11). Касније, током касног деветнаестог века, развиле су се индустрије које су биле предмет интересовања креатора политике јер су обезбеђивале производе и услуге за које се сматрало да су корисни, ако не и суштински за војни, економски и друштвени развој (De

[95] О одређивању (не)критичне инфраструктуре видети више у: Moteff, D. John, and Parfomak, Paul. (2004). *Critical Infrastructure and Key Assets: Definition and Ientification, Congressional Research Service*. Washington, DC: Congressional Research Service, Library of Congress; Lewis, G. Ted. (2006). *Critical infrastructure protection in homeland security: defending a networked nation*. New Jersey: John Wiley and Sons;

Bruijne and Van Eeven, 2007, p. 26). Такве инфраструктурне индустрије развијале су се од „локалних до регионалних и коначно великих, интегрисаних, хијерархијских система“ током деветнаестог и двадесетог века (Coutard, 1999, p. 3) представљајући резултат техничког развоја, повећања сложености и међузависности и све софистицираних претњи.[96] На прелазу у двадесети век радикална међусобна повезаност великих урбаних техничких система који се баве енергијом, комуникацијама, транспортом и основним робама постала је очигледна (Duffield, 2011, p. 759). Данас, несумњиво је да је, као последица умреженог друштва, међузависност међу различитим инфраструктурним системима порасла. Она је створила и нове могућности и рањивости, које могу произвести негативне утицаје који су све чешћи, дуготрајнији или обухватнији, а све у зависности од карактеристика инфраструктуре.

За концепт критичне инфраструктуре могуће је рећи да је релативно нов. Истиче се да је употребу овог концепта као „овлашћеног концепта политике на којем се граде програми, акциони планови, законодавство“ и са њим повезаног концепта заштите критичне инфраструктуре могуће пратити од Сједињених Америчких Држава (Pursiainen, 2009, p. 722). Иако постоји став да се настанак ових концепата везује за стварање Националног комуникационог система још 1963. године када су настали проблеми у комуникацији између Сједињених Америчких Држава и Совјетског Савеза за време Кубанске кризе (Lewis, 2006, p. 30), термини критична инфраструктура и заштита критичне инфраструктуре улазе у употребу тек средином деведесетих година прошлог века.

Након терористичког напада у Оклахоми 1995. године[97], председник Бил Клинтон (*William Jefferson Clinton*) је употребио термин заштита критичне инфраструктуре и тај случај се узима за први када је званично неко употребио овај термин. Извршном наредбом којом је то учињено истакле су се одређене националне инфраструктуре, „које су од виталног значаја за САД, а чија би неспособност или уништење имало велики утицај на одбрану, економску безбедност и добробит грађана“ (Kešetović, Putnik and Rakić, 2013, p. 133). У Извештају Председничке комисије за заштиту критичне инфраструктуре из 1997. године, критична инфраструктура је дефинисана као „инфраструктура која је толико витална да би њена неспособност или уништење имало исцрпљујући утицај на нашу одбрану и националну безбедност“ (US President's Commission on Critical Infrastructure Protection, 1997). Са друге стране, постоји став да се о концепту заштите критичне инфраструктуре говори од 1998. године када је администрација Била Клинтона покренула „програм интервенција, размене знања и каталогизације који је познат као заштита критичне инфраструктуре“ (Duffield, 2011, p. 764). На основу изнетог, могуће је закључити да је тридесетак година након што се о заштити критичне инфраструктуре почело говорити овај појам добио и своје одређење. Током деведесетих година прошлог века, критична инфраструктура постала је важан елемент националне безбедности, а њена заштита је постала један од приоритета сваке државе (Moteff and Parfomak, 2004; Radvanovsky and McDougall, 2024, p. 3; Јаковљевић, 2010, стр. 64).

Током Хладног рата, теорије стратешког бомбардовања у Европи и Сједињеним Америчким Државама фокусирале су се на „виталне мете“ непријатељског индустријског система. Тако, витални системи су постали предмет забринутости по националну безбедност и за неке ауторе било је и више него потребно померити фокус са становништва на виталне системе (Collier and Lakoff, 2008). Ипак, упркос оваквом ставу, који супротставља становништво наспрам виталних система или система критичне

[96] О самој инфраструктури видети више у: Ракић, М. Марко. (2015). *Кризни менаџмент у функцији заштите критичних инфраструктура у земљама у транзицији* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

[97] Овај терористички акт се сматра најсмртоноснијим на тлу Сједињених Америчких Држава све до 11. септембра 2001. године.

инфраструктуре, Клаудиа Ардау (*Claudia Aradau*) сугерише да инфраструктура није супротстављена људима, већ се материјализује у интра-дејствима између људи и нељуди, материје и значења (2010, p. 507). Интересантно је да се Сједињене Америчке Државе препознају као главни одговорни за промену безбедносног дискурса када су „агресивне намере држава" као претње замењене ширим спектром ризика који циљају на „'меке мете' од суштинског значаја за функционисање читавог њеног друштва". Као два разлога за то, Мириам Кавелти (*Myriam Cavelty*) наводи експанзију спектра претњи по безбедност након Хладног рата, а онда и промену у перцепцији могућих мета, јер се више не сматрају метама само војни циљеви, већ и неке друге рањиве тачке (2007, pp. 16).

У ризичном друштву, када претње по „меке мете" укључујући и цивиле постају све различитије и сложеније, потребе за заштитом критичне инфраструктуре која их обезбеђује добија све више на значају. Уништавање критичне инфраструктуре, које је увек праћено масовним ефектима, познато је још и као „морално бомбардовање". Тврдило се да се уништавањем животног окружења непријатеља „воља за борбом може сломити и подстаћи народна побуна и позиви на смиривање" (Duffield, 2011, p. 759). Треба имати на уму да су многе од (ако не и све) инфраструктура међусобно повезане и зависне. Та њихова карактеристика додаје на значају њихове заштите без обзира на то да ли их угрожавају претње из природне, техничко-технолошке средине или оне које потичу од човековог деловања.

У многим земљама, осамдесетих и деведесетих година прошлог века дошло је до приватизације кључних делова критичне инфраструктуре (Boin and Smith, 2010, p. 295), односно њеног институционалног реструктурирања (заједнички назив за приватизацију, либерализацију и дерегулацију) (De Bruijne and Van Eeten, 2007, p. 19). 1980-те године биле су период либерализације тржишта, што је захватило и област критичне инфраструктуре мењајући њен карактер (Pursiainen, 2009, p. 732). Остварен је прелаз са продуктивне на шпекулативну економију, а за разлику од неких правних лица која су национализована, критична инфраструктура је фрагментирана (Duffield, 2011, p. 764). Интересантан је податак да упркос томе што већина људи у САД-у сматра да је критична инфраструктура у власништву и под управом владе, у стварности је 80% критичне инфраструктуре у власништву и под управом приватног сектора (Pesch-Cronin and Marion, 2017, p. 6).[98] Осим ако мета терориста није војна или друга безбедносна државна установа, „први" који реагују ће скоро сигурно бити цивили. Национална безбедност и припремљеност нације стога често почињу од приватног сектора (The 9/11 Commission Report, 2004). Одатле неопходност укључивања приватног сектора у планирање заштите те имовине. Иако постоји став да је корпорацијама прва одговорност према акционарима, а не према националној безбедности (Lewis, 2006, p. 2), погрешно би било извести закључак да се државе и владе „боље старају" о критичној инфраструктури него корпорације. Некада су критичне инфраструктуре у власништву приватно сектора боље заштићене него оне које припадају држави.[99] Зато, пре би се

[98] У војне сврхе се користи велики проценат цивилних ресурса и критичне инфраструктуре који су у власништву или којима управља приватни сектор. Око 90% војног транспорта за велике војне операције обезбеђује се цивилним средствима из комерцијалног сектора; преко 70% сателитских комуникација које се користе у одбрамбене сврхе обезбеђује комерцијални сектор; приближно 95% трансатлантског интернет саобраћаја, укључујући војне комуникације, преноси се преко подморских кабловских мрежа од којих већина припада субјектима из приватног сектора (NATO, 2024).

[99] Посебно питање које се отвара односи се на субјекта приватног сектора који располаже имовином која је идентификована или представља критичну инфраструктуру. Да ли је реч о домаћем или страном субјекту, да ли постоје скривени интереси или намере или други фактори од значаја за управљање заштитом критичне инфраструктуре. Чест проблем који се у пракси јавља јесте коришћење услуга страних приватних субјеката што, не улазећи у разлоге коришћења истих на тај начин, може бити озбиљна претња по националну безбедност (нпр. складиштење података на серверима страних приватних субјеката).

могло рећи да сваки случај говори за себе. Тед Левис (*Ted Lewis*) уочава негативан тренд када је у питању заштита критичне инфраструктуре с обзиром на то да ни владе ни власници из приватног сектора нису јасни у вези са својим улогама и одговорностима у погледу ове заштите (2006, p. 29). Са друге стране, аутори упозоравају да без интервенције влада, приватни сектор не може успешно да спроведе заштиту критичне инфраструктуре јер пре свега не могу да сагледају свеукупне трошкове заштите и услуга безбедности (De Bruijne and Van Eeten, 2007, p. 23).

Данас, готово да не постоји држава или међународна или регионална организација која није приступила развоју програма заштите критичне инфраструктуре. Како се развој концепата критичне инфраструктуре и њене заштите прати са тла Сједињених Америчких Држава, заштита критичне инфраструктуре препозната је као саставни део мисије унутрашње безбедности (Chertoff, 2006, p. 5). Национални комуникациони систем, основан 1963. године и Саветодавни комитет за националну безбедност, основан 1982. године, били су прве агенције за критичну инфраструктуру у оквиру владе Сједињених Америчких Држава.[100] Ипак, тек двадесетак година касније, критичност националне инфраструктуре постаје важно питање националне (унутрашње) безбедности. Тадашњи председник Клинтон издао је 1996. године *Извршну наредбу ЕО-13010* (енг. *Executive Order EO-13010*) којом је успостављена Председничка комисија за заштиту критичне инфраструктуре (енг. *Presidential Commission on Critical Infrastructure Protection (PCCIP)*). Овом комисијом је председавао Роберт Марш (*Robert Marsh*), па је отуда позната и као „Маршов извештај". Овај извештај је био прва публикација која је користила термин критична инфраструктура и као такав представља документ који је поставио основе свакој даљој дискусији на тему заштите критичне инфраструктуре (Lewis, 2006, pp. 30-34). У овом извештају критична инфраструктура обухвата „инфраструктуру која је толико витална да би њена неспособност или уништење имало исцрпљујући утицај на нашу одбрану и националну безбедност".[101] То су сектори „енергије, банкарства и финансија, транспорта, виталних људских услуга и телекомуникација" (US President's Commission on Critical Infrastructure Protection, 1997). Из овако дефинисане одредбе, јасно је да је реч о инфраструктурама које су толико виталне за државу да су морале бити обухваћене концептом свеобухватне националне безбедности. Након терористичких напада, усвојен је *Патриотски закон*, односно *Закон о уједињењу и јачању Америке пружањем одговарајућих алата потребних за пресретање и ометање тероризма из 2001. године.* У овом Закону, секција број 1016. бави се заштитом критичне инфраструктуре где се иста дефинише као „системи и средства, било физички или виртуелни, толико витални за Сједињене Државе да би онеспособљење или уништење таквих система и средстава имало исцрпљујући утицај на безбедност, националну економску безбедност, национално јавно здравље или сигурност, или било коју комбинацију тих ствари" (USA PATRIOT Act, 2001, sec. 1016). У наредним годинама становници Сједињених Америчких Држава добили су нову *Националну стратегију унутрашње безбедности* (2002), која користи дефиницију из Патриотског закона и *Националну стратегију за физичку заштиту критичних инфраструктура и кључне имовине* (2003), као и *Председничку директиву о домовинској безбедности 7* (2003) која успоставља политику за федерална одељења и агенције како би идентификовале и дале приоритет критичној инфраструктури и заштитили их од терористичких напада. Тада је дефиниција заштите проширена на 13 критичних сектора плус пет кључних имовина: национални споменици и иконе, нуклеарне електране, бране, владини објекти и

[100] О другим агенцијама видети више у: Кешетовић, Želimir, Putnik, Nenad, and Rakić, Marko. (2013). „Possibilities of Improving Critical Infrastructure Protection in Countries in Transition". In: *National critical infrastructure protection regional perspective*, (pp. 131-142). Belgrade: University of Belgrade, Faculty of Security Studies; Ljubljana: Institute for Corporative Security Studies.

[101] Дефиниција инфраструктуре из овог документа наведена је у оквиру појмовног оквира.

комерцијална кључна имовина.[102] Корак даље начињен је усвајањем *Плана заштите критичне инфраструктуре* 2006. године чија дефиниција критичне инфраструктуре бива коришћена у *Националној стратегији унутрашње безбедности из 2007. године*. Из ових докумената проистиче да критична инфраструктура „укључује средства, системе и мреже, било физичке или виртуелне, које су толико виталне за Сједињене Државе да би њихово онеспособљавање или уништење имало ослабљујући ефекат на безбедност, националну економску сигурност, јавно здравље или безбедност, или било коју комбинацију ових елемената“ (Chertoff, 2006, p. 103; Homeland Security Council, 2007, p. 25). Она обухвата 17 сектора критичне инфраструктуре и кључних ресурса, од којих сваки има физичке, сајбер и људске елементе: пољопривреда и храна, банкарство и финансије, хемикалије, комерцијални објекти, комерцијални нуклеарни реактори, материјали и отпад, бране, одбрамбена индустријска база, пијаћа вода и системи за пречишћавање воде, хитне службе, енергетика, владини објекти, информационе технологије, национални споменици и иконе, пошта и бродарство, јавно здравље и здравствена заштита, телекомуникације и транспортни системи (Homeland Security Council, 2007, p. 27). Стратегија кроз свој текст наглашава заштиту америчког народа и критичне инфраструктуре и кључних ресурсаод различитих претњи укључујући несреће изазване људским фактором и природне катастрофе, а посебно претњи тероризма.

Влада Канаде предложила је 2001. године дефиницију критичне инфраструктуре која се користи у документима Уједињених нација. По тој дефиницији, „критична инфраструктура се састоји од физичких и информационих технолошких објеката, мрежа, служби и материјалних добара који, уколико буду урушени или уништени, могу имати озбиљан утицај на здравље, безбедност, сигурност и економско благостање или ефикасно функционисање власти“ (Јаковљевић, 2010, стр. 65). У једном од докумената Уједињених нација који се баве смањењем ризика налази се дефиниција критичних структура које представљају елементе инфраструктура који подржавају основне услуге у друштву и обухватају „примарне физичке структуре, техничке објекте и системе који су друштвено, економски или оперативно неопходни за функционисање друштва или заједнице, како у рутинским околностима, тако иу екстремним околностима ванредне ситуације“ (United Nations Office for Disaster Risk Reduction, 2008, p. 3).

Са „америчког“ тла, концепти критичне инфраструктуре и њене заштите постали су актуелни на међународној сцени, па и у Европи. Унутар Европске уније (ЕУ) о овим темама је почело да се дискутује са развојем Европског програма за заштиту критичне инфраструктуре. Од 2004. године, ЕУ ради на развоју стратегије заштите критичне инфраструктуре. На нивоу Европске уније 2004. године покренута је иницијатива за припрему опште стратегије за унапређивање заштите критичне инфраструктуре. Комисија је исте године усвојила документ који се односио на тероризам као потенцијалну опасност под називом *Заштита критичне инфраструктуре у борби против тероризма*.[103] Комисија је 2005. године изразила намеру да развије *Европски програм за заштиту критичне инфраструктуре* (у даљем тексту: Програм)[104] и исте године је усвојила *Зелени папир о Европском програму за заштиту критичне инфраструктуре*.[105] Исте године је од Комисије затражен нацрт поменутог Програма.

---

[102] Видети више у: Office of Homeland Security. (2002). *National Strategy for Homeland Security*; White House. (2003). *The Physical Protection of Critical Infrastructures and Key Assets*; United States Department of Homeland Security. (2003). *Homeland Security Presidential Directive 7 - HSPD-7*; Homeland Security Council. (2007). *National Strategy for Homeland Security*.

[103] Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism, COM/2004/0702 final.

[104] Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final.

[105] Green Paper on a European programme for critical infrastructure protection, COM/2005/0576 final.

Наредне године, 2006. године, донета је одлука о финансирању пилот пројекта овог Програма. Комисија је 12. децембра 2006. представила предлог директиве о идентификацији и одређивању европских критичних инфраструктура и заједничком приступу за процену потребе за побољшањем њихове заштите и усвојила *Саопштење о Европском програму за заштиту критичне инфраструктуре*.[106]

Општи циљ Програма је побољшање заштите критичне инфраструктуре у Европској унији (ЕУ). Образложење овог циља заснива се на уверењу да би поремећај у инфраструктури која пружа кључне услуге могао наштетити безбедности и економији ЕУ и добробити њених грађана. У саопштењу се јасно наводи да се овај циљ може постићи извесним активностима, односно усвајањем процедура за идентификацију и одређивање европске критичне инфраструктуре и заједнички приступ процени потребе за унапређивањем заштите такве инфраструктуре, усвајањем мера којима се постиже имплементација Програма (акциони план, Информациона мрежа за упозорење о критичној инфраструктури, успостављање група стручњака за заштиту критичне инфраструктуре на нивоу ЕУ, размена информација и идентификација и анализа међузависности), обезбеђивањем подршке земљама Заједнице, јачањем међународне сарадње кроз секторске споразуме и усвајањем неопходних финансијских мера (Commission of the European Communities, 2006). Први део Програма који се односи на процедуре за идентификацију и одређивање европске критичне инфраструктуре испуњен је планираним и каснијим усвајањем посебне директиве, о којој ће касније бити речи. Програм је истакао значај међузависности у континуираном функционисању инфраструктуре, а нарочито у безбедносном окружењу где постоје повећани ризици попут природних катастрофа, тероризма и криминалних активности, а који нису ограничени на националне територије. Информациона мрежа за упозорење о критичној инфраструктури која је једна од мера предвиђених за олакшавање имплементације, треба да обезбеди платформу за размену најбољих пракси у овој области. Од средине 2013. године све чланице Заједнице могу ову мрежу као заштићени информационо-комуникациони систем да користе за размену информација и добрих пракси.

Значајан напор начињен у овој области јесте доношење *Директиве Већа 2008/114/ЕС о утврђивању и означивању европске критичне инфраструктуре и процени потребе побољшања њене заштите* коју је Заједница добила 2008. године.[107] Ова директива дефинише критичну инфраструктуру, заједничке процедуре за идентификацију и означавање европске критичне инфраструктуре, заједнички приступ у процени потреба за побољшавање заштите и то првенствено од претњи тероризма. Рок њеног важења ограничен је до 17. октобра 2024. доношењем *Директиве 2022/2557 ЕВРОПСКОГ ПАРЛАМЕНТА И ВЕЋА о отпорности критичних субјеката и о стављању ван снаге Директиве Већа 2008/114/ЕС*.[108]

ЕУ дефинише критичну инфраструктуру као „средство, систем или његов део који се налази у државама чланицама и неопходан је за одржавање виталних друштвених функција, здравља, безбедности, заштите, економског и социјалног благостања људи, чије би нарушавање или уништење, као последица неодржавање тих функција, могло имати значајан ефекат у држави чланици“, док је европска критична инфраструктура сва она која се „налази у државама чланицама, чије би нарушавање или уништење имало значајан утицај на најмање две државе чланице“ (Directive 2008/114/EC, 2008, art. 2).

[106] Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM/2006/0786 final.

[107] COUNCIL DIRECTIVE 2008/114/ECof 8 December 2008on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[108] 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.

Новом Директивом 2022/2557 критична инфраструктура означава „имовину, објекат, опрему, мрежу или систем или део имовине, објекта, опреме, мреже или система, који је потребан за пружање кључне услуге“, док је кључна услуга свака „услуга која је кључна за одржавање виталних друштвених функција, економских активности, јавног здравља и сигурности или околине“ (Directive (EU) 2022/2557, 2022, art. 2). Новодонета директива изоставља дефиницију европске критичне инфраструктуре, а критичну инфрастурктуру дефинише тако да изоставља да је реч о инфраструктури државе чланице. Ипак, када је реч о секторима идентификованим као критична инфраструктура, од два сектора идентификована у ранијој директиви, новом директивом број сектора износи 11. Реч је о следећим: енергија, информационе и комуникационе технологије, вода, храна, финансије, грађанске власти, јавни и правни поредак и сигурност, саобраћај, хемијска и нуклеарна постројења, космос и научно истраживање (Directive (EU) 2022/2557, 2022, ANNEX).

Анализом стратегија заштите критичне инфраструктуре, Организација за економску сарадњу и развој предлаже дефиницију критичне инфраструктуре одређујући је као „физичку или нематеријалну имовину чије би уништење или поремећај озбиљно нарушио јавну безбедност, друштвени поредак и испуњавање кључних владиних одговорности“, док би штета проузрокована на овај начин била катастрофална и далекосежна (Gordon and Dion, 2008, p. 3). У истраживању се закључује да су дефиниције углавном врло широке и да укључују како физичке елементе тако и оне неопипљиве и да све дефиниције имају сверизичан приступ (извори ризика могу бити природни или изазвани људским фактором).

НАТО критичну инфраструктуру дефинише као „објекте, услуге и информационе системе који су толико витални за нације да би њихова неспособност или уништење имало исцрпљујући утицај на националну безбедност, националну економију, јавно здравље и безбедност и ефикасно функционисање владе“ (Jahier et al., n.d.). НАТО и Европска унија објавили су у јуну 2023. године завршни извештај о процени који је израдила Оперативна група НАТО-ЕУ за отпорност критичне инфраструктуре.[109] На мање од 10 страна, радна група је указала на значај критичне инфраструктуре посебно у енергетици, транспорту, дигиталној инфраструктури и свемиру и њену заштиту од тренутних претњи у безбедносном окружењу. Сумирано, критичну инфраструктуру чине „средство, систем или његов део, који је од суштинског значаја за одржавање виталних друштвених функција, здравља, заштите, безбедности, економског или социјалног благостања људи, где би нарушавање или уништење имало значајан утицај на друштво као резултат неодржавања тих функција“ (European Committee for Standardization, 2021).

4.1.1. Идентификација критичне инфраструктуре

Један од предуслова разумевања критичне инфраструктуре управо је то – разумети велике и сложене инфраструктурне системе и одредити шта је „критично“, а шта не. Приоритизација се може извршити на неколико начина. Реч је о идентификовању критичне имовине, идентификовању рањивости или решења која се односе на више од једне инфраструктуре, идентификовању међузависности између инфраструктура, коришћењу географске локације у одређењу приоритета или фокусирању на оне инфраструктуре које су или у потпуном власништву и којима управља владаили на оне приватне или локалне инфраструктуре од којих савезна влада зависи (Moteff, Copeland and Fischer, 2003).

[109] EU-NATO Task Force on the Resilience of Critical Infrastructure. (2023). *Final Assessment Report*.

Анализирајући начин идентификације критичне инфраструктуре на нивоу Европске уније, аутори Шкеро и Атељевић указали су на три могућа приступа. Први приступ идентификује основне услуге које су друштву неопходне, а потом утврђује које инфраструктуре обезбеђују те услуге. Други приступ идентификује кључне инфраструктуре у сваком сектору. Трећи приступ идентификује кључне операторе за сваки сектор који ће потом идентификовати критичну инфраструктуру. Такође, аутори сугеришу на то да државе користе различите критеријуме за коначну оцену критичности. Код неких се у обзир узимају објективна мерила као што су финансијски губитак или број становника на које се може утицати, док други прате субјективна мерила која се углавном односе на стручна мишљења (Škero i Ateljević, 2015, str, 203).

Приступ који идентификује кључне инфраструктуре у сваком сектору, познат још и као секторски, сматра се да у савременом добу није довољан. Аутори предлажу друге приступе попут асиметричног приступа решавању проблема заштите, приступа код ког би се критична инфраструктура посматрала као систем састављен од низа других система или међусекторски приступ. Управо последње наведен приступ прихваћен је као најбољи метод за идентификовање критичне инфраструктуре (Ракић, 2015, стр. 57).[110] Зато, када се говори о идентификацији критичне инфраструктуре, говори се о идентификацији сектора што уједно представља и услов заштите критичне инфраструктуре како по секторима, тако и у целини. Изостављање неког објекта који чини део инфраструктуре може имати трагичне последице у виду материјалних као и људских губитака. Са друге стране, идентификацију је могуће спроводити у контексту услуга по секторима које се пружају. Тако, постоје два приступа: од врха према доле (енг. *top-down*) и одоздо према горе (енг. *bottom-up*). У првом случају, влада има водећу улогу у дефинисању и одређивању приоритета критичних услуга преко координационог тела или надлежног органа (пример су Швајцарска, Естонија, Холандија и Чешка), док у другом случају та одговорност припада операторима критичних инфраструктура (пример су Француска и Уједињено Краљевство) (Petrakos and Kotzanikolaou, 2019, p. 22-23).

Након идентификације критичне инфраструктуре требало би спровести и поступак њене класификације. На пример, елементи критичне инфраструктуре могу бити бројни, а незамисливо је обезбедити једнаку заштиту за све елементе. Стога, врши се њихова класификација према степену угрожености на оне са највишим степеном угрожености, са средњим и ниским степеном угрожености. Даље, класификацију је могуће извршити према значају и степену (стратегијског значаја (највиши степен), регионалног значаја (средњи степен) и локалног значаја (нижи степен)), према међузависности елемената критичне инфраструктуре (оне које не зависе од других елемената, оне које делимично зависе од других елемената и оне које апсолутно зависе од других елемената), према броју јединица које чине елементи критичне инфраструктуре (Једна јединица један елемент, две и више јединица један елемент и мноштво (више стотина) јединица један елемент), према утицају на међународну критичне инфраструктуре (оне са делимичним или појединачним утицајем, оне без утицаја и оне са апсолутним утицајем – међузависност)) (Стајић, 2018, стр. 126).

Истраживање које је анализирало секторе критичне инфраструктуре у чак 194 земаља[111] дошло је до закључка да је тек мало више од половине анализираних земаља дефинисало секторе критичне инфраструктуре (100 од 194 земаља). Земље Северне Америке и скоро

[110] Међусекторски приступ између осталог уважава чињеницу да су услед повезаности и зависности ефекти који настају унутар једног сектора увек међусекторског карактера, јер се „преносе“ и на неки друге секторе. Уједно, међусекторски приступ уважава и прекогранични карактер ефеката. О томе видети више у наредним поглављима.

[111] 193 чланице Уједињених нација и Тајван.

све земље Европе су дефинисале секторе, док земље Азије (49%), Латинске Америке и Кариби (42%), Аустралије и Океаније (29%) и на последњем месту Африке (28%) каскају за њима. Од идентификованих сектора, најчешће се помињу енергетика (96%), информационе и комуникационе технологије (ИКТ) (95%), транспорт (93%), привреда и финансије (89%), јавне услуге (84%) и здравство (83%) (Weber, Pericàs Riera and Laumann, 2023, pp. 4, 1).[112] Јасно је да не препознају све земље исте секторе критичне инфраструктуре. Сектори се разликују како на нивоу региона, тако и на нивоу континената.

Упркос општем тренду да је све већи број сектора који се дефинишу као „критични", означити сву инфраструктуру која се користи свакодневно за друштвене активности као „критичну" нема рационалну основу. Штавише, и сама критична инфраструктура је превише велика и сложена да би целокупна била заштитићена, а нарочито узмајући у обзир реалну опасност да буде нападнут било који њени део и било када, било којим оружјем. Можда решење лежи у фундаменталнијем приступу који се концентрише на „друштвене функције" уместо на пуке „инфраструктуре" (Pursiainen, 2009, p. 736). У том контексту, критична инфрастурктура више не значи стабилне и конкретне физичке или информационо-комуникационе системе, већ отворене и рањиве мреже или системе „виталних функција друштва у целини или инфраструктуре уграђене у ове функције" (Pursiainen, 2009, p. 723; Lundborg and Vaughan-Williams, 2011, p. 369). Овакав холистички приступ критичној инфраструктури има свој ослонац у стварним догађајима. Наиме, терористички напади са почетка двадесет првог века на финансијске и транспортне мреже од виталног значаја за „континуирани проток информација, роба и услуга" подстакли су заштиту суштинских функција за друштво, односно заштиту критичне инфраструктуре (Lundborg and Vaughan-Williams, 2011, p. 368).

Критична инфраструктура обухвата ресурсе који се по правилу могу идентификовати као номиналне вредности, чије би оштећење или уништење проузроковано природним, техничко-технолошким и људским фактором изазвало последице по свеобухватну безбедност и благостање, односно функционисање државе и друштва. Уважавајући секторски приступ, она обухвата ресурсе из следећих сектора:

- Електрична мрежа са енергијом (производња, дистрибуција и складиштење електричне енергије);
- Нафтоводи и гасоводи (производња, дистрибуција и складиштење нафте и гаса);
- Информационе и телекомуникационе технологије (информациони и телекомуникациони системи, електронске комуникације, интернет, пренос података);
- Транспорт (друмски, железнички, ваздушни, водени);
- Здравство (здравствене установе, фармацеутска индустрија);
- Вода (снабдевање пијаћом водом, отпадне воде, безбедност воде);
- Храна (производња и снабдевање храном, безбедност хране, залихе);
- Банкарство и финансије (берзе, инвестиције, системи плаћања);
- Јавне службе (службе безбедности, хитне службе, државни органи) и
- Наука, истраживање и развој (укључујући заштиту културног и националног наслеђа, истраживање космоса).

[112] Идентификација критичне инфраструктуре и прецизирање њених елемената се разликује међу државама. Видети више и упоредити у: Kljajić, Zdenko, Mandžuka, Sadko, i Škorput, Pero. (2010). „Primjena ICT-a u upravljanju kritičnom infrastrukturom u tranzicijskim zemljama". U *18. Telekomunikacioni forum TELFOR 2010* (str. 75-78). Beograd; Škero, Mirko i Ateljević, Vladimir. (2015). Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope 2008/114/ES. *Vojno delo* 3, str. 192-207; Марковић, Јана. (2023б). Улога корпоративне безбедности у заштити критичне инфраструктуре Републике Србије. *Безбедност* 65 (2), стр. 197-214.

Наведена класификација врло је слична детаљном прегледу сектора и њиховим елементима које је група аутора категоризовала на основу поменутог истраживања сектора критичне инфраструктуре. У наставку је табеларно представљен један од резултата истраживања, како би се што је могуће више и прецизније приказало шта је то што је неопходно држави за функционисање и задовољење потреба њеног становништа, а што је као такво препознато од стране доносица одлука (видети Табелу 6).

Табела 6: Категоризација сектора критичне инфраструктуре (прилагођено према Weber, Pericàs Riera and Laumann, 2023, pp. 7-8)

СЕКТОР КРИТИЧНЕ ИНФРАСТРУКТУРЕ	**ЕЛЕМЕНТИ**
Енергија	електрична енергија; природни гас; уље; нафтни деривати; нафтна и гасна инфраструктура; енергетски објекти и мреже; снабдевање енергијом; енергетски ресурси и горива; комплекс енергије; необновљиви природни ресурси; електрични пренос; енергетика и комуналије; нуклеарни реактори; електронско напајање; грејање; струја и вода.
Информационо-комуникационе технологије	телекомуникације; електронска комуникација; комуникационе и информационе технологије; дигитална инфраструктура; информациони системи; клијент и информациони системи за пацијенте; аудиовизуелни материјал и информације; информационе телекомуникационе мреже; информационе и комуникационе мреже; сателитска комуникација; правна лица и индивидуални предузетници који поседују информационе системе; услуге информационог друштва; дигитална економија; електромагнетни спектар и геостационарна орбита; радиоелектрични спектар; телефонија; кључне базе података; оптички кабл; подморски каблови; телекомуникационе линије; постови; дата центри; сектор складиштења и обраде података; јавна комуникација; електронски медији; веза између науке и технологије.
Транспорт	саобраћај; поштанска услуга; транспортна инфраструктура; транспорт и рафинација угљоводоника; јавни превоз; ваздушни саобраћај; цивилна авијација; авијација; различити облици превоза; копнени саобраћај; систем поморског транспорта; систем ваздушног транспорта; транспорт робе; развој лука и аеродрома; здравствено транспортно спасавање; железница; копнени путеви; лучка или железничка веза.
Здравље	здравствена заштита; здравство; спашавање у транспорту; медицинске услуге и услуге неге; спасилачке службе; контрола незгода; системи националног или јавног здравља и безбедност; објекти за заштиту здравља; медицински сектор; хитне помоћи и болница.
Храна	пољопривреда; залихе хране; вода; прехрамбени производи; прехрамбена индустрија; прехрамбени сектори; залихе хране са финансијског аспекта; сигурност хране; шумарство; водопривреда; прехрамбени сектори; пољопривреда и плантаже.

Табела 6: наставак

СЕКТОР КРИТИЧНЕ ИНФРАСТРУКТУРЕ	ЕЛЕМЕНТИ
Вода	снабдевање и дистрибуција воде за пиће; водопривреда; храна и вода; отпадне воде; струја и вода; пиће; вода, шуме и животна средина; бране; третман непитких вода; канализације; очување вода; водовод; енергетски сектор за струју и воду.
Јавне услуге	социјалне услуге; поштанске и курирске услуге; правда, јавни ред; безбедност; државна и друштвена управа; регионални развој и јавни радови; животна средина; културна баштина; заштита од катастрофа; спортски објекти; производња, складиштење и транспорт опасних материја; национални споменици и вредности; национални споменици и културно наслеђе; безбедносне услуге; хитне службе; државне агенције; управљање отпадом; цивилне активности државе; правосудне активности; одлагање комуналног отпада; држава и управа; медији и култура; културни објекти; закон и влада; влада; службе владе; национална безбедност; инфраструктура полиције и јавне безбедности; дигитална влада; производно складиштење и коришћење хемијских и радиоактивних материја; заштита животне средине; администрација; администрација владе; општинске техничке службе; места масовне агломерације; државни органи; државне институције; јавна добра; власт; јавна безбедност; цивилна заштита становништва и територије; биолошка сигурност и биозаштита; биодиверзитет и генетско наслеђе; поштански и отпремнички субјекати; јавна безбедност; туризам; локалитети наслеђа; е-управа; услуге електронске управе; јавна краљевска управа; логистика; владине инсталације; покрајинске и општинске власти; основне хитне службе;закон; спровођење кривичног закона; друштвени поредак и безбедност; урбана подручја.
Економија и финансије	финансијске услуге; финансијско тржиште и валута; осигурање; банке; берза инфраструктура; институције финансијског тржишта; платни промет; набавке готовине; финансирање државног буџета; порески систем; трговина и индустрија; инжењеринг; рударство; металуршка и хемијска индустрија; услуге осигурања; имовина; државна регистрација права на непокретности и трансакције са информационим технологијама; међународна трговина; трговина; производња; угоститељство; комерцијални објекти; критична индустрија; царински центри; буџетирање; паркови високе технологије.
Истраживање и образовање	наука и технологија; истраживачки објекти; академски сектор; образовне институције; високо образовање.
Национална безбедност	одбрана; национална одбрана, национална безбедност; јавна безбедност; безбедност и сигурност; поморски систем; војни сектор; војне активности државе; свемир; свемирски систем и програм; свемирска технологија; заштита; ракете; нуклеарни систем; одбрамбена индустрија; одбрамбена база; међународни односи; безбедносне и обавештајне службе.

Приложена табела не само да треба да разјасни шта је то што је критично за функционисање државе и друштва, односно шта је то што треба да се штити уколико се жели континуитет у снадбевању производима и услугама које су неопходне за свакодневно функционисање, већ потврђује резултат примене секторског приступа у идентификацији критичне инфраструктуре.

Као што је већ наведено, идентификација критичних објеката, система и мрежа предуслов је заштите истих тих елемената, те уједно заштите економске стабилности и свеукупне безбедности државе. Без обзира на приступ који је изабран приликом идентификације, сам процес идентификовања укључује процену рањивости, међузависности и потенцијалних последица поремећаја критичних елемената. Овај процес треба да укључи како државне/владине субјекте, тако и власнике/операторе критичне инфраструктуре, као и релевантне субјекте из приватног сектора.

4.1.2. Отпорност, рањивост и међузависност као кључна својства критичне инфраструктуре

Ако би се о критичној инфраструктури говорило као о систему, дакако да је реч о комплексном систему састављеном од великог броја међусобно повезаних и зависних елемената (делова) који функционишу заједно у динамичном унутрашњем и спољашњем окружењу. Ови системи морали би бити отворени, флуидни, спремни да издрже деловање унутрашњих и спољашњих сила и способни да се опораве од тог деловања настављајући да функционишу, бар минимално уз претрпљене губитке.

Да би се у потпуности разумела сложеност критичне инфраструктуре, неопходно је сагледати њене различите аспекте, узимајући у обзир кључне карактеристике које играју значајну улогу у њеној функционалности и стабилности. То укључује отпорност као способност да издржи и опорави се од поремећаја или криза, рањивост као подложност ризицима и кваровима, и међузависност као међусобну повезаност различитих инфраструктурних компоненти, при чему квар једног система може имати каскадне ефекте на друге. Истражујући ова критична својства, могуће је остварити боље разумевање како критична инфраструктура функционише и како се може заштитити.

4.1.2.1. Отпорност критичне инфраструктуре

Отпорност критичне инфраструктуре је њено својство које све више завређује пажњу. Уједно, она представља главни елемент заштите критичне инфраструктуре, па се неретко говори о „заштити и отпорности“ критичне инфраструктуре. То је способност опоравка, способност прилагођавања, способност да се издржи, да се апсорбује (Setola et al., 2016, p. 13). Отпорност критичне инфраструктуре сматра се индикатором који квантификује способност да се обезбеди рад у условима када делују негативни спољашњи и унутрашњи фактори (Lukas and Hromada, 2011, p. 1138).

У литератури је широко прихваћен став да је концепт отпорности развијен у екологији од стране Стенли Крофорд Холинга (*Stanley Crawford Holling*), и да се као такав раширио на све друштвено-еколошке системе (Berkes, 2007, p. 286). Ипак, постоје аутори који сматрају да за „корен“ овог концепта не треба узимати екологију већ механику (Alexander, 2013, p. 2712). Са еколошког становишта, Холинг отпорност одређује као „упорност/истрајност односа унутар система“ и „способност ових система да апсорбују промене промењивих стања, али да параметри и даље постоје“ (Holling, 1973, p. 17). Дакле, реч је о способности да се издрже поремећаји и да се настави са функционисањем. Значајно одређење отпорности даје Питер Тимерман (*Peter Timmerman*) који исту дефинише као изградњу „тампон капацитета“ (енг. *Buffering Capacity*) друштва како би оно постало отпорно на шокове катастрофа (1981, p. 20).

Концепт отпорности критичне инфраструктуре је добио на значају у ери након терористичких напада 2001. године када је постао стратегија важна за националну безбедност. Ревидирана Национална стратегија САД усвојена 2007. године уједињује „структурну отпорност критичних инфраструктура и оперативну отпорност владиних институција за реаговање у ванредним ситуацијама и приватних правних лица у суочавању са кризом“ (Walker and Cooper, 2011, p. 152). Тај однос који се успоставља између владе и корпорација у контроли критичне инфраструктуре итекако је од значаја за националну безбедност (Ridley, 2011, p. 122).

Група аутора усваја дефиницију по којој је отпорност „капацитет система да апсорбује сметње, подлеже променама и задржи исте основне функције, структуру, идентитет и повратне информације“. Како истичу, елементи ове дефиниције садржани су у дефиницијама прихваћеним од стране неких владиних агенција (Longstaff et al., 2010, p. 3). Знатно опсежнију дефиницију отпорности нуди група аутора која отпорност одређује као „способност да се разумеју и предвиде ризици – укључујући нове/настајуће ризике – који прете критичној функционалности инфраструктуре, да се припреми за очекиване или неочекиване поремећаје, да оптимално апсорбује/издржи њихове утицаје, реагује и опорави се од њих, и да се прилагоди/трансформише инфраструктура или њен рад на основу научених лекција, чиме се побољшава отпорност инфраструктуре против крхкости” (Jovanovic, Chakravarty and Jelic, 2021). Концепт отпорности критичне инфраструктуре укључује три елемента: капацитет апсорпције (степен до којег систем може да апсорбује утицај и минимизира последице уз мало напора), адаптивни капацитет (способност система да се прилагоди нежељеним ситуацијама подвргавањем неким променама) и ресторативни капацитет (брзина повратка на нормалне или побољшане операције) (Francis and Bekera, 2014, p. 94).

Нова Директива Европске уније отпорност дефинише као „способност критичног субјекта (јавни или приватни субјекти за које је утврђено да припадају једној од 11 категорија критичне инфраструктуре) да спречи инцидент, заштити се од њега, одговори на њега, одупре се инциденту, ублажи га, апсорбује га, прилагоди му се, те се опорави од истог“ (Directive (EU) 2022/2557, 2022, art. 2). Отпорност би значила унапређивање механизама за предвиђање и рано упозорење, односно бржу и ефикаснију реакцију и опоравак од последица, или способност да се настави са функционисањем које је оптимално за одржавање кључних функција. Еган истиче да је тежња ка хиперефикасности и приватизација многих критичних инфраструктура смањила њихову отпорност. Он као једно од решења види стварање системске отпорности чему у прилог не иде чињеница да извршни директори обично нису спремни да улажу у мере предострожности (Egan, 2007, p. 14). Различити заинтересовани субјекти укључујући истраживаче, стручњаке, институције дали су велики број дефиниција отпорности које имају потенцијал за примену на безбедност инфраструктуре. Група аутора их је систематично издвојила (Biringer, Vugrin and Warren, 2013, pp. 80-83).

У литератури је могуће пронаћи и другачији став. Према неким ауторима (Kaufmann, 2013; Fjäder, 2014), безбедност и отпорност јесу супротни концепти. Први се односи на оно што је проактивно како не би дошло до инцидента, док други значи реаговање када до инцидента дође. То би значило и да концепт отпорности увек значи постојање неког ризика, што није упитно с обзиром на такозвано ризично друштво у којем живимо. За разлику од оних ризика који имају поуздане историјске и статистичке податке па се могу квантификовати, отпорност је препоручена стратегија у управљању оним ризицима које карактерише висок ниво неизвесности (или веома мала вероватноћа), али велики утицај (Ninković, 2021, p. 1207). Пример оваквог ризика јесте пандемија Ковид-19, која је итекако указала на рањивост друштва.

Уз све наведено, први предуслов јачања отпорности свакако је успостављање правног оквира којим би се обезбедили услови за ефикасно понашање и функционисање критичних субјеката. На нивоу Европске уније и њених чланица исто је учињено усвајањем поменуте Директиве, као и доношењем и усаглашавањем националних нормативних докумената. Штавише, Заједница позива државе чланице да усвоје стратегије јачања отпорности критичних субјеката (Directive (EU) 2022/2557, 2022, Preambule). Стратегије јачања отпорности требало би да се развијају унутар свеобухватне политике заштите критичне инфраструктуре, и њихово усвајање не треба да буде ограничено на наднационалне и националне нивое. Националне државе никада немају само обавезу, већ и реалну потребу за успостављањем правних механизама и предузимање даљих корака који ће развијати отпорност како целокупне заједнице тако и националне критичне инфраструктуре. Поред њих, сви критични субјекти исто тако као предуслов опстанка треба да имају стратегије и на њима развијене структуре и процедуре јачања отпорности. Развијена отпорност која захтева „флексибилност, редундантност и капацитет за поновно састављање расположивих ресурса“ (Boin and Smith, 2010, p. 298) јесте услов који обезбеђује брз опоравак од инцидената или поремећаја. Ипак, како аутори примећују „промовисање стратегија отпорности у припреми за кварове критичне инфраструктуре је тежак позив“ јер се увек ове стратегије „суочавају и надмећу“ са индивидуалним, институционалним и друштвеним рањивостима и приоритетима (Boin and McConnell, 2007, p. 57). Потребно је пронаћи механизме који ће задовољити и јачање отпорности и реализовати друге приоритете који постоје на различитим нивоима заједнице.

Корпоративна безбедност успостављена у секторима критичне инфраструктуре директно утиче на отпорност критичне инфраструктуре. Проактивним и реактивним мерама безбедности повећава се капацитет апсорпције, адаптивни капацитет и ресторативни капацитет, односно да се утиче на предвиђање и рано упозорење на поремећај, бржу и ефикаснију реакцију и опоравак од последица. Функцијама корпоративне безбедности успоставља се механизам за јачање отпорности. У првом реду, издвајају се функције попут управљања ризицима и кризама, а потом и континуитет пословања. Прве две треба да предвиде ризике и минимизирају последице ако се ризик оствари. Трећа функција фокусира се на прилагођавање новонасталој ситуацији и одржавању способности да се настави са функционисањем које је оптимално за одржавање кључних функција, као и са испоруком производа или услуга. Ипак, није оправдано ограничити се на ове функције. Разлог је чињеница да су сви капацитети корпоративне безбедности неопходни да се спречи поремећај, заштити се и реагује, те опорави од истог. Дакле, поред управљања ризицима и кризама/катастрофама и континуитета пословања, незаобилазни елементи у јачању отпорности јесу и физичка и техничка заштита, заштита запослених, заштита података и информација, надзор и контрола, као и по потреби спровођење интерних истрага и других функција. Сумирано, корпоративна безбедност јесте фактор јачања отпорности.

4.1.2.2. Индекс (мерења) отпорности критичне инфраструктуре

Национална лабораторија Аргон (енг. *Argonne National Laboratory*) у сарадњи са Секретаријатом за унутрашњу безбедност САД развила је Индекс отпорности (енг. *Resilience Index*) и Индекс мерења отпорности (енг. *Resilience Measurement Index*). Иста лабораторија развила је и Индекс мера заштите, о којем ће више речи бити у делу о заштити критичне инфраструктуре.[113]

[113] Постоји и трећи индекс, Индекс мерења последица (енг. *Consequences Measurement Index*), који карактерише потенцијално максималне последице изазване нежељеним догађајем у објекту.

Индекс отпорности упоређује ниво отпорности на критичним инфраструктурама и усмерава давање приоритета ограниченим ресурсима за побољшање отпорности. Такође, пружа вредне информације власницима/операторима о статусу њиховог објекта у односу на имовину сличних сектора и о начинима на које могу да повећају отпорност (Fisher et al., 2010, p. 1). Главне компоненте и подкомпоненте које чине отпорност су робусност (способност одржавања критичних операција и функција у условима кризе), сналажљивост или довољност у погледу ресурса (способност да се вешто припреми, одговори и управља кризом или поремећајем како се она одвија) и опоравак (способност да се врате и/или поново успоставе нормалне операције што је брже и ефикасније могуће након прекида) (National Infrastructure Advisory Council, 2009, p. 13). Свака компонента има субкомпоненте које су представљене у Табели 7.

Табела 7: Компоненте Индекса отпорности по нивоима (Fisher et al., 2010)[114]

НИВО 1	**НИВО 2**
Робусност	Редундантност
	Превенција/ублажавање
	Одржавање кључних функција
Сналажљивост или Довољност у погледу ресурса	Рестаурација
	Координација
Опоравак	Обука/вежбе
	Постојање свести
	Заштитне мере
	Залихе
	Одговор
	Нови ресурси
	Алтернативна места

Индекс мерења отпорности представља индикатор отпорности критичне инфраструктуре. Наиме, овај индекс треба да послужи као основа за развијање индикатора учинка који карактерише отпорност објекта. Основне компоненте Индекса су припремљеност, мере ублажавања, могућности одговора и механизми опоравка. Свака од ових компоненти састоји се од субкомпоненти представљених у Табели 8.

[114] Објашњење: Ниво 1 се рашчлањује на ниво 2, тако да свака компонента Индекса има своје подкомпоненте. За детаљнији приказ видети у: Fisher, R. E., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Eaton, L. K., Haffenden, R. A., Hussar, N. E., Klett, M. S., Lawlor, M. A., Millier, D. J., Petit, F. D., Peyton, S. M., Wallace, K. E., Whitfield, R. G., and Peerenboom, J. P. (2010). *Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program* (No. ANL/DIS-10-9). Argonne: Argonne National Lab (ANL) (pp. 31-33).

Табела 8: Компоненте Индекса мерења отпорности по нивоима (Petit, Bassett, Black et al., 2013)[115]

НИВО 1	НИВО 2	НИВО 3
Припремљеност	Постојање свести	Операције отпорности
		Дељење информација
	Планирање	Нове мере планирања
		План континуитета пословања
		Операција у ванредним ситуацијама/План за хитне случајеве
		Сајбер план
Мере ублажавања	За конструкције	Природне опасности
		Нове мере ублажавања
		Раздаљина
		Значајно смањење имовине/подручја
	Алтернативна места	/
	За ресурсе	Електрична енергија
		Природни гас
		Комуникације
		Информациона технологија
		Вода
		Отпадне воде
		Транспорт (железница, ваздушни, копнени, поморски саобраћај, цевоводи)
		Критични производи (хемикалије, гориво, биопроизводи, отпадни материјал, сировине)
Могућности одговора	Могућности на лицу места	Нове мере за одговор
		Могућностиза управљање инцидентима
	Могућности ван лица места	Интеракција првих који одговарају (на инцидент)
		Уговори о нивоу услуге коришћења ресурса
		Еквивалентни број зависности
	Центар за управљање инцидентима и командовање	Укљученост локалних центара за ванредне ситуације
		Карактеристике објекта
Механизми опоравка	Уговори о рестаурацији	Дељење информација
		Уговори о обнови ресурса
	Време опоравка	Значајан опоравак имовине/подручја
		Опоравак ресурса

Без преобимне разраде начина употребе ових индекса, у наредном тексту су представљене компоненте и једног и другог индекса из разлога указивања на један од начина којим је могуће приступити повећању отпорности критичне инфраструктуре и њене заштите. Са једне стране, наведени индекси се могу користити посредством посебне платформе под називом Алат за испитивање инфраструктуре (енг. *Infrastructure Survey Tool*) док са друге стране, није немогућа или погрешна њихова употреба ван оквира ове платформе, као нека врста „чек-листе".

[115] Објашњење: Ниво 1 се рашчлањује на ниво 2, који се даље рашчлањује на ниво 3, тако да свака компонента Индекса има своје подкомпоненте класификоване у два нивоа.

Индикаторе који су представљени у склопу индекса могуће је, поред класификације према компонентама, класификовати и у односу на поремећај. То би значило да се неки индикатори односе на период пре поремећаја дајући релативну процену отпорности, док се други односе на период након поремећаја дајући апсолутну меру (тако што се мера поремећаја мери и процењује у односу на унапред одређену основну линију) (Prior, 2015, p. 5). Један од извештаја који се бави управо потенцијалним индикаторима, који могу да се користе за процену отпорности критичне инфраструктуре, исте групише на оне који су карактеристични за период пре поремећаја и оне који су карактеристични за период након поремећаја. Првој групи припадају: вероватноћа квара, квалитет инфраструктуре, функционалност инфраструктуре пре догађаја, заменљивост, међузависност, квалитет/обим ублажавајућих карактеристика, квалитет планирања/реаговања на поремећаје, квалитет комуникација у кризним ситуацијама/размена информација, безбедност инфраструктуре. У другој групи, препознати су следећи индикатори: отказивање система, озбиљност квара, функционалност после догађаја, процена штете после догађаја, цена враћања функционалности након догађаја, време опоравка после догађаја, однос опоравак/губитак (Prior, 2015).

На основу изнетих података уочава се да, без обзира на приступ који се користи у одређивању индикатора отпорности критичне инфраструктуре, поједини индикатори су незаобилазни. Реч је о планирању, мерама реаговања, комуницирању и размени информација, способности враћања у стање пре поремећаја, ресурсима који су потребни за то. Чак и када се разматра безбедност критичне инфраструктуре (физичко обезбеђење, безбедносни менаџмент, безбедносне снаге) коју је могуће одредити као посебан индикатор, тај индикатор се даље може рашчлањивати на елементе од којих се састоји и чија процена омогућава процену индикатора. На том путу, могуће је „ући у поље“ претходно појашњеног Индекса мера заштите.

4.1.2.3. Рањивост критичне инфраструктуре

Јачање отпорности директно је повезано са смањењем рањивости. Заправо, један од извора рањивости јесте управо недостатак еластичности или отпорности (Cardona, 2004). Могло би се констатовати да је критична инфраструктура „генератор рањивости“, чије локације и зависности могу ширити ризик преко географских простора (D'Ercole and Metzger 2009 према Pescaroli and Alexander, 2006, p. 178). Рањивост се може дефинисати као „слаба тачка, изложена малигним радњама, које се врше у циљу уништења или оштећења одређених средстава критичне инфраструктуре“ (Tagarev and Pavlov, 2007, p. 41). То је својство сваке критичне инфраструктуре, она је уграђена у њих и зависи како од унутрашњих фактора (попут унутрашње структуре) тако и од броја и врсте поремећаја као једног дела спољашњих фактора. Уствари, сви ти фактори могли би се распоредити у три велике групе: операције (менаџмент, организациона структура, култура, финансије, процедуре...), окружење (тржиште, стејкхолдери, животна средина, социо-економски парамери...) и ресурсе (технологија, знање, вештине...).

Идентификовати, мерити и оцењивати ризике у сложеним системима као што је критична инфраструктура комплексна је активност. Ова активност неопходна је у циљу смањења рањивости и јачања отпорности. Један од начина за процену ризика код сложених критичних система јесте аналитички оквир који укључује горенаведене операције, окружење и ресурсе и разматра међузависности између њих (Koubatis and Schönberger, 2005). У прошлости су стратегије отпорности биле фокусиране на предвиђање ризика и ублажавање рањивости. Данас се међутим оне осмишљавају тако да интегришу и отпорност (спречавање, заштиту) и еластичност (реаговање, опоравак) (Longstaff et al., 2010, p. 2). С обзиром на то да критичну инфраструктуру не чине само

физички ресурси, неопходно је имати то у виду и спречити уско фокусирање на рањивости ове категорије ресурса. Аутори сматрају да се латентна рањивост може идентификовати и разумети пре него што се појаве окидачи, те у вези са тим саветују да пажња треба да буде преусмерена са сценарија ризика заснованих на хазардима на сценарије рањивости засноване на потенцијалним тачкама ескалације (Pescaroli and Alexander, 2016, p. 188). Код таквог приступа издваја се процена рањивости која у суштини треба да одговори на питање *Шта може да крене наопако ако систем буде изложен конкретним претњама?*[116] Типови рањивости управо могу да варирају у зависности од природе претње. У вези са тим, Џорџ Бејкер (*George Baker*) предлаже следеће кораке у процени рањивости: 1. разумети мисију објекта/организације и системе и функције који су критични; 2. идентификовати њихове рањивости; 3. разумети дизајн и рад система како би се утврдили начини и вероватноће квара; 4. ако је могуће, идентификовати последице кварова у смислу времена застоја, ефеката на људе и било каквих каскадних ефеката на друге ентитете и 5. препоручити побољшања објекта/организацијекако би се смањила рањивост (2005, p. 3).

Рањивост је дакле подложност ефектима неког догађаја или осетљивост на догађај. Када је реч о рањивости критичне инфраструктуре, основа разумевања и процене рањивости лежи у процени ризика. Процењивање ризика укључује идентификацију, анализу и вредновање ризика да би се одлучило о поступању са ризиком. Управо се корпоративна безбедност, а посебно функција управљања ризиком, бави проценом, контролом и управљањем свим оним ризицима који се могу десити правном лицу, у овом случају објекту, систему или мрежи критичне инфраструктуре. Стога, значајан елемент смањења рањивости критичне инфраструктуре јесу успостављене организација и функције корпоративне безбедности. Корпоративна безбедност у циљу заштите лица, имовине и пословања критичне инфраструктуре проактивно и реактивно смањује изложеност ризицима и рањивост те критичне инфраструктуре.

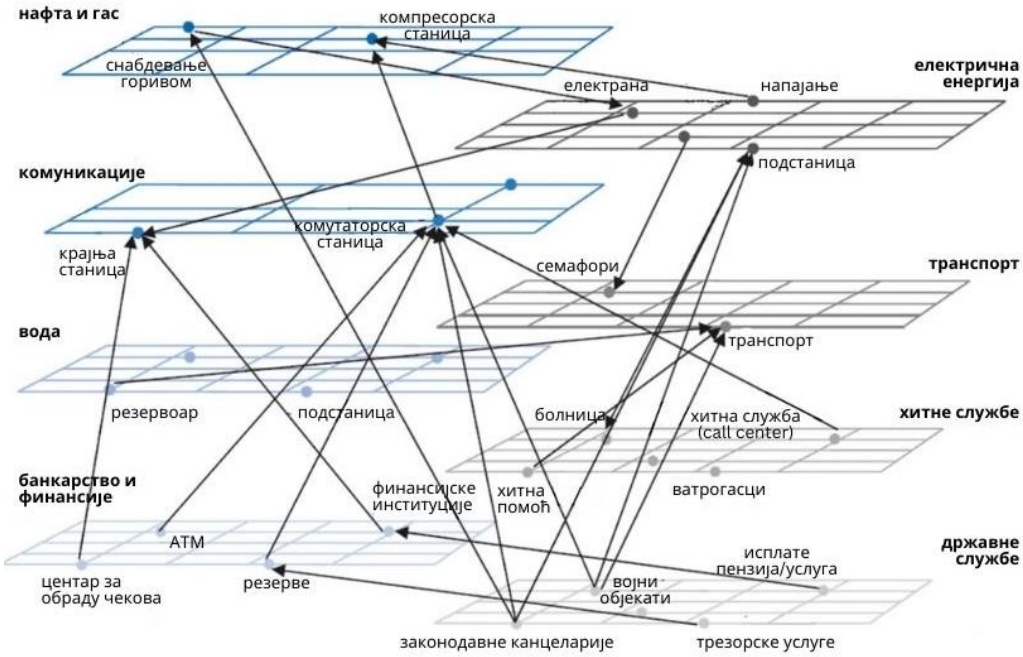
4.1.2.4. Међузависност критичне инфраструктуре

Оно што додатно компликује рањивост, и тиме отежава развој отпорности јесте међузависност критичне инфраструктуре. Растућа зависност праћена је повећаним осећајем рањивости на нове и будуће претње као што су тероризам и климатске промене (Zimmerman et al., 2005; Boin and McConnell, 2007, p. 55; Collier and Lakoff, 2008, p. 40; Karagiannis et al., 2019a; Karagiannis et al., 2019b). Очекује се да ће климатске промене и повезани ризици, укључујући пораст нивоа мора, олујне ударе и екстремне временске прилике, повећати рањивост многих критичних инфраструктура на неколико континената, апосебно оних који се налазе на обали мора и дуж пловних путева (OECD, 2019; Pal, Kumar and Mukhopadhyay, 2023, p. 681). Од последица климатских промена, највише штете би могли имати индустријски, транспортни и енергетски сектори (European Union, 2023). Транспортна инфраструктура, хемијска постројења и нуклеарни реактори, као и водоводни системи посебно су рањиви на терористичке нападе. Поред директних и тренутних губитака (нпр. губитак људских живота, економски губици), напади на ове инфраструктуре могу оставити дугорочне негативне последице (нпр. прекид у пружању услуга, контаминација животне средине…).

Данас, постоје студије случаја које проучавају међузависност (Amin, 2000; Rinaldi, Peerenboom and Kelly, 2001; Little, 2002; Zimmerman, 2004; Pederson et al., 2006; Gordon

[116] Данас постоје бројне методологије и апликативни софтвери који омогућавају процену рањивостии анализу рањивости у критичној инфраструктури. О томе, видети више у: Yusta, Jose M., Correa J. Gabriel, and Lacal-Arántegui, Roberto. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy policy* 39 (10), pp. 6100-6119.

and Dion, 2008; Ouyang, 2014) и бројни политички документи који препознају њену важност[117]. Међузависност као „двосмерни однос између инфраструктура кроз који на стање сваке инфраструктуре утиче или је у корелацији са стањем друге“ (Rinaldi, 2004, p. 4) може бити физичка, сајбер, географска или логичка (Rinaldi, Peerenboom and Kelly, 2001, p. 14). Просторна и функционална категорија, које је развио Ре Цимерман (*Rae Zimmerman*), обухватају већину елемената ове типологије. Просторна је еквивалентна географској категорији, док функционална комбинује физичку, сајбер и логичку (2004, p. 4059).[118] Просторна међузависност подразумева физичку блискост једне инфраструктуре другој, док функционална међузависност подразумева да је један тип инфраструктуре неопходан за функционисање друге. На пример, кварови електричних или телекомуникационих система могу имати последице по друге критичне секторе који зависе од снабдевања електричном енергијом или од телекомуникационих услуга. Односно, било који сектор критичне инфраструктуре који трпи последице поремећаја имаће негативан утицај на друге секторе са којима је повезан (видети Илустрацију 7).



Илустрација 6: Међузависности услуга и мрежа (NARUC, 2005 према OECD, 2019)

На повећање међузависности, пре свега је утицао развој технологије и иновација. Као што је већ поменуто, до повезивања критичних инфраструктура и стварања или увећања њихове међузависности дошло је како у функционалном тако и у географском смислу. Тако, добили смо критичне инфраструктуре које све мање функционишу за једну државу, а све више пружају добра и услуге како на националном нивоу тако и на наднационалном. Створили смо мрежу система где се ефективни рад једног сектора критичне инфраструктуре све више ослања на нормалан (оптималан) рад других сектора. Иако већа међузависност критичне инфраструктуре нуди друштву бројне бенефите, иста је њену заштиту учинила захтевнијом. Инфраструктурне међузависности једноставно су и прилике и тачке рањивости. Ефекте инцидента, поремећаја или кварова једне инфраструктуре могуће је лако пренети на друге

[117] Вероватно први овакви документи били су: Национална стратегија физичке заштите критичних инфраструктура и кључних средстава, Национална стратегија унутрашње безбедности, Критичне основе: Заштита америчке инфраструктуре, Политика Клинтонове администрације о заштити критичне инфраструктуре (Rinaldi, 2004, p. 1).

[118] О типологијама међузависности видети више у: Ouyang, Min. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability engineering and System safety* 121, pp. 43-60.

инфраструктуре.[119] Зато, од суштинске је важности у најкраћем року изоловати и решити квар чиме се ланчане реакције и ескалације предупређују или бар заустављају за краћи временски период.

Када је комуникациони сателит ПанАмСат Галакси 4 (енг. *PanAmSat Galaxy IV*) ротирао из своје орбиталне позиције у мају 1998. године, преко 80% дигиталних пејџера у Сједињеним Америчким Државама је искључено. Овај догађај је имао озбиљне последице по кабловски и радио-дифузни пренос, ауторизацију кредитних картица и трансакције на банкоматима, као и по здравствени систем јер није било могуће позвати лекаре и друге здравствене раднике (Little, 2002, p. 11). Прекид телекомуникација који је у јуну 2019. погодио велике делове Холандије угрозио је рад хитних служби и учинио недоступним полицију и друге службе (Reuters, 2019). Исте године, у Естонији је олуја изазвала нестанак струје који је довео до озбиљних поремећаја у снабдевању горивом и пијаћом водом, угрозио телекомуникације и рад болница (ERR, 2019).[120] Преношење ефеката како унутар истог сектора тако и између различитих сектора услед све веће прекограничне и међузависне мреже пружања добара и услуга у савременим условима све чешће има прекогранични карактер. На пример, прекид у електрани у Шпанији довео је до великих осцилација струје стотинама километара далеко у Немачкој, Мађарској и Пољској, иако ове локације нису зависне нити директно повезане са шпанском електричном енергијом (Koubatis and Schönberger, 2005, p. 210). Ефекти које је изазвала криза КОВИД-19 имали су међусекторски и уједно прекогранични карактер. Поред здравственог сектора који је био први на удару, негативне ефекте су претрпели и други сектори попут економије и снадбевања. Били су угрожени послови, туризам, као и ланци снадбевања (European Commission, 2020).

Ефекти се могу интензивирати тако да се од релативно малих поремећаја развију озбиљне кризе. Криза представља „сваки изненадни прекид до тада непрекидног функционисања одређеног система или циклуса“ (Jakovljević i Gačić, 2012, str. 281) претећи основним структурама, вредностима и нормама који у условима „временског притиска и несигурних околности, захтевају доношење критичних одлука“ (Rosenthal, Charles and ‘t Hart, 1989). Вероватно најбољи пример (међу)зависности јесте енергетска критична инфраструктура. Каскадни ефекти поремећаја или кварова на њој осетили би се на бројним другим секторима критичне инфраструктуре. Електрична мрежа је једна од најстаријих критичних инфраструктура. Она се у основи састоји од трафостаница, мреже за пренос електричне енергије од електрана до енергетских трафостаница, дистрибутивне мреже за пренос од трафостаница до потрошача и контролног система који омогућава управљање и контролу мреже. Електрична енергија је неопходна за сваки систем, сваки уређај који за своје функционисање користи напајање. Од снадбевања домаћинстава електричном енергијом, преко коришћења исте у саобраћају и за транспорт, за коришћење информационе и телекомуникационе технологије, пружања услуга у банкарском сектору, за функционисање јавних служби и низа других активности, електрична енергија је неопходна за добијање нафте и природног гаса, воде и хране што опет обезбеђује основу за нормалан живот и функционисање. Ако узмемо у обзир секторе критичне инфраструктуре, без сумње можемо рећи да енергетика итекако има утицаја на све друге секторе. Ипак, и други сектори су ти који стварају условеза

[119] Кварови се могу класификовати као кварови са заједничким узроком (заједнички узрок доводи до прекида рада две или више инфраструктуре у исто време), ескалирајући кварови (поремећај/квар у једној инфраструктури погоршава независан поремећај/квар друге) или каскадни кварови (поремећај/квар у једној инфраструктури узрокује поремећај/квар у другој) (Koubatis and Schonberger, 2005, p. 201).

[120] О међусекторским последицама изазваних природним несрећама видети више у: Schweikert, Amy, Nield, Lindsey, Otto, Erica, and Deinert, Mark. (2019). *Resilience and critical power system infrastructure: Lessons learned from natural disasters and future research needs*, Policy Research Working Paper 8900. World Bank.

ефикасно или бар оптимално функционисање енергетике, па отуда зависности и међузависности критичне инфраструктуре постају једно од главних питања у области критичне инфраструктуре и њене заштите.

Тек недавно, информационе технологије и рачунарски системи препознати су као један од кључних елемента у одржавању националних система критичне инфраструктуре. Њихов значај огледа се у два правца. Најпре, многи од постојећих елемената критичне инфраструктуре се у великој мери ослањају на умрежено рачунарство и други, све је више заступљено општије ослањање на информационе технологије и интернет (Merabti, Kennedy and Hurst, 2011). С обзиром на степен технолошког развоја, експанзију информационе инфраструктуре и интернета, данас готово да ниједан сектор критичне инфраструктуре не може функционисати без ових елемената. Уколико узмемо у обзир и то да је реч о инфраструктури која превазилази територијалне границе, могуће је да се инфраструктурни елементи који су од значаја за функционисање једне државе и њену националну безбедност физички налазе на територији других држава. Генерално, сајбер простор где се дешава сва размена која се заснива на употреби информационих технологија и интернета нема границе. Као такав, он ограничава државе или међународне организације да самостално управљају њиме или га регулишу и контролишу. Потребни су дакле сарадња свих актера међународне заједнице и транснационална решења развијања политике коришћења и заштите информационе инфраструктуре. Значај потреба за ефикаснијом сарадњом и решењима додатно се увећава имајући у виду чест транснационални карактер ове критичне инфрастурктуре, као и њену повезаност и међузависност са другим.[121] Група аутора је спровела истраживање које је обухватило скуп података од 1749 кварова на критичној инфраструктури у 29 европских земаља, од којих је 95% било након 2000. године. Аутори су открили да енергетски сектор чини 60% свих каскадних ефеката, 28% потиче из сектора телекомуникација и интернета, 5% долази из сектора транспорта, а 3% се налази у сектору вода и 4% у осталим секторима (Luiijf et al., 2008, p. 305). У енергетском сектору међуповезаност као својство инфраструктуре се итекако истиче. Истина је да међусобно повезивање и напредне технологије доводе до веће ефикасности и поузданости, али оне такође доносе нове изворе рањивости кроз све већу сложеност и спољне претње (Li et al., 2005, p. 918).

Када је у питању међузависност као атрибут критичне инфраструктуре, они који се баве безбедношћу у било ком објекту, систему или мрежи критичне инфраструктуре не смеју да изгубе из вида међусобну повезаност инфраструктура. Кризе и ефекти у инфраструктури коју штите могу да се пренесу на друге инфраструктуре, као што и негативни ефекти са других инфраструктура могу да се пренесу на оне које они штите. У том контексту, праћење и поступање са ризицима, као и управљање кризама не смеју да буду ограничени на окружење једне инфраструктуре која се штити. Корпоративна безбедност не сме да буде ограничена на интерно окружење инфраструктуре у оквиру које је успостављена, већ да континуирано сагледава и анализира екстерно окружење од којег је штићена инфраструктура зависна.

4.1.3. Угрожавање критичне инфраструктуре са освртом на економске последице

Објекти критичне инфраструктуре су објекти које можемо окарактерисати као подложне за различите врсте претњи, од природних непогода и катастрофа, преко

[121] Појам транснационалних инфраструктура везује се за Јохана Шота (*Johan Schot*) који у свом раду говори о транснационалним инфраструктурама у модерној Европи (2003).

техничко-технолошких несрећа до криза које је човек својим деловањем проузроковао. Као посебно озбиљне претње издвајају се природне катастрофе, индустријски удеси, тероризам укључујући претње бомбом, употреба дронова, саботажа и диверзија, претње по безбедност података и информација или сајбер инциденти.[122] Свака од наведених претњи може се испољити било када, и то како у време мира тако и током оружаних сукоба, као део борбених дејстава. Као део борбених дејстава, наравно, доминантне су претње које потичу од човека, а које имају циљ да дестабилизују државу и ослабе морал и одбрану становништва циљајући основне услуге попут енергије, воде, хране, здравства. Све претње које се остварују човековим деловањем могу потицати како од домаћих актера, чак и оних запослених у објектима критичне инфраструктуре, тако и од иностраних актера. Такође, циљеви ових претњи се могу разликовати, те бити усмерени на конкретан објекат или ширу заједницу. У вези са последњим, неке претње могу бити усмерене против државе и имати за циљ њено угрожавање или чак дестабилизацију. Претње је могуће сагледати далеко опсежије (CIP Strategy, 2009, p. 9):

- природни догађаји – екстремни временски догађаји (нпр. олује, обилне падавине, падови температуре, поплаве, топлотни таласи, суше); шумски и други пожари; сеизмички догађаји; епидемије и пандемије код људи, животиња и биљака; космички догађаји, између осталог, енергетске олује, метеорити и комете;
- технички квар/људска грешка – квар система (нпр. недовољна или превелика сложеност планирања, неисправне хардверске и/или софтверске грешке); немар; несреће и ванредне ситуације; неуспеси у организацији (нпр. недостаци у управљању ризицима и кризама, неадекватна координација и сарадња) и
- тероризам, саботажа и други облици криминала; грађански ратови и ратови.[123]

Посебну пажњу завређује и група претњи усмерена на податке и информације, као и инфраструктуру која их подржава. Највећа опасност са наведеног аспекта проистиче из претњи људског карактера у које се убрајају „крађа, намерно или ненамерно оштећење или уништење опреме укључујући и медије за трајно или привремено складиштење података и информација од стране инсајдера, аутсајдера или њиховим заједничким деловањем; неовлашћено или незаконито откривање и приступ информацијама, њихово обрађивање, односно неовлашћено читање, умножавање, измена или брисање информација; вршење напада у циљу долажења до жељених информација без обзира да ли се користе малициозни програми, врши опструкција услуга или се користе технике обмањивања корисника; грешке корисника (ненамерна измена или брисање, погрешно усмеравање); технички кварови хардвера, софтверске грешке, сметње у

[122] Из спроведеног истраживања, претње које су испитаници идентификовали уклапају се у изнети оквир. Издвајају се тероризам, диверзија и саботажа. Посебна забринутост је изражена у вези са дојавама о постављеном минско-експлозивном средству и употреби дронова. Сајбер претње, а посебно цурење информација је такође пропознато као претња међу појединим испитаницима. Свему наведеном додајмо дела имовинског криминалитета, често не велике, али веома учестале крађе које доводе до великог економског губитка. Проблем корупције такође је од стране неких испитаника препознат као озбиљна претња. Догађаји попут несташице воде, корона вируса или поплава, а који могу да изазову ванредну ситуацију препознати су као претња. Елементарне непогоде, пожар као последица топлотног удара или непоштовања законске регулативе (посебно приликом изградње или реконструкције објеката где се не поштују прописи) такође су ризик по било који систем. Код одређених делатности, као значајна претња идентификовани су и хемијски удеси. Увек постоје и претње које су везане за непридржавање или лоше придржавање правила рада, немарност, незнање, а које су посебно опасне у процесу производње или других индустријских процеса рада.

[123] Приложена класификација обухватила је и претње које се испољавају ван мирнодопских услова, попут ратова, у којима је, по правилу, критична инфраструктура увек мета напада.

комуникационим мрежама и друге претње попут прекида у снадбевању електричном енергијом, повлачења опреме или дела опреме која се користи у раду“ (Марковић, 2023в, стр. 17-18). Значај препознавања ових претњи велика је из разлога што је информациона инфраструктура данас неискључиви фактор функционисања осталих инфраструктура.

Значајно је истаћи да је веома тешко предвидети неке од претњи које имају значајан утицај на рад и функционисање инфраструктурних објеката. Посебно се издвајају оне које потичу од деловања човека (нпр. пожар и други акциденти, криминалне активности, саботажа, диверзија, терористички напад). Уз то, с обзиром на повезаност и зависност различитих инфраструктура, није довољно сагледати једино ове врсте претњи. Претња је увек и „нека друга“ критична инфраструктура у тој мрежи повезаних инфраструктура. Стога је неопходно да се превазиђе процена претњи заснована на парадигми редукционог узрока и ефекта и пређе на више „системску“ парадигму (Jaradat and Keating, 2014, p. 87). Приликом заштите, важно је избећи такозвану „загонетку рањивости“. Иако се идентификовањем најзначајније рањивости (са најгорим исходом) и заштитом од ње гарантује да не може доћи до максималне штете, јасно је да у таквом случају алтернативни сценарији који се игноришу заправо могу нанети скоро онолико колико и најгори исход (Murray and Grubesic, 2012).

Иако је тешко проценити економски и друштвени утицај поремећаја критичне инфраструктуре, неки примери указују на њихову (процењену) величину и импликације изражене у облику економских губитака.[124] Сходно томе, у тексту који следи, наведени су финансијски губици. Добро познато, Североисточно Замрачење (енг. *Northeast blackout*) 14. августа 2003. које је погодило преко 50 милиона људи изазвало је економску штету која се процењује на између 4 и 10 милијарди долара само у Сједињеним Америчким Државама (ELCON, 2004; Koonce et al., 2008, p. 170).[125] Услед ерупције исландског вулкана 2010. године, летови су били забрањени на седам дана у чак 20 земаља унутар европског ваздушног простора, а сама авиоиндустрија је претрпела штету од бар 1,7 милијарди долара (IATA, 2010). Исте године, Чиле је погодио земљотрес који је довео до укупне штете у вредности од 30 милијарди долара (18% БДП-а), од чега је 20,9 милијарди долара (12,7% БДП-а) настало због оштећења инфраструктуре (OECD, 2019). Суперолуја Сенди која је погодила Њу Џерси и Њујорк 2012. године утицала је на секторе енергетике, транспорта, комуникација, воде и здравства у ширем градском подручју Њујорка и Њу Џерсија и проузроковала око 68 милијарди долара штете (Flynn, 2015, p. 5). Белгијско нуклеарно постројење морало је 2014. године да буде затворено на шест месеци због саботаже, због чега је велики део капацитета за производњу електричне енергије у земљи био недоступан и захтевало је поправке у износу од 138 милиона евра. После терористичког напада 2016. године, белгијски аеродром Завентем је остао затворен две недеље, а процењени трошкови за реконструкцију инфраструктуре износили су 160 милиона евра. Урушавање моста у Ђенови 2018. године проузроковало је штету од 360 милиона евра за око 2.000 компанија и губитак од 100 милиона евра за лучку, индустријску и логистичку привреду. Дрон који је 33 сата ометао лондонски аеродром Гетвик 2018. године коштао је авио компаније процењених 55 милиона евра (European Commission, 2020). Експлозија складишта опаснихи токсичних материјала и гасова, која се догодила 2015. године у луци Тјенђин (трећи највећи град у Народној Републици Кини) проузроковала је материјалну штету од 2,4 милијарде долара што је

[124] Утицаје катастрофалних догађаја није једноставно измерити. О техникама које се користе у појединим земљама видети више у: OECD. (2018b). *Assessing the Real Cost of Disasters: The Need for Better Evidence*. Paris: OECD Publishing. Доступно на: https://www.oecd-ilibrary.org/governance/assessing-the-real-cost-of-disasters_9789264298798-en.

[125] Замрачење у Бразилу у марту 1999. било је још озбиљније погодивши преко 97 милиона грађана (Venkatachary, Prasad and Samikannu, 2017, p. 252).

чини једном од најгорих индустријских катастрофа које су се догодиле у Кини и једном од највећих у свету када је реч о величини осигураних губитака (Swiss Re, 2016). Експлозија више од 2.750 тона амонијум нитрата несигурно ускладиштеног у луци Бејрут 2020. године проузроковала је штету од између 3,8 и 4,6 милијарди америчких долара. Недавно рушење моста у Балтимору затворило је луку, а процењује се да ће затварање луке коштати 50 милиона долара дневно (The Economist, 2024). Тајван је ове године погодио земљотрес, најјачи у последњих 25 година. Процене економске штете углавномсе фокусирају на последице у ланцима снадбевања полупроводницима и чиповима, у вези са чим је оцењено да су губици минимални или скоро занемарљиви. Међутим, 1999. године Тајван је погодио земљотрес магнитуде 7,7, а који се сматра најгорим недавним земљотресом, након којег је Влада Тајвана проценила да ће економски трошкови земљотреса бити 9,2 милијарде долара, укључујући трошкове реконструкције уништених зграда и 1,2 милијарде долара губитака у индустријској производњи (Baum, 1999b према Papadakis and Ziemba, 2001, p. 261).

Као што је већ истакнуто, информационе технологије и рачунарски системи препознати су као један од кључних елемента критичних инфраструктура и уопште функционисања држава. Паралелно са тим, треба имати на уму да су наведене области такве да у њима предњачи приватни сектор и индустрија јер поседују и управљају великим делом дигиталне инфраструктуре. Све већа дигитализација многих критичних инфраструктура учинила их је рањивијим на различите претње из дигиталног или сајбер простора. Једна од таквих претњи „повреда података“ јавља се као озбиљан проблем по пословне ентитете, али и националне службе. Једна од америчких мултинационалних корпорација робних кућа (енг. *TJX Companies*) морала је да издвоји 118 милиона долара за покривање трошкова и потенцијалних обавеза у 2008. години због цурења података. Хартленд систем плаћања (енг. *Heartland Payment Systems*) из истог разлога имала је нето губитак од више од 52 милиона долара. Због сајбер напада на ентитете у власништву корпорације Сони (енг. *Sony's PlayStation Network and Sony Online Entertainment*) 2011. године, иста је имала губитке од више од 250 милиона долара. Постоје такође процене да уколико би дошло до крађе идентитета у Америци, појединац би изгубио у просеку 5.000 долара, у Аустралији око 790 долара. У Уједињеном Краљевству сваке године украде се идентитет за скоро два милиона људи, што националну економију кошта 3,48 милијарди долара (OECD, 2013, p. 29). Према подацима из 2023. године, глобална просечна цена повреде података највећа је до сада и представља повећање од 15 одсто у последње три године. Трошкови повреде података за критичне инфраструктуре (финансијске услуге, индустрије, технологија, енергетика, транспорт, комуникације, здравство, образовање и јавни сектор) премашују 5 милиона долара, док на остале индустрије одлази мање од 4 милиона долара (Ribeiro, 2023).

У примерима који су представљени наведени су финансијски губици проузроковани угрожавањем критичне инфраструктуре у различитим секторима и различитим претњама у мирнодопским условима.[126] Ипак, финансијски губици било директни или индиректни (скоро) никада нису једине последице ове врсте угрожавања. Поремећаји на критичној инфраструктури, без обзира чиме изазвани, потенцијална су претња по живот и здравље људи, као и биљни и животињски свет, односно по животну средину изазивајући њену контаминацију. Поремећаји могу утицати на пружање основних услуга

[126] Уколико се за разматрање узму и услови рата и оружаних сукоба, сагледавање последица било би далеко обимније и сложеније. Чак и уколико се за разматрање узму тренутне оружане активности Русије према Украјини, сагледавање угрожавања и губитака по критичну инфраструктуру захтевало би доста простора, и излазило би ван оквира предмета рада. Из тог разлога, на овом месту се указује на то да се последице угрожавања увек могу сагледати у два правца: последице настале угрожавањем у условима мира и последице настале угрожавањем у условима рата или оружаних сукоба, односно последице проузроковане нападима током борбених дејстава.

и производа, а озбиљност утицаја зависи од трајања поремећаја, отпорности критичних процеса, али и спремности власти да реагује. Проблеми се могу осетити у ланцима снадбевања, али и изазвати озбиљне друштвене ефекте који би чак могли да угрозе стабилност државе.

Као прилог изнетом, наводи се пример: Београдски водовод годишње произведе преко 200 милиона кубних метара воде у пет производних погона. Поред производних погона, водоводни систем чине и 149 бунара, 34 резервоара, 35 црпних станица и 4.016 километара дистрибутивне мреже (Београдски водовод и канализација, н.д.). Највећи производни погон се налази у Макишу и снадбева највећи део Београда. Уколико дође до, на пример, терористичког физичког напада и контаминације[127] услед њега у једном производном погону, последице су вишеструке: потенцијални губитак живота, повреде или болест, уништење и/или оштећење погона, прекид у снадбевању водом, економски губици. Ту је и незаобилазан ефекат на становништво који се огледа у изазивању панике и стварању неповерења о систем снадбевања водом на временски период вероватно далеко дужи од оног који је потребан за свеукупни опоравак водовода. Са другачијег аспекта, номиналне последице се могу сагледати на следећи начин: директне – укупан трошак који је потребан за ремонт погона и трошак који Београдски водовод има због престанка рада и снадбевања водом; и индиректне – трошак који је потребан за свеукупну деконтаминацију (водовода и животне средине уколико је и она контаминирана) и последице са којима се суочавају крајњи корисници (физичка и правна лица, односно домаћинства и индустрија). Када је реч о домаћинствима као крајњим корисницима, последице се сасвим сигурно могу приказати номинално јер недостатак воде из водовода директно утиче на набавку воде из других извора, у првом реду, повећава куповину воде. Када је реч о индустрији, недостатак воде условљава прекид свих процеса за чије је спровођење она неопходна. На тај начин, сва роба и услуге чија производња и пружање зависе од водних ресурса бива угрожена. Последице које би индустрија имала под таквим околностима такође могу бити номинално изражене.

Оваква ситуација међутим указује на још једну значајну ствар. Негативан утицај у једном сектору може бити еквивалент позитивном утицају у другом сектору. Са једне стране, израчунајмо колико просечно домаћинство троши воде на дневном нивоу, док са друге стране израчунајмо колико би та количина воде коштала домаћинство уколико исту купи. Свакако, домаћинство би на дневном нивоу трошило далеко мање воде у условима када исту не може да добије из водовода, али количина воде коју купи за основне потребе има своју номиналну вредност која је лако рачунљива.

4.1.4. Заштита критичне инфраструктуре

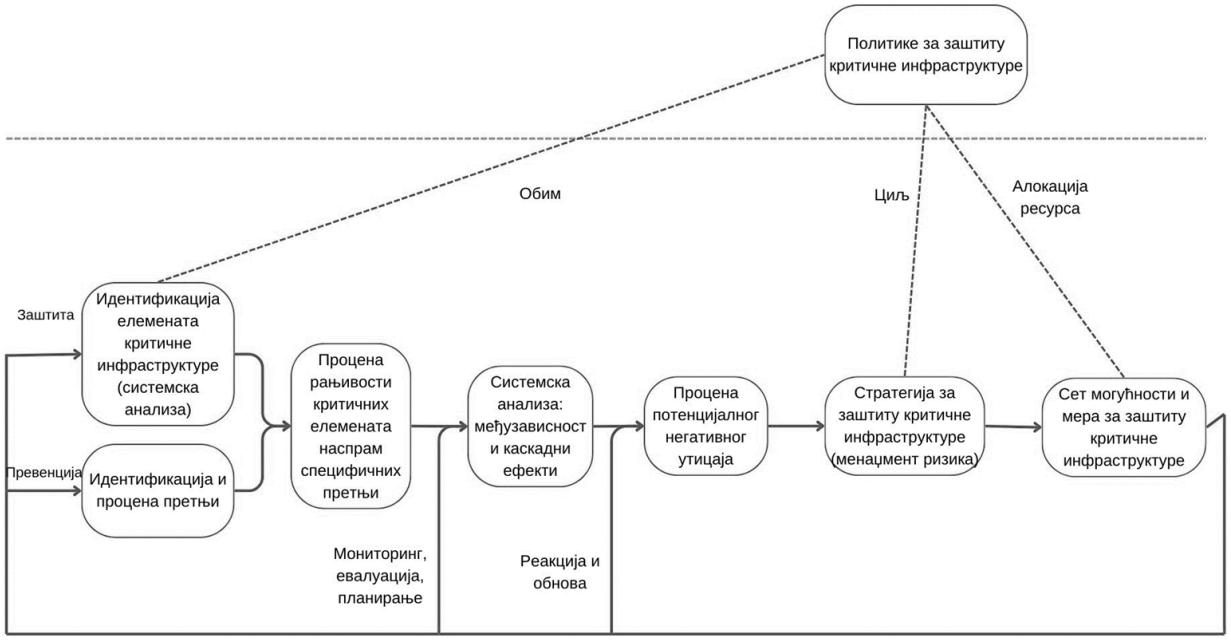
У тексту који је претходио већ је у извесној мери било речи о заштити критичне инфраструктуре. Заштита критичне инфраструктуре један је од примарних задатака било које државе. Заштитом би се омогућило постизање правилног функционисања економског тржишта, побољшала сигурност снабдевања енергијом, омогућила интеграција тржишта и потрошачима омогућиле користи од нових технологија (Yusta, Correa and Lacal-Arántegui, 2011, p. 6100). Разумевање заштите критичне инфраструктуре као „процеса који се непрестано развија је од виталног значаја за циљ безбедне и отпорне нације“ (Pesch-Cronin and Marion, 2017, p. 272). Могуће је говорити о

[127] Историја познаје случај потенцијалног напада на Београдски водовод, 1972. године од стране Бугојанске групе (хрватска екстремна организација Хрватско револуционарно братство): „Мало је познато да је група донела теглу са килограмом експлозивног отрова, који је требало да постави у београдски водовод, чиме би побила скоро цео Београд“, наводи Божидар Спасић (Ćuruvija, 2016 према Addicted to food, 2019).

начинима заштите или подели улога и одговорности између јавног и приватног сектора, о такозваном Паретовом принципу 80-20%[128], али никако о неопходности заштите.

Заштита се може сагледати са два аспекта. Најпре, критична инфраструктура укључује физичке и логичке системе неопходне за подршку безбедности, сигурности и благостања заједнице. Потом, реч је о самој заштити критичне инфраструктуре и томе да ли је способна да пружи своје предвиђене услуге заједници (Radvanovsky and McDougall, 2024, p. 8). У истраживању Организације за економску сарадњу и развој о управљању критичним ризицима које је спроведено 2016. године, половина земаља ове организације је навела поремећај критичне инфраструктуре као један од њихових националних критичних ризика (OECD, 2018a, p. 26).

Оно на шта је претходни текст још указао јесте то да је предуслов заштите критичне инфраструктуре њена идентификација. У вези са тим, могуће је рећи да је идентификација уједно и први корак заштите. Поред ње, заштита би најмање требало да обухвати спровођење анализе ризика на основу сценарија главних претњи, рањивости сваког средства и потенцијалног утицаја и идентификацију, избор и приоритизацију противмера и процедура са разликом између сталних мера безбедности које идентификују неопходна безбедносна улагања и средства која су релевантна за употребу у сваком тренутку и степенованих мера безбедности које се могу активирати према различитим нивоима ризика и претњи (Directive 2008/114/EC, 2008, ANNEX II). Такве мере су управо проактивно и реактивно деловање одговорних субјеката у заштити критичне инфраструктуре (видети Илустрацију 7). Односно могло би се говорити о „безбедносним контролама“ које укључују где, шта, како и када акција може да промени функционалност система и ко то треба да уради (Alcaraz and Zeadally, 2015, p. 69).



Илустрација 7: Процес заштите критичне инфраструктуре (Tagarev and Pavlov, 2007, p. 42)

Под заштитом критичне инфраструктуре могуће је обухватити „све активности које имају за циљ да обезбеде функционалност, континуитет и интегритет критичне инфраструктуре у циљу одвраћања, ублажавања и неутралисања претње, ризика или рањивости“ (Directive 2008/114/EC, 2008, art. 2). Приложена дефиниција важила је на нивоу Европске уније док није установљено да „заштитне мере које се односе само на

[128] Левис сматра да се заштита заснива на принципу 80-20% (Парето прицип), односно 80% заштите критичне инфраструктуре (новца који се улаже) треба да се троши на 20% земље, где тих 20% обухвата најзначајније елементе и услове за земљу (Lewis, 2006, p. 18).

појединачну имовину нису довољне да спрече настанак свих поремећаја због све веће међуповезаности и прекограничне природе". У том правцу, утврђено је да приступ треба преусмерити на јачање отпорности критичних инфраструктура, односно боље уважавање ризика и боље дефинисање улога и дужности релевантних субјеката одговорних за критичне инфраструктуре (Directive (EU) 2022/2557, 2022, Preambule). На нивоу критичног субјекта, субјекта који је одговоран за критичну инфраструктуру, неопходно је преузети одговарајуће и пропорционалне техничке, безбедносне и организационе мере које би обухватиле мере за спречавање настанка инцидената, обезбеђивање адекватне физичке и техничке заштите њихових просторија и критичне инфраструктуре уз процедуре рада; реаговање на последице инцидената, пружање отпора и њихово ублажавање, водећи рачуна о примени процедура и протокола за управљање ризицима и кризним ситуацијама; опоравак од инцидената, узимајући у обзир мере за континуитет пословања и идентификујући алтернативне ланце снабдевања за наставак пружања критичних услуга; обезбеђивање одговарајућег управљања безбедношћу запослених, са провером подобности и едукација релевантног особља кроз курсеве обуке, информативне материјале и вежбе.[129] У ери развоја интернета, све више се говори о сајбер-физичкој безбедности која представља спрегу између рачунске и физичке компоненте система обухватајући бројне апликације од паметних мрежа преко праћења пацијената до интелигентних транспортних система (Li et al., 2012, p. 551).[130]

Заштита критичне инфраструктуре требало би да иде у, најгрубље речено, два правца – развој планова заштите инфраструктуре проактивног карактера и развој акционих планова за одговор на претњу и последице уколико се претња оствари. Друга група би по правилу требало да садржи планове за обезбеђивање континуитета пословања, као и планове за реконструкцију изгубљених ресурса. Како аутори указују, обично су за реаговање у случају инцидента одговорни власници и оператори, док владе заједно са њима раде на идентификацији критичне инфраструктуре и процени њене угрожености. Уз то, све више је заступљена идеја о „глобалној перспективи" заштите критичне инфраструктуре (Pesch-Cronin and Marion, 2017, p. 9). Заштита критичне инфраструктуре треба да буде прозвод заједничког напора владиних агенција, власника инфраструктуре и оператора, као и истраживачке заједнице (Amin, 2000, p. 4). Она треба да обухвати концепте, стратегије, методологије, планове и организације које се баве проактивним деловањем и реаговањем у случају постојања ризика, претњи, или рањивости критичне инфраструктуре на било ком нивоу, било локалном, регионалном, националном или међународном. Ракић закључује да због транснационалног карактера инфраструктура логично произилази постојање транснационалног интереса и високог нивоа сарадње свих битних актера у заштити (2015, стр. 48).

Поменута глобална перспектива заштите критичне инфраструктуре може бити значајан недостатак. Став појединих аутора је да уколико је заштита прекомерно регулисана, национална привреда може изгубити своје конкурентске предности. Код таквог приступа, где је главна одговорност за нормално функционисање инфраструктурена приватним субјектима, оне ће на цену својих производа додати трошкове тако да ће мере заштите инфраструктуре платити купац, односно становништво. Са друге стране, уколико би трошкове сносила влада, онда је могуће повећати конкурентности одређених правних ентитета (Tagarev and Pavlov, 2007, pp. 38-39).

[129] Видети више у: „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" Official Journal of the European Union L, pp. 164–198, 27.12.2022, art. 13.

[130] О сајбер-физичкој безбедности видети више у: International Security Ligue and CoESS. (2023). *Cyber-Physical Security and Critical Infrastructure*. Zollikofen: International Security Ligue; Brussels: CoESS.

Заштиту критичне инфраструктуре можемо посматрати кроз *отпорност* као способност да се издржи и опорави од природног или намерно изазватог поремећаја и *безбедност* у смислу активности и мера за смањење вероватноће и утицаја криминалних и терористичких акција (CoESS, 2016, p. 10). О отпорности је било више речи у ранијем поглављу, када се иста разматрала као један од елемената критичне инфраструктуре. Са друге стране, мере безбедности би на овом месту обухватале скуп физичких, техничких и организационих мера за праћење и заштиту елемената критичне инфраструктуре. Оне треба да обезбеде одвраћање потенцијалних нападача, откривање упада у заштићени објекат, просторе или зоне или откривање настанка опасне ситуације у објекту или у његовој непосредној околини, кашњење кретања нападача и одговор на ометање заштићеног објекта, простора или зоне (Hofreiter and Zvaková, 2017, p. 143).

4.1.4.1. Индекс мера заштите критичне инфраструктуре

Национална лабораторија Аргон (енг. *Argonne National Laboratory*) у сарадњи са Секретаријатом за унутрашњу безбедност САД развила је Индекс мера заштите критичне инфраструктуре (енг. *Protective Measures Index*). Како је главни циљ овог Индекса да измери способност критичне инфраструктуре да се одупре реметилачким догађајима, исти служи и за упоређивање нивоа заштите критичне инфраструктуре иусмеравање одређивања приоритета у контексту коришћења ограничених ресурса за побољшање заштите и смањење рањивости. Индекс мера заштите критичне инфраструктуре обухвата мере које су разврстане у пет категорија (ниво 1), а које се даље рашчлањују на још два нивоа (ниво 2 и ниво 3) (видети Табелу 9). Из приложене табеле, уочиће се да се свака компонента нивоа један рашчлањује на мањи или већи број нижих компоненти, док скоро свака компонента нивоа два садржи мањи или већи број још нижих компоненти које чине ниво три.

Табела 9: Заштитне мере критичне инфраструктуре по нивоима (Petit, Bassett, Buehring et al., 2013)

НИВО 1	**НИВО 2**	**НИВО 3**
Физичка безбедност[131]	Ограде	Тип
		Висина
		База
		Остале карактеристике
		Ограђен простор
	Капије	Капије за возила
		Капије за пешаке
		Капије за железницу
	Систем видео обезбеђења	Монитор
		Снимање
		Одржавање, ажурирања и тестирање
		Технологија
	Систем за откривање упада	Ентеријер
		Екстеријер
	Паркинг	Покривеност
		Непокривеност
	Контрола уласка	Контрола за запослене

[131] Под наведеним мерама подразумева се да постоје одговарајуће контроле за ублажавање ризика које треба да се позабаве физичким рањивостима и да предузму кораке за онемогућавање напада на физички доступне елементе (Radvanovsky and McDougall, 2024, p. 181). О подацима о перформансама карактеристика физичке заштите видети више у: Biringer, Betty, Vugrin, Eric, and Warren, Drake. (2013). *Critical Infrastructure System Security and Resiliency*. Boca Raton: CRC Press, pp. 179-192.

Табела 9: наставак

НИВО 1	НИВО 2	НИВО 3
		Контрола за посетиоце
		Контрола за извођаче радова/добављаче
		Контрола за купце/покровитеље/јавност
	Осветљење	Ограде, капије и паркинг
		Улаз у зграду и подручја испоруке
		Приобална подручја
	Баријере	Баријере за приступ великом брзином
		Баријере за спречавање приступа
	Окружење зграде	Прозори
		Врата
		Зидови
		Плафон/кров
		Вентилација
		Приступ објекту
Безбедносни менаџмент	Менаџер безбедности	/
	Безбедносни план	Карактеристике
		Процедуре
	Безбедносни план комуникације	Комуникација за запослене
		Процедуре за пријављивање
	Сумњиви пакети	/
	Радне групе за безбедност	/
	Осетљиве информације	Руковање осетљивим информацијама
		Безбедносни контејнери
	Провере	/
Безбедносне снаге	Особље	Опште карактеристике
		Ауторитет за хапшење
		Ауторитет за задржавање
		Покривање статичних (контролних) тачака
		Патроле
	Опрема	Униформа
		Наоружање
		Мање смртоносно оружје
		Ограничавање (кретања)
		(Лична) заштитна опрема
		Патрола са псима
		Комуникација
	Обука	Програми
		Учесталост
		Теме
	Налози (процедуре)	/
	Команда и контрола	/
Дељење информација	Агенције	/
	Механизми дељења информација	Механизми
		Меморандуми о разумевању/Споразуми

Табела 9: наставак

НИВО 1	НИВО 2	НИВО 3
Историја/позадина безбедносних активности	Механизми процене претходне рањивости/нове заштитне мере	Спроведена процена претходне рањивости
		Нове заштитне мере или унапређење усвојених и имплементираних у протеклих годину дана
	Додатне заштитне мере	Додатна контрола приступа
		Додатне баријере
		Повећана комуникација и обавештавање
		Повећана сајбер безбедност
		Додатно унапређивање инфраструктуре/развој редундантности
		Унапређен одговор на инциденте
		Додатни мониторинг и надзор
		Иницијација планирања и припремљености

Индекс има своју вредност која се креће између 0 (ниска заштита) и 100 (висока заштита). При чему, висок индекс не значи потпуну заштићеност, као што низак индекс не значи да ће реметилачки догађај аутоматски довести до квара критичне инфраструктуре и до озбиљних последица. Да би се добила укупна вредност, прикупљају се информације за сваки ниво, дакле све компоненте и субкомпоненте Индекса. Информације се прикупљају помоћу питања на које је могуће дати одговор Да (ако је елемент присутан) или Не (ако елемент није присутан). Одговор Да носи вредност 100, док одговор Не носи вредност 0. На основу добијених одговора, рачуна се средња вредност (између 0 и 100).[132] За приказ резултата могуће је користити Алат за испитивање инфраструктуре (енг. *Infrastructure Survey Tool*).

Индекс мера заштите критичне инфраструктуре могуће је користити самостално или у комбинацији са другим индикаторима попут Индекса мерења отпорности и Индекса мерења последица развијених од стране исте лабораторије.

Вредност Индекса мера заштите критичне инфраструктуре, иако има и своје недостатке, на овом месту треба сагледати са аспекта степена развоја у областима управљања ризицима и заштите критичне инфраструктуре. Без обзира на употребу овог индекса за поменути Алат, чије је коришћење иначе ограничено, препознате категорије разрађене у три нивоа нуде могућност даље разраде овог Индекса, али и његову употребу од стране тимова или појединаца чији је задатак заштита критичне инфраструктуре. Како примена овог Индекса захтева уважавање свих специфичних карактеристика за сваки сектор критичне инфраструктуре, делатности и локације, тако постоји простор за његово коришћење у заштити система и објеката који нису окарактерисани као критична инфраструктура. Индекс може да помогне не само за анализу постојећих заштитних мера у објектима, већ и у идентификацији потенцијалних начина за повећање нивоа заштите тих објеката.

Индекс мера заштите критичне инфраструктуре представљен у овом поглављу у основи садржи мере и индикаторе који који ће се у наредном поглављу посматрати у контексту

[132] За детаљнији поступак одређивања вредности Индекса мера заштите критичне инфраструктуре видети више у: Petit, F., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Haffenden, R. A., Klett, M. S., M. S., Phillips, J. A., Veselka, S. N., Wallace, K. E., Whitfield, R. G., and Peerenboom, J. P. (2013). *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability* (No. ANL/DIS-13/04). Argonne: Argonne National Lab (ANL).

безбедности критичне инфраструктуре као другог правца (први правац је отпорност) заштите критичне инфраструктуре. У вези са наведеним, из текста који следи уочиће се веза између мера и индикатора Индекса и мера и активности безбедносног аспекта заштите критичне инфраструктуре.

4.1.4.2. Безбедност као аспект заштите критичне инфраструктуре

Као што је речено, уколико се безбедност критичне инфраструктуре са својим елементима упореди са мерама заштите које су одређене кроз Индекс мера заштите закључује се да је на оба места реч о претежно истим мерама. На овом месту, разрада наведених елемената биће ограничена с обзиром на то да је реч о теми чија би свеобухватна разрада изашла из оквира теме овог рада.[133]

Безбедност критичне инфраструктуре обухвата неколико елемената:

1) служба обезбеђења (физички елемент заштите),
2) механичка средства или баријере (пасивни елемент заштите),
3) електронски системи и средства (активни елемент заштите) и
4) такозване „режимске мере“ (безбедносни менаџмент) (Hofreiter and Zvaková, 2017, p. 142; Vidriková et al., 2017).

Служба обезбеђења овлашћена је да у складу са законском и интерном регулативом врши послове безбедности у штићеном простору или објекту. Она може да буде оформљена у организацији где врши послове безбедности (сопствена), да буде ангажована од професионалних субјеката који пружају услуге безбедности (ангажована) или комбинација наведеног (делимично сопствена, делимично ангажована).

Службеници обезбеђења своје послове врше најчешће уз коришћење техничких система и средстава. Ова лица могу да врше контролу лица, пртљага или превозних средстава при уласку или изласку из објекта и захтевају одређену документацију на увид, изврше идентификацију, одржавају ред, дају информације, наредбе или упозорења, забране лицима улазак или боравак у штићеном простору, привремено задрже лице или привремено одузму предмете када за то постоје одређене околности, врше обилазак простора или објекта у предвиђено време, по потреби да спроводе пратњу кроз штићени простор или објекат, пријављују све неуобичајене догађаје, воде евиденције и извештаје. У току обављања послова заштите, прате индикаторе одређених вредности попут температуре ваздуха, воде, притиска, напона, као и све промене на механичким и електронским средствима заштите која користе у свом раду, те предузимају извесне радње када дође до одступања тренутних вредности или тренутног стања од оних прописаних (нпр. повећана температура ваздуха изнад дозвољене у магацину или активација противпровалног алармног система). Службеници обезбеђења могу бити обучена и за рад са службеним псима, што им омогућава да послове обезбеђења врше са њима. По потреби, могу да обезбеђују место штетног догађаја, да обезбеде евакуацију, да пруже прву помоћ, гасе иницијални пожар.

Службеници обезбеђења јесу обучена и оспособљена лица, лиценцирана за обављање ове врсте делатности према легислативи државе у којој делатност обављају. Најчешће су униформисана, док наоружање зависи од околности конкретног случаја, односно од процене спроведене за конкретно радно место. У раду се придржавају законских и подзаконских прописа који регулишу њихов рад, као и интерних докумената којима се

[133] Видети више у: Vidriková, Dagmar, Boc, Kamil, Dvořák, Zdenek, Řehák, David. (2017). *Critical Infrastructure and Integrated Protection*. Ostrava: The Association of Fire and Safety Engineering; Мандић, Ј. Горан, и Станојевић, Петар. (2020). *Корпоративна безбедност*. Београд: Универзитет у Београду, Факултет безбедности.

уређује њихов рад. За свој рад увек одговарају одређеном лицу (координатор или менаџер безбедности). Професионалним и етичким обављањем ове врсте делатности, службеници обезбеђења доприносе ефикасности интегрисаног система заштите критичне инфраструктуре.

Механичке баријере јесу средства која својим конструкцијским особинама треба да разграниче или дефинишу штићену зону, односно, да спрече, одврате или отежају улазак у штићени простор или приступ штићеном објекту или предмету. У зависности од намене постављају се у неколико кругова заштите:

1) периметар дворишта – ограде (укључујући парапет и додатну, најчешће бодљикаву жицу на врху ограде), капије, непокретни тј. фиксирани стубови као баријера,
2) простор дворишта,
3) периметар објекта – зидови објекта, врата (укључујући браве и друге карактеристике врата попут атрибута противпожарних), прозори (укључујући отпорност на вандализам, ударце, метак или експлозију), сигурносне фолије, решетке, ролетне, роло врата,
4) унутрашњост објекта и
5) заштита предмета – ормари, трезори, касе.

Електронски системи и средства треба обезбеде заштиту штићеног простора, објекта или предмета. Иако делују одвраћајуће, основна намена условљена је њиховом врстом. Електронска средства заштите обухватају:

1) баријере које нису чисто механичке, већ користе као извор напајања струју или батерију – аутоматске капије и аутоматска врата, аутоматске рампе, хидрауличне баријере (аутоматски блокирајући стубићи, аутоматска блокада гума), потапајући стубићи, различите пешачке баријере (периметар дворишта), аутоматска врата, ролетне, роло врата (периметар објекта), електронски ормари, трезори и касе (заштита предмета) и
2) електронске уређаје који имају заштитну намену – уређаји за уништавање докумената, средства за заштиту од индустријске шпијунаже (детекцију и спречавање тајног снимања), уређаји за онемогућавање периферних уређаја рачунарских система (на пример, онемогућавање хардверских килогера), уређаји за заштиту од дронова (ометач дронова, посебно оружје за обарање дронова или беспилотних летелица).

Када је реч о електронским системима, издвајају се:

1) алармни системи – Противпровални алармни систем намењен је за откривање и сигнализирање неовлашћеног покушаја уласка, уласка или присуства у штићеном простору или објекту, односно, приступ штићеном предмету уз сигнализацију тог нежељеног догађаја заинтересованим субјектима. Алармни систем против разбојништва намењен је за сигнализирање нежељеног догађаја заинтересованим субјектима онда када људски фактор активира тај сигнал. Други алармни систем намењени су за детектовање догађаја попут пожара или поплава и сигнализирање таквог догађаја заинтересованим субјектима.
2) систем видео обезбеђења – Системи видео обезбеђења поред одвраћања, у првом реду омогућавају мониторинг или осматрање, снимање (континуирано или у случају детекције), верификацију узрока аларма,
3) систем контроле приступа – Систем контроле приступа спречава неовлашћен улазак у штићени простор или објекат, односно, приступ штићеном предмету. Идентификацијом и ауторизацијом овај систем омогућава улазак овлашћених

лица у штићени простор или објекат, односно, приступ штићеном предмету. Систем контроле приступа могуће је користити и за евиденцију радног времена запослених и

4) систем заштите података и информација - Подразумева софтверску заштиту на нивоу читавог рачунарског и информационог система. Обухвата решења попут антивирусних програма, фајервол система, система за детекцију и спречавање упада у мрежу.

Да би се било који од наведених система користио, претходно је неопходно израдити документе који се захтевају у скаду са прописима државе на чијој територији се постављају и користе, онда планирати, пројектовати и вршити надзор над извођењем система, вршити послове монтаже, пуштања у рад и одржавања система и на крају, спровести обуку корисника.

Режимске мере[134], како их дефинишу Хофрајт и Звакова (Hofreiter and Zvaková) обухватају мере које омогућавају ефикасно функционисање осталих елемената заштите. Оне се могу поделити на:

1) нормативне мере – документи на којима се заснива функционалност осталих елемената заштите (политике, планови, процедуре и упутства) и
2) организационе мере – мере које треба да устроје такву организацију безбедности да апсолутно свака област рада и сви ресурси буду обезбеђени како у нормативном, тако и у организационом смислу.

Дакле, нормативне мере обезбеђују правну основу, док организационе мере обезбеђују организациону основу за предузимање свих мера и активности различитих категорија запослених на пословима безбедности и заштите критичне инфраструктуре.

Нормативне мере треба да обухвате две врсте мера. Једна врста се односи на документа чије је доношење обавезно у складу са прописима државе на чијој територији се послује, док се друга врста односи на документа која нису прописана законским одредбама али су неопходна са оптимално функционисање интегрисаног система безбедности. Нека од ових докумената су следећа: процена ризика, свеукупни безбедносни план или издвојен план за ванредне догађаје и план континуитета пословања, услови понашања и рада свих запослених, услови понашања и рада службеника обезбеђења, услови коришћења механичких средстава, услови коришћења електронских средстава и система, услови издавања и коришћења кључева (лозинки) и других медија за контролу приступа, услови уласка и изласка лица, возила и њихово кретање унутар објекта, услови реализације посета и понашања лица, спискови и спецификације механичких средстава, електронских средстава и система који се користе у објекту са пропратном техничком документацијом и евиденцијама сервисирања и кварова.

Период током пандемије Ковида-19, указао је на то да безбедност критичне инфраструктуре треба обезбедити и под околностима које нису уобичајене. У вези са тим, подвлачи се потреба да се процедуре рада правовремено и без одлагања прилагоде новонасталој ситуацији, те по потреби и усвоје нове како би се задовољили захтеви за безбедношћу. Група аутора поставља оправдано питање „Да ли су куће које су државни службеници користили за обраду информација током периода рада од куће стављене под исти ниво контроле“ (који уживају њихове пословне канцеларије)? (Radvanovsky and McDougall, 2024, p. 178).

Организационе мере, како је већ наведено, обухватају мере којима се обезбеђује организација безбедности у штићеном простору или објекту. Организација сектора

[134] Режимске мере могуће је поистоветити са безбедносним менаџментом, конкретно у корпоративној безбедности, који представља менаџмент као начин организовања и управљања корпоративном безбедношћу у правном лицу.

безбедности као посебне целине, организација послова безбедности, и посебно, организација службе обезбеђења (број контролних тачака, време покривености контролних тачака, број службеника, радно времене/трајање смена, опрему и средства која користе, процедуре рада).

Значајан сегмент режимских мера јесте едукација у вези са пословима безбедности. Едукација треба да обухвати апсолутно све запослене. Свакако, један правац едукације би био намењен за све запослене без обзира на њихово радно место и позицију, док би други правац едукације био намењен запосленима на пословима безбедности.

4.1.4.3. Заштита критичне инфраструктуре као елемент тоталне одбране

У контексту тоталне одбране, критична инфраструктура игра кључну улогу у обезбеђивању отпорности друштва и континуитета пружања основних услуга и производа током периода кризе или сукоба. Тотална одбрана јесте приступ читавог друштва којим се обезбеђује отпорност и спремност за суочавање не само са ратом и ванредним стањем, већ и са елементарним непогодама. У такав концепт укључени су поред војске и полиције и цивилне службе, приватни сектор и општа популација (Milosavljević and Štrbac, 2024, pp. 46-47), односно оружане снаге, друге државне снаге безбедности, организације цивилног друштва, приватни сектор и појединци (Живановић и Радојевић, 2024, стр. 167).

Отпорност друштва све више „игра улогу“ у функционисању система одбране и националне безбедности. Отпорност друштва једним делом се постиже јачањем отпорности критичне инфраструктуре као основе функционисања државе и друштва како у мирнодопским условима, условима ванредне ситуације, тако и условима ратног или ванредног стања. Како је о отпорности критичне инфраструктуре раније писано, отпорност друштва у целини „почива на вољи и способности да се издрже спољни притисци и утицаји и/или опорави од ефеката тих притисака или утицаја“ (Милковски и Божић, 2023, стр. 21).

Заштита критичне инфраструктуре препозната је као један од елемената цивилне димензије тоталне одбране (Milosavljević and Štrbac, 2024, p. 50). Цивилна димензија тоталне одбране или само цивилна одбрана постала је значајна у концепту тоталне одбране онда када су ратови и борбена дејства избрисала разлику између војника и цивила. То се десило са првим „тоталним ратом“, односно Другим светским ратом када се због „подједнаке изложености ратним сукобима како војних циљева тако и цивилних објеката и инфраструктуре и читаве животне средине“ закључило да на тотални рат треба одговорити тоталном одбраном (Живановић и Радојевић, 2024, стр. 168).

Цивилна одбрана међутим не игра важу улогу само током рата, већ и у случајевима криза и ванредних ситуација. Систем цивилне одбране „организује се, припрема и делује у рату и свим кризним ситуацијама у миру на заштити, безбедности и одбрани цивилног становништва, привреде, материјалних и културних добара и у заштити животне средине“ (Јовић, 2000, стр. 50). Цивилна одбрана је стога постала важан чинилац безбедности и отпорности под различитим околностима. Односно с обзиром на директно учешће цивилног друштва, критична инфраструктура и отпорност друштва постали су витални део тоталне одбране (Sellevåg, 2022).

„Јачање отпорности, посебно система одбране и критичне инфраструктуре, важан је фактор одвраћања“ наводи се у Белој књизи одбране Републике Србије.[135] Даље, наводи се да је „изградња отпорности друштва, државе и грађана на испољене претње

[135] НАТО је 2016. године усвојио друштвену отпорност као интегрални елемент одвраћања и као део опредељења за јачање отпорности (NATO Summit Guide, 2016).

безбедности, као способности да наставе функционисање у неповољним условима“ посебно значајно у припреми и извођењу тоталне одбране (Почуч, 2023, стр. 32). Тотална одбрана „обухвата војну и цивилну одбрану, а планира се, организује и спроводи у миру, ванредном стању и рату“ као „свеобухватни одговор система одбране на изазове, ризике и претње безбедности значајне за одбрану Републике Србије“ (Стратегија одбране, 2019, 5). Република Србија је концепт тоталне одбране усвојила кроз Стратегију одбране 2009. године, а опредељење за овај концепт потврдила је и тренутно актуелном Стратегијом националне безбедности (увод) и Стратегијом одбране (глава 5). Стратешким документима концепт тоталне одбране није образложен, нити је објашњено шта ће значити у пракси[136], иако овај концепт није новина на нашим просторима. Наиме, Југославија је била једна од држава које су имале имплементиран концепт тоталне одбране, поред Финске, Шведске, Швајцарске и Аустрије у Европи (Stein, 1990, p. 17).[137] Она је операционализовала овај концепт кроз општенародну одбрану и друштвену самозаштиту од средине седамдесетих година прошлог века усвајањем Устава 1974. године.[138] Југославија је међутим била и пример где је укупни систем одбране постао нефункционалан у ситуацији растућег национализма и републичких тежњи за независношћу (Dulić and Kostić, 2010, 1065). Концепт је „живео“ док је било Комунистичке партије Југославије, док је „живео“ Јосип Броз Тито.[139] Тако, случај Југославије као мултиетничке земље показао је да је социјална кохезија дефинитиван предуслов да потпуна или свеобухватна одбрана буде ефикасна, а не да постане претња друштву (Berzina, 2020, p. 4).

У Финској је рецимо из концепта тоталне одбране развијен концепт свеобухватне безбедности. Познатији као „модел свеобухватне безбедности“ (енг. *model for comprehensive security*) реч је о моделу приправности заснованом на сарадњи, у којем виталним функцијама друштва заједнички управљају власти, пословни субјекти, организације и грађани (Security Committee, 2017, p. 7). Добра страна овог модела лежи у чињеници да обухвата све нивое и актере друштва. Власт и јавна управа, универзитети и истраживачке институције играју централну улогу у изради нацрта закона и других аката, управљању и развоју, као и у имплементацији прописаних мера. Пословни субјекти обезбеђују функционисање привреде и инфраструктуре планирајући и континуирано функционисање у случају ометања рада, као и социјалну и здравствену заштиту. Организације (као и уговорна тела и волонтерски сектор) играју важну улогу у припреми за несреће и поремећаје пружајући подршку властима кроз обучавање или организовање грађана. Активни грађани су још један значајан субјекат. Они се кроз сопствени избор и рад поседујући знања и вештине одлучују да учествују и помогну када је то потребно било као појединци било као организоване групе (Security Committee, 2017, pp. 7-8). Сви ови субјекти, иако са различитим улогама, доприносе јачању отпорности друштва. У стратегији која одређује концепт свеобухватне безбедности

[136] Милосављевић указује на још неке проблеме попут потребе за обученошћу ширег друштва за адекватно реаговање у ванредним ситуацијама, адекватних материјално-техничких и инфраструктурних капацитета, економског потецијала, као и демографске структуре становништва који тренутно не иду у прилог развоју и примени овог концепта (2019, стр. 312).

[137] Концепт тоталне одбране од европских држава данас примењују Швајцарска, Шведска, Србија и балтичке државе (Đukić i Vuletić, 2023, str. 625).

[138] Општенародна одбрана и друштвена самозаштита два су концепта која су се узајамно развијала и међусобно допуњавала. Основна разлика огледа се у објекту заштите. Друштвеном самозаштитом штите се уставни поредак и основне друштвене вредности од претежно унутрашњих облика угрожавања, док се општенародном одбраном штити и брани независност, суверенитет, територијални интегритет од претежно спољашњих облика угрожавања (нпр. случај непосредне ратне опасности или оружане агресије) (Simić i Arnautović, 1987, str. 21).

[139] О развоју концепта видети више у, на пример: Поточар, Стане (1974). Концепција општенародне одбране – резултати и задаци. *Војно дело* 2, стр. 5-26.

посебан део одвојен је за критичне индустрије и услуге. Фокус ставља на производњу која је критична (круцијална) за снабдевања, оперативне предуслове извозне индустрије, способност одржавања и поправке одбрамбеног материјала и система, хитно складиштење критичних сировина, компоненти и других производних инпута, обезбеђивање неометаног партнерства између приватног и јавног сектора, као и међународне економске сарадње (Security Committee, 2017, p. 78). За реализовање ових задатака предвиђени су, између осталог, развој управљања континуитетом посебно у снадбевању, надлежности над управљањем и координацијом, развој комуникације и сарадње између кључних актера (Security Committee, 2017, p. 78). У Финској, адекватна заштита критичне инфраструктуре остварује се сарадњом цивилног становништва, пословне заједнице и Владе. Анализирајући елементе овог модела и начин на који организује свеукупну безбедност, постоји простор да се управо овај модел узме као основ развоја онога што се назива „тотална одбрана".

Сумирано, критичну инфраструктуру могуће је посматрати као темељ концепта тоталне одбране. Критична инфраструктура подржава војне операције, обезбеђује основне потребе током криза, чиме уједно осигурава отпорност цивила и ширу отпорност друштва. Последично, заштита критичне инфраструктуре доприноси националној безбедности и друштвеном благостању.

4.2. Критична инфраструктура и њена заштита у Републици Србији

Република Србија до 2018. године није имала закон који је уређивао питања критичне инфраструктуре. Најближе што је Република Србија била на путу правног регулисања ове области били су Закон о ванредним ситуацијама и Уредба о садржају и начину израде планова заштите и спасавања у ванредним ситуацијама, која је донета на основу овог Закона. Овом Уредбом први пут се, 2011. године, у правни систем наше државе уводи појам критичне инфраструктуре, али само са аспекта њене процене са становишта елементарних непогода и других већих несрећа (Уредба о садржају и начину израде планова заштите и спасавања у ванредним ситуацијама, члан 8). Корак више учињен је усвајањем Упутства о Методологији за израду процене угрожености од елементарних непогода и других несрећа и планова заштите испасавања у ванредним ситуацијама. Иако су Упутством дефинисани „објекти и друга инфраструктура од посебног значаја (критична инфраструктура), област критичне инфраструктуре у Републици Србији није још увек била законски уређена. Први секторски закон у области критичне инфраструктуре и њене заштите, Закон о критичној инфраструктури ступио је на снагу 2018. године. Њиме је успостављен нормативни оквир за дефинисање, идентификацију, одређивање и заштиту националне и европске критичне инфраструктуре. На основу овог закона, 2022. године усвојена је Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије, која је заменила Уредбу о ближим критеријумима за одређивање обавезно обезбеђених објеката и начину вршења послова њихове заштите из 2016. године.

4.2.1. Развој заштите критичне инфраструктуре у Републици Србији

Појам критичне инфраструктуре у Републици Србији ушао је у употребу релативно касно и као последица његове употребе на Западу. Системи и објекти критичне инфраструктуре нису ништа друго него системи и објекти од виталног значаја за државу и друштво. Раније, пре увођења појма критичне инфраструктуре, говорило се о

објектима од посебног интреса или значаја за одбрану земље или о великим техничким системима. Данас, када се говори о критичној инфраструктури не прави се грешка када се она посматра као еквивалент овим великим техничким системима, односно објектима од посебног (интреса) значаја. Узимајући у обзир наведено, развој заштите критичне инфраструктуре могуће је пратити само преко заштите објеката од посебног (интреса) значаја.

Да би се поткрепила изнета тврдња наводи се следеће: „Предузећа и друга правна лица која производе предмете и врше услуге од посебног интереса за одбрану земље, за Војску Југославије, јединице и органе унутрашњих послова, државне органе, цивилну одбрану, цивилну заштиту, предузећа, становништво и друге приоритете у случају ратног стања, непосредне ратне опасности или ванредног стања, дужни су да у миру планирају мере којима обезбеђују вршење те производње и услуга, снабдевање сировинама, репроматеријалом, енергијом и другим потребама …“ (Закон о одбрани, 1994, члан 31). У једној од наредних одредаба, посебно се апострофирају велики технички системи у области веза, информатике, ваздушног и железничког саобраћаја, електроенергетике, водоснабдевања и другим областима од интереса за одбрану земље (Закон о одбрани, 1994, члан 36). Подзаконским актом, Одлуком о одређивању великих техничких система од интереса за одбрану земље, прецизирају се предузећа која се сматрају великим техничким системима. На основу изнете одредбе из члана 31 произилази да наведена предузећа и друга правна лица функционишу у миру само како би обезбедили предмете и услуге за потребе одбране, док се потпуно занемарује њихово функционисање у миру, а за потребе државе и становништва у мирнодопском стању. Зато се поставља питање функционисања ових правних лица и за потребе у миру. Са тим у вези, нормативно је уређено обављање делатности од општег интереса у које се убрајају делатности области: производње, преноса и дистрибуције електричне енергије; производње и прераде угља; истраживања, производње, прераде, транспорта и дистрибуције нафте и природног и течног гаса; промета нафте и нафтних деривата; железничког, поштанског и ваздушног саобраћаја; телекомуникација; издавања службеног гласила Републике Србије; информисања; издавања уџбеника; коришћења, управљања, заштите и унапређивања добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач), као и комуналне делатности. Све наведене делатности сматрале су се делатностима од стратешког значаја, као и делатности неопходне за рад државних органа и органа јединице локалне самоуправе (Закон о јавним предузећима и обављању делатности од општег интереса, 2000, члан 2).[140]

У привредним системима попут објеката и система критичне инфраструктуре постојала је такозвана индустријска милиција, која је била у саставу Народне милиције и под њеном контролом. Она је имала задатак да осигурава спољну безбедност правних лица (од диверзија, паљевине, разбојништва, крађа) и унутрашњу безбедност (превасходно ради разоткривања саботажа, диверзија, шпијунаже) (Даничић и Стајић, 2008, стр. 89). Како је средином педесетих година прошлог века дошло до расформирања Индустријске милиције, сви привредни системи су остали незаштићени. 1963. године донет је Правилник о служби за обезбеђење имовине привредних организација и других установа, којим је требало решити питање обезбеђивања привредних система (Кешетовић и Симоновић, 2009, стр.

[140] По тренутно важећем Закону о јавним предузећима, у основне делатности убрајају се делатности у области: рударства и енергетике, саобраћаја, електронских комуникација, издавања службеног гласила Републике Србије и издавања уџбеника, нуклеарних објеката, наоружања и војне опреме, коришћења, управљања, заштите, уређивања и унапређивања добара од општег интереса и добара у општој употреби (воде, путеви, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја и др.), управљања отпадом, комуналне делатности и другим областима (2016, члан 2).

149). Међутим, како је исти важио тек неколико година, ова област добија своју регулативу тек седамдесетих година увођењем система друштвене самозаштите.

Република Србија некада је познавала систем друштвене самозаштите, и као теоријски концепт и као једну од бољих пракси које је имала у погледу заштите. Правни основ система друштвене самозаштите произилазио је из Устава СФРЈ, устава и закона република и покрајина. Од закона, за територију (Савезне Републике) Србије од значаја су били Закон о основама друштвене самозаштите, Сл. гласник РС, бр. 39/73, а касније Закон о систему друштвене самозаштите, Сл. гласник РС, бр. 14/86, по којима је свако предузеће (правно лице) било у обавези да има успостављену и организовану службу заштите.

Наиме, Бакић као стварне основе за изградњу друштвене самозаштите наводи појаву одумирања државе, подруштвљавање државних активности, конституисање и проширивање самоуправних права радних људи кроз доношење Закона о предаји привредних предузећа на управљање радним колективима још у јулу 1950. године (1976а, стр. 23). Новоформирани друштвени односи довели су до подруштвљавања послова безбедности и заштите, односно стварања новог облика самоуправљања у домену безбедности и заштите друштва (Najman, 1979, str. 36). Тај процес се састоји у томе што га „стварају радни људи и грађани као основни носиоци друштвене самозаштите организовани у самоуправне субјекте“; кроз њега се „реализују послови безбедности и заштите друштва као свакодневни послови радних људи и грађана које они остварују уз рад и кроз рад“ и могуће га је „остварити једино уз примену метода самоуправне свести и добровољности и њему адекватних мера“ (Najman, 1979, str. 38).

Оваквим процесом, послови безбедности и заштите изашли су изван строгих оквира власти и постали су ствар која „се тиче“ свих субјеката самоуправних друштвених односа. Другим речима, „самоуправни субјекти подруштвљују послове осигурања спољне и унутрашње безбедности предупређивања контрареволуције и сузбијања свих облика социјалне патологије чиме се доприноси жељеној стабилности социјалистичке самоуправне земље“ (Najman, 1979, str. 40).

Дакле, носиоци друштвене самозаштите били су грађани, а првенствено радни људи. Они су своју функцију остваривали превасходно кроз асоцијације у које су се удруживали ради остваривања друштвених, радних активности. То су у првом реду организације удруженог рада, друштвено-политичке заједнице и друштвено-политичке организације, организације општенародне одбране, месне заједнице. Односно субјекте друштвене самозаштите могуће је поделити на класичне и самоуправне, где се у прву групу убрајају судови, тужилаштва, правобранилац, Секретаријат унутрашњих послова, инспекције, Служба друштвеног књиговодства, царина; док се у другу групу убрајају организације удруженог рада, месне заједнице, Самоуправна интересна заједница, организације од посебног значаја за друштвену самозаштиту, аеродроми (Najman, 1979, str. 33).

Устав СФРЈ одређивао је друштвену самозаштиту као „функцију самоуправног друштва, остварује се активностима радних људи, грађана, организација удруженог рада и других самоуправних организација и заједница, друштвенополитичких и других организација и друштвено-политичких заједница, ради заштите уставног уређења самоуправних права радних људи и других права и слобода човека и грађанина, ради заштите друштвене имовине, обезбеђивања личне и имовинске сигурности радних људи и грађана и ради слободног друштвеног развоја“ (Устав СФРЈ, 1974). Уопштено, реч је о „систему повезаних и складних активности свих организованих социјалистичких снага у заштити основних принципа, институција и вредности југословенског социјалистичког самоуправног друштва“ (Бакић, 1976б, стр. 50).

У циљу остваривања заштите свих вредности друштва, а посебно самоуправљања и друштвене имовине запослени су предузимали следеће мере: непосредне мере заштите

од свих облика непријатељског деловања, других друштвено – штетних појава и понашања као и свих облика и метода специјалног рата; заштите самоуправних права, друштвеног уређења и интереса радника од свих врста угрожавања; заштите друштвене имовине од неодговорног и неправилног коришћења, противправног присвајања и отуђивања расипништва, „корисних малверзација" и разних оштећења, упропашћивања и саботажа; заштите удруженог рада од свих облика несавесног пословања, нелојалне конкуренције, мита, корупције, злоупотреба, нарушавања пословног морала и других друштвено штетних појава; против сваког облика нарушавања радних обавеза, несавесног извршавања радних задатака и других неодговорних понашања у раду; мере чувања и заштите државне, војне, службене и пословне тајне и организовање и спровођење мера заштите од пожара и експлозија, елементарних непогода, угрожавања човекове радне средине и других опасности и несрећа (Simić i Arnautović, 1987, str. 23). Свеукупни систем друштвене самозаштите у предузећима (правним лицима) састојао се од неколико елемената: права, дужности и одговорности радних људи; права, дужности, одговорности и начин рада самоуправних и стручних органа и организација; заштита друштвене имовине и свих материјалних добара; заштита свих тајних података; заштита радних места; заштита на раду; заштита од пожара; заштита од елементарних непогода и других несрећа и заштита угрожавања човекове радне средине (Simić i Arnautović, 1987, str. 24).[141] Наведене мере или елементи поменутог система значајни су јер се у њима препознаје оно што данас обухвата корпоративна безбедност као заштитна функција правног лица. Нарочито, и тада је још била препозната физичко-техничка заштита људи и друштвене имовине преко које је систем друштвене самозаштите у предузећима (правним лицима) спроводио своју функцију. Ова заштита, обухватала је следеће активности: чување зграда, постројења и друге имовине; спречавање и откривање појава које могу нанети штету имовини; онемогућавање приступа непознатим лицима у зграде, постројења и друге просторе, које треба штитити; неометан процес рада и заштиту радника.

Ступањем на снагу Закона о престанку важења одређених закона и других прописа, Сл. гласник РС, бр. 18/93, престао је да важи и Закон о систему друштвене самозаштите. Тада је Република Србија остала без, по многима, веома добро осмишљеног и организованог, система друштвене самозаштите. Усвајањем Закона о приватном обезбеђењу, 2013. године, члановима 4 и 5, уређена је област заштите (обавезно обезбеђених) објеката. Правни основ за обезбеђење објеката од виталног значаја за државу и друштво били су законски и подзаконски прописи из области одбране. Поред Закона о одбрани који ће бити наведен касније, издвајају се следећи подзаконски акти, сви тренутно важећи, а кључни за разумевање развоја заштите критичне инфраструктуре:

- Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије, Сл. гласник РС, бр. 18/1992
- Уредба о критеријумима за утврђивање података значајних за одбрану земље који се морају чувати као државна или службена тајна и о утврђивању задатака и послова од посебног значаја за одбрану земље које треба штитити применом посебних мера безбедности, Сл. лист СРЈ, бр. 54/94 и Сл. гласник РС, бр. 88/2009, 111/2009. *Следбеник и тренутно важећа:* Уредба о подацима и пословима значајним за систем одбране који се морају чувати и штитити у складу са законом којим се уређује заштита тајности података и о критеријумима за попуну радних места на којима се ти задаци и послови обављају, Сл. гласник РС, бр. 8/2020

[141] Видети више у: Najman, Velizir. (1979). *Uređivanje društvene samozaštite: zakonodavstvo, teorija, praksa*. Šabac: Dragan Srnić.

- Одлука о одређивању војних и других објеката и рејона који су забрањени за осматрање, снимање и приступ и о мерама за њихову заштиту, Сл. лист СРЈ, бр. 11/1996, 42/2005
- Одлука о одређивању великих техничких система од интереса за одбрану земље, Сл. лист СРЈ, бр. 54/94, 58/94, 65/94, 10/97. *Следбеник и тренутно важећа:* Одлука о одређивању великих техничких система од значаја за одбрану, Сл. гласник РС, бр. 41/2014, 35/2015, 86/2016, 53/2017, 26/2019, 94/2019, 67/2021, 62/2022
- Одлука о одређивању производа и услуга од посебног интереса за одбрану земље, Сл. лист СРЈ, бр. 43/94, 28/96. *Следбеник и тренутно важећа:* Одлука о одређивању производа и услуга од посебног значаја за одбрану Републике Србије, Сл. гласник РС, бр. 58/2008, 26/2019.
- Одлука о објектима од посебног значаја за одбрану, Сл. гласник РС, бр. 112/2008

Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије, Сл. гласник РС, бр. 18/1992 из 1992. године. У складу са овом уредбом, објектима од посебног значаја за одбрану Републике Србије 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 Републике, док се рејонима за одбрану од посебног значаја за одбрану Републике сматрају подручја у непосредној близини објекта од посебног значаја за одбрану (Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије, члан 1). Реч је о објектима у области саобраћаја, телекомуникације, енергетике, водопривреде, индустрије, млинови, складишта за чување различитих добара, болнице, објекти за производњу лекова и других фармацеутских средстава и одређени објекти и заштићена природна добра у области заштите животне средине (Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије, члан 2). Безбедност ових објекта обухвата организовање и спровођење мера за његову заштиту од оштећења или уништења, односно откривања тајних података о објекту или самог објекта-локације (Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије, члан 7). Мере које се спроводе су: контролисање лица и возила при уласку и изласку из објекта; постављање знакова забране приступа, осматрања и снимања осим код објеката чија се локација чува у тајности; утврђивање посебне мере заштите у односима са странцима и утврђивање посебних дужности радника физичког обезбеђења у предузимању мера према лицима затеченим у недозвољеном приступу, осматрању и снимању објекта (Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије, члан 8).

Уредба о критеријумима за утврђивање података значајних за одбрану земље који се морају чувати као државна или службена тајна и о утврђивању задатака и послова од посебног значаја за одбрану земље које треба штитити применом посебних мера безбедности, Сл. лист СРЈ, бр. 54/94 и Сл. гласник РС, бр. 88/2009, 111/2009 из 1994. године. Правни следбеник ове уредбе јесте *Уредба о подацима и пословима значајним за систем одбране који се морају чувати и штитити у складу са законом којим се уређује заштита тајности података и о критеријумима за попуну радних места на којима се ти задаци и послови обављају, Сл. гласник РС, бр. 8/2020* из 2020. године, која препознајуе непходност да се подаци о војним објектима и објектима који су одлуком надлежног органа одређени као објекти од посебног значаја за одбрану земље (локација, назив, структура, опремљеност и други подаци који би у ратном и ванредном стању били од посебног значаја за одбрану земље) чувају и штите као тајни подаци (члан 2). Свеукупна заштита било ког објекта нужно укључује и заштиту података и информација које су од круцијалне важности за објекат, његова лица, имовину и пословање. С обзиром на степен важности одређених података за, у овом случају, објекте од посебног значаја за одбрану

земље намеће се нужност њихове заштите на највишем могућем нивоу. Даље, то само значи да одређени подаци за све објекте од посебног значаја за земљу уопште заслужују и требају заштиту на највишем нивоу.

Одлука о одређивању војних и других објеката и рејона који су забрањени за осматрање, снимање и приступ и о мерама за њихову заштиту, Сл. лист СРЈ, бр. 11/1996, 42/2005 из 1996. године. У складу са овом одлуком објекти од посебног значаја за одбрану земље су: објекти или делови објеката у којима су смештени велики технички системи, предузећа и друга правна лица од посебног интереса за одбрану земље; објекти у којима се производе, складиште или чувају предмети или врше услуге од посебног значаја за одбрану земље; инвестициони објекти значајни за одбрану земље (Одлука о одређивању војних и других објеката и рејона који су забрањени за осматрање, снимање и приступ и о мерама за њихову заштиту, члан 3). Као мере заштите (мере физичког обезбеђења, мере техничке заштите, опште мере безбедности и мере контраобавештајне службе) наводе се: примена најпогоднијег начина физичког обезбеђења објеката, дела објеката и рејона објеката (стражари, чувари, патроле, осматрачи, заседе, коришћење паса чувара, групе за интервенцију, дежурни и контролни органи, погодна лица која су настањена у близини објекта) и других мера за спољно обезбеђење објекта; примена електронских и других уређаја за осматрање, контролу и заштиту објеката и рејона објекта; постављање ограде и других сличних препрека ради онемогућавања приступа објекту и рејону објекта; изградња прилазних путева објекту и постављање одговарајућих рампи; постављање знака забране осматрања, снимања и приступа и саобраћајних знакова забране; маскирање објекта од осматрања са земље и из ваздуха, посебно кад је у питању објекат чија се локација чува у тајности и примена мера легендирања и дезинформисања; забрана уношења у објекат, односно део објекта и рејон објекта средстава за снимање (фото–апарати, фото–кино, ТВ и видео камере, камкордери и мобилни телефони), експлозива и слично, без одобрења старешине надлежне војне команде, односно овлашћеног лица надлежног органа; избор лица за рад у објекту и за његово обезбеђење; регулисање приступа објекту, делу објекта и рејону објеката, функционисање пријавница, издавање пропусница, евиденција посета и предузимање других мера ради обезбеђења прописаног режима кретања у објекту и рејону објекта; контрола лица и возила при уласку и изласку из објекта, односно која се нађу у рејону објекта; стална безбедносна обука и информисање лица запослених у објекту или задужених за његово обезбеђење; заштита техничке и друге документације која се односи на објекат у складу са прописима о заштити тајности; контрола спровођења прописаних и наређених мера заштите, реда и режима у објекту, делу објекта и рејону објекта и друге потребне и прописане мере (Одлука о одређивању војних и других објеката и рејона који су забрањени за осматрање, снимање и приступ и о мерама за њихову заштиту, члан 5).

Одлука о одређивању великих техничких система од интереса за одбрану земље, Сл. лист СРЈ, бр. 54/94, 58/94, 65/94, 10/97 из 1994. године. Правни следбеник ове одлуке јесте Одлука о одређивању великих техничких система од значаја за одбрану, Сл. гласник РС, бр. 15/09, 54/10, 4/11, 58/11, односно *Одлука о одређивању великих техничких система од значаја за одбрану, Сл. гласник РС, бр. 41/2014, 35/2015, 86/2016, 53/2017, 26/2019, 94/2019, 67/2021, 62/2022*. Овом одлуком одређују се велики технички системи од значаја за одбрану и пратећа техничка средства. Тако, у ресурсе критичне инфраструктуре укључено је четири велика техничка система из области телекомуникација, осам из области саобраћаја, седам из области енергетике, седам из области водоснадбевања и пет из других области (радиодифузије, производња и промет гасова и пратеће опреме, газдовања шумама) (Одлука о одређивању великих техничких система од значаја за одбрану, члан 3). Ови велики технички системи нису ништа друго

него инфраструктура која обезбеђује виталне услуге друштву и као таква има атрибут критичне. Реч је о правним лицима:

1) у области телекомуникација: Предузеће за телекомуникације „Телеком Србија" акционарско друштво, Београд; Yettel d.o.o. Beograd; CETIN d.o.o. Beograd – Novi Beograd и Al Srbija d.o.o. Beograd;
2) у области саобраћаја: Akcionarsko društvo za vazdušni saobraćaj Air SERBIA, Beograd; BELGRADE AIRPORT d.o.o. Beograd; Контрола летења Србије и Црне Горе SMATSA д.о.о., Београд; Јавно предузеће „Пошта Србије", Београд и Акционарско друштво „Железнице Србије", Београд; Акционарско друштво за железнички превоз путника 'Србија Воз', Београд; Акционарско друштво за железнички превоз робе 'Србија Карго', Београд и Акционарско друштво за управљање јавном железничком инфраструктуром 'Инфраструктура железнице Србије', Београд;
3) у области енергетике: Акционарско друштво „Електропривреда Србије", Београд са зависним привредним друштвима; „Електродистрибуција Србије" д.о.о. Београд; Акционарско друштво 'Електромрежа Србије', Београд; „НИС" а.д., Нови Сад и његова зависна привредна друштва; Јавно предузеће „Србијагас", Нови Сад; Друштво за производњу уља Рафинерија нафте акционарско друштво, Београд; и ТРАНСНАФТА АД Панчево;
4) у области водоснабдевања: Јавно водопривредно предузеће „Србијаводе", Београд; Јавно водопривредно предузеће „Воде Војводине", Нови Сад; Јавно комунално предузеће „Београдски водовод и канализација", Београд; Јавно предузеће за водоснабдевање „Рзав", Ариље; Јавно комунално предузеће за водовод и канализацију „NAISSUS", Ниш; Јавно предузеће за водоснабдевање и за производњу и дистрибуцију електричне енергије „Ибар", Зубин поток и Јавно комунално предузеће „Водовод и канализација", Нови Сад;
5) у другим областима: Јавна медијска установа Радио-телевизија Србије, Београд; Јавно предузеће „Емисиона техника и везе", Београд; „Messer Tehnogas" акционарско друштво за производњу и промет техничких и медицинских гасова и пратеће опреме, Београд; Јавно предузеће за газдовање шумама „Србијашуме" са потпуном одговорношћу, Београд и Јавно предузеће „Војводинашуме", Петроварадин.

Одлука о одређивању производа и услуга од посебног интереса за одбрану земље, Сл. лист СРЈ, бр. 43/94, 28/96 из 1994. године. Правни следбеник ове одлуке јесте Одлука о одређивању производа и услуга од посебног интереса за одбрану земље, Сл. лист СЦГ, бр. 13/06, односно *Одлука о одређивању производа и услуга од посебног значаја за одбрану Републике Србије, Сл. гласник РС, бр. 58/2008, 26/2019.* Овом одлуком одређују се производи и услуге од посебног значаја за одбрану Републике Србије. Без навођења свих производа и услуга који припадају наведеној врсти, значај ове одлуке огледа се у томе што су и производи и услуге препознати као критични, што указује још једном да објекат заштите није довољно да буду само физички системи и објекти (инфраструктура), већ и производи и услуге које та инфраструктура обезбеђује.

Одлука о објектима од посебног значаја за одбрану, Сл. гласник РС, бр. 112/2008 из 2008. године. Овом одлуком су таксативно одређени објекти од посебног значаја за одбрану и то за сваку врсту појединачно. У овој Одлуци дат је детаљан приказ објеката од посебног значаја за одбрану. Поред објеката који су одређени матичним законом, а то су: велики техничко-технолошки системи, објекти у којима се производе, складиште или чувају предмети или врше услуге за потребе одбране, објекти у којима су смештени државни органи и правна лица од посебног значаја за одбрану земље, као и одређени инфраструктурни објекти, обухваћени су и објекти у којима је седиште правног лица које

је одређено актом надлежног органа као правно лице од посебног значаја за одбрану и склоништа и други јавни објекти намењени за заштиту људи и материјалних добара и заштиту животне средине (Одлука о објектима од посебног значаја за одбрану, члан 2). Безбедност ових објеката обухвата организовање и спровођење мера за њихову заштиту од оштећења или уништења, односно откривања тајних података о објектима или самих објеката, односно њихових локација, а мере заштите одређују се посебним прописом (Одлука о објектима од посебног значаја за одбрану, члан 4).

4.2.2. Нормативни оквир заштите критичне инфраструктуре у Републици Србији – тренутно стање

По питању нормативне уређености области критичне инфраструктуре у Републици Србији, треба поћи од највиших правних прописа. Највиши акт у области заштите критичне инфраструктуре требало би да буде документ који има стратешку вредност. Међутим, у Републици Србији, такав документ у виду стратегије заштите критичне инфраструктуре не постоји, већ је кровни документ у овој области Закон о критичној инфраструктури. Стратегија националне безбедности бива и остаје највиши политичко-безбедносни документ, односно највиши стратешки документ у области националне безбедности и индиректно у области заштите критичне инфраструктуре.

Стратегија националне безбедности Републике Србије, Сл. гласник РС, бр. 94/2019 не садржи децидне одредбе о одређењу, идентификацији или заштити критичне инфраструктуре, већ укључује само неколико одредби које се односе на ову тему. Реч је о одредбама чији редослед на овом месту одговара редоследу у поменутој Стратегији: 1) потреби за појачаном заштитом критичне енергетске инфраструктуре услед повећаног броја сукоба изазваних надметањем за обезбеђење енергената и других природних сировина, питке воде и хране која би чак укључила и употребу војних снага; 2) опасности од напада на критичну инфраструктуру услед глобалног развоја информационих технологија и интензивирања активности у сајбер простору (видети део 1. Стратегије); 3) идентификовању и заштити објеката критичне инфраструктуре и спровођењу мера раног упозорења и превентивног реаговања у вези са очувањем унутрашње стабилности и безбедности Републике Србије и њених грађана (видети део 4.2. Стратегије); 4) јачању регионалне стабилности, унапређењу развоја и повезивања кроз инфраструктуру (видети део 4.4. Стратегије), 5) унапређењу појединих сегмената инфраструктуре (видети део 4.6. Стратегије) и 6) субјектима значајним за националну безбедност, а надлежних за инфраструктуру (видети део 5.1.2. Стратегије) (Стратегија националне безбедности Републике Србије, 2019).

Опасност од извођења сајбер напада на објекте критичне инфраструктуре и то услед развоја информационих технологија препозната је и у *Стратегији одбране, Сл. гласник РС, бр. 94/2019*. Одредба по којој Стратегија одбране предњачи по питању „поклањања пажње" критичној инфраструктури у односу на Стратегију националне безбедности тиче се осигурања безбедности објеката критичне инфраструктуре што је препознато као један од циљева заштите безбедности Републике Србије и њених грађана. Реч је о нормативно-правно уређењу и усклађивању са регулативом Европске уније области одређивања и заштите објеката критичне инфраструктуре, као и посвећивању пажње потпуном спровођењу нормативно-правних решења. „Ради осигурања безбедности објеката критичне инфраструктуре непрекидно ће се предузимати све превентивне мере, а посебно са аспекта њихове заштите од пожара, експлозија и терористичких напада. Успоставиће се интегрисани информациони систем за безбедносни надзор објеката критичне инфраструктуре" (Стратегија одбране РС, 2019).

Од значаја је и *Стратегија развоја информационог друштва и информационе безбедности у Републици Србији од 2021. до 2026. године, Сл. гласник РС, бр. 86/2021.* У оквиру одељка који се односи на унапређивање сарадње и подизање капацитета, критична информациона инфраструктура препозната је као ИКТ систем од посебног значаја „јер је неопходно одржавати њихово несметано функционисање будући да ометање, престанак или уништење ових система могу имати значајне последице у случајевима када се односе на велики број корисника, велики део територије или јавну безбедност" (Стратегија развоја информационог друштва и информационе безбедности у Републици Србији од 2021. до 2026. године, 2021). Значај ове одредбе огледа се у томе што предвиђа одређене мере у циљузаштите, попут превенције од инцидената или превенције и смањења штете од инцидената.

Законом о критичној инфраструктури, Сл. гласник РС, бр. 87/2018, уређује се национална и европска критична инфраструктура, идентификација и одређивање критичне инфраструктуре Републике Србије, заштита критичне инфраструктуре, надлежност и одговорност органа и организација у области критичне инфраструктуре и информације, извештавање, пружање подршке одлучивању, заштита података, управљање и надзор у области критичне инфраструктуре. Овим актом, критична инфраструктура одређена је као скуп „система, мрежа, објеката или њихових делова, 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, 2018, чланови 1 и 4). Из наведене дефиниције разликују се два елемента „инфраструктура" и „критично", два појма која су међусобно повезана те их није могуће разматрати појединачно. Први елемент обухвата системе, мреже, објекте и њихове делове. Односно реч је о физичкој инфраструктури, али и робама и услугама које су од круцијалног значаја за функционисање државе. Други елемент односи се на инфраструктуру која пружа сустинску подршку за националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно функционисање државе.

Заштита критичне инфраструктуре обухвата „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" (Закон о критичној инфраструктури, 2018, члан 2). Поред Министарства унутрашњих послова, активности од значаја за заштиту критичне инфраструктуре спроводе и министарства задужена за секторе критичне инфраструктуре и оператори критичне инфраструктуре[142], као и Републички штаб за ванредне ситуације.

Једна од основа сваке заштите јесте познавање предмета заштите, поред познавања претњи и начина заштите.[143] Како је предуслов заштите критичне инфраструктуре идентификација и одређивање њених елемената, намеће се као незаобилазно дати одговор на питање шта је то што се штити и уједно утврдити шта је то што чини критичну инфраструктуру.[144] *Уредбом о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије,*

[142] Оператори критичне инфраструктуре су државни органи, органи аутономне покрајине, органи јединице локалне самоуправе, јавна предузећа, привредна друштва или друга правна лица која управљају системима, мрежама, објектима или њиховим деловима који су одређени као критична инфраструктура (Закон о критичној инфраструктури, 2018, члан 2).

[143] Да би се нешто заштитило потребно је дати одговор на три питања: Шта се штити?, Од чега се штити? и Како се штити?

[144] Стајић указује на то да ни у једном документу није одређено степеновање елемената критичне инфраструктуре што препознаје као пропуст с обзиром на то нису сви елементи истог значаја, већ је потребно одредити степен значаја, а самим тим и степен заштите елемената (2018, стр. 125).

Сл. гласник РС, бр. 69/2022 прописани су критеријуми идентификације и то у односу на процену последица које могу да наступе услед ометања или уништења критичне инфраструктуре, као и на основу последица које могу да наступе у случају претњи по критичну инфраструктуру (члан 2). Уз то, критеријуми, односно последице одређене су за сваки сектор критичне инфраструктуре, а уважавајући специфичности појединачних сектора. Реч је о секторима енергетике, саобраћаја, снабдевања водом и храном, здравства, финансија, телекомуникационих и информационих технологија, заштите животне средине и функционисања државних органа (Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије, члан 4).

Оно што је занимљиво јесте да је у *Националној процени ризика Републике Србије од катастрофа* идентификовано 11 сектора критичне инфраструктуре. Поред осам сектора наведених у предметном Закону о критичној инфраструктури и Уредби о критеријумима за идентификацију критичне инфраструктуре, у Националној процени ризика Републике Србије од катастрофа издвајају се и сектори: снадбевање водом и снадбевање храном, унапређује функционисање државних органа у функционисање органа државне управе и хитних служби и наука и образовање као посебан сектор (МУП РС, 2019). 11 сектора наведених у Националној процени ризика Републике Србије од катастрофа проистекли су из Методологије израде и садржаја процене ризика од катастрофа и плана заштите и спасавања где су идентификовани, а о којој ће бити више речи у тексту који следи.

Идентификовани сектори критичне инфраструктуре у нашој земљи не разликују се превише од сектора идентификованих у земљама у окружењу. На основу анализе правних аката којима се регулише ова област у свакој земљи у окружењу, а за које су подаци доступни, могуће је уочити да све државе препознају седам сектора критичне инфраструктуре (енергетика, саобраћај/транспорт, снабдевање водом, снадбевање храном, здравство, финансије/банкарство, (теле)комуникационе и информационе технологије/инфраструктуре) одређених у истом или сличном (проширеном) контексту.[145]

Министарства задужена за секторе критичне инфраструктуре предлажу објекте критичне инфраструктуре у свом сектору. Предложену критичну инфраструктуру коначно одређује Влада. Закон предвиђа обавезу министарстава да у року од шест месеци од усвајања горепоменуте Уредбе Министарству унутрашњих послова доставе предлоге критичне инфраструктуре у свом сектору, те да редовно извештавају о новонасталим променама и да Акт о одређивању критичне инфраструктуре ажуририрају сваке године (Закон о критичној инфраструктури, 2018, члан 7). Већ почетком 2023. године, требало је да акти о одређивању критичне инфраструктуре буду донети. На основу доступних података, није познато да ли су ти акти донети, као ни да ли су у министарствима одређена лица која би се овим питањем бавила. Такође, није познато да ли су правна лица која спадају у критичну инфраструктуру извршила своју обавезу и одредила и саставила списак објеката критичне инфраструктуре под својом управом.

Акционим планом за Поглавље 24 у преговорима о приступању Србије Европској унији, Министарство унутрашњих послова Републике Србије препознато је као орган надлежан да изради предлог законодавног оквира у овој области. У оквиру овог Министарства, Сектор за управљање ванредним ситуацијама одређен је као орган који координира активности на формирању међуресорне радне групе која ће дефинисати националну

[145] Видети више у: Марковић, Јана. (2023). Улога корпоративне безбедности у заштити критичне инфраструктуре Републике Србије. *Безбедност* 65 (2), стр. 197-214.

политику заштите критичне инфраструктуре или спроводи анализу недостатака на основу изабраног модела најбоље праксе у Европској унији (Action Plan for Chapter 24, 2015, pp. 257-258). Група аутора је анализирајући систем заштите критичне инфраструктуре у Републици Србији, установила да се систем састоји од управљачког и извршног дела, попут других државних система, те да управљање овим системом обухвата активности на три нивоа и то стратешком, координирајућем и оперативном нивоу (Стајић, Мирковић и Радивојевић, 2021, стр. 13). На стратешком нивоу, прописани су поступци идентификације и одређивања критичне инфраструктуре, надлежност и одговорност субјеката система заштите критичне инфраструктуре, као и начела деловања. На координирајућем нивоу, одређени су Министарство унутрашњих послова да уређује, планира, координира, контролише активности, комуницира и даје информације у вези са критичном инфраструктуром и Републички штаб за ванредне ситуације да руководи и координира спровођење мера и задатака у случају наступања околности угрожавања, ометања рада или уништења критичне инфраструктуре. На оперативном нивоу, одређују се оператори критичне инфраструктуре, као и Министарства надлежна за секторе критичне инфраструктуре.

Према тренутним прописима, Министарство унутрашњих послова одређено је да „уређује, планира, координира, контролише активности, комуницира и даје информације у вези са критичном инфраструктуром“ (Закон о критичној инфраструктури, 2018, члан 4).[146] Изузетак су објекти од посебног значаја за одбрану над којима покровитељство има Министарство одбране, док се „заштита, чување, коришћење, контрола и надзор критичне инфраструктуре у надлежности Министарства одбране и Војске Србије спроводи се у складу са Законом о одбрани и Законом о војсци Србије“ (Закон о критичној инфраструктури, 2018, члан 7). Закон је одредио и да измене акта о унутрашњем уређењу и систематизацији радних места у Министарству унутрашњих послова министар донесе у року од 30 дана од дана ступања на снагу овог закона (члан 23). Информације о томе да ли је исто учињено нису доступне под претпоставком да је реч о подацима означеним одређеним степеном тајности.[147] На основу спроведеног истраживања, поставља се и питање тренутних капацитета Министарства унутрашњих послова да спроводи и буде одговорно за активности које му је овај закон одредио. Да ли ће постојати посебна организациона целина овог Министарства која ће се бавити искључиво заштитом критичне инфраструктуре, као што на пример, постоји Одељење за послове приватног обезбеђења и детективске делатности (у склопу Управе полиције) или ће ова активност бити поверена Сектору за ванредне ситуације према индицијама које постоје тренутно?! У сваком случају, Министарство унутрашњих послова има улогу координирајућег субјекта система заштите (оперативни ниво). На нижим нивоима, субјекти заштите на оперативно извршном нивоу јесу субјекти националне безбедности, различите агенције и друга тела која се формирају за сваку појединачно област критичне инфраструктуре на том нивоу управљања, док су непосредни извршиоци заштите полиција, штабови за ванредне ситуације, медицинске установе, ватрогасно-спасилачке јединице, као и службе обезбеђења, односно целокупна приватна безбедност са својим ресурсима.

Закон предвиђа израду безбедносног плана оператора за управљање ризиком. Реч је о документу којим се „утврђују мере смањења ризика, дефинишу одговорности и одређују

[146] У Нацрту Закона о критичној инфраструктури предвиђало се формирање посебне организационе јединице које регулише, планира, координира, контролише, комуницира и даје информације у вези са критичном инфраструктуром. Реч је било о Центру за координацију и заштиту критичне инфраструктуре, чије није усвојено (Нацрт Закона о критичној инфраструктури, 2018, члан 4).

[147] О овом питању видети више у: Синдикат полиције Слога. (2021, Септембар 9). *Систематизација у МУП недоступна иако је информација од јавног значаја*. Доступно на: https://sindikatpolicije.org.rs/?p=4740#more-4740.

дужности, те успоставља оквир за поступање у циљу отклањања, односно смањења последица безбедносних претњи дефинисаних у анализи ризика, која је саставни део плана“ (Закон о критичној инфраструктури, 2018, члан 8). Закон међутим није одредио мере смањења ризика, па се оставља сваком оператору да сам одреди и дефинише мере на основу идентификованих безбедносних претњи. На овај начин, како није дат ни било какав оквир за наведене мере, начин заштите је потпуно остављен операторима. Министар надлежан за унутрашње послове требало је да пропише методологију, начин израде и садржај Безбедносног плана оператора за управљање ризиком (Закон о критичној инфраструктури, 2018, члан 8). Скоро шест година након ступања на снагу овог закона, Методологија није израђена, односно усвојена. Група аутора у вези са наведеним даје препоруку да процена ризика и Безбедносни план буду два одвојена акта и наводи три разлога за то. Први разлог се односи на то да с обзиром на то да процена ризика садржи елементе попут идентификованих ризика, вероватноће наступања последица и самих последица које би настале, најпре би требало добити сагласност на процену, на основу које ће се даље развијати безбедносни план. Други разлог је да би израда процене ризика требало да се врши на основу посебне методологије, попут оне која постоји у области смањења ризика од катастрофа. На крају, требало би донети процену ризика на националном нивоу, затим на секторском нивоу и тек на крају на нивоу појединачног оператора, па и с обзиром на различите нивое, процена ризика треба да буде засебан документ (Стајић, Мирковић и Радивојевић, 2020, стр. 961).

У пракси су препознати одређени недостаци који могу да створе проблеме у систему заштите критичне инфраструктуре, а односе се на израду докумената (на пример, горе поменутих) и спровођење мера пре и након криза. Најпре, међузависност критичне инфраструктуре условљава израду процена и планова који су међусобно комплементарни, а тиме и сарадњу и комуникацију оних лица која их израђују. Међутим, пракса је лишена повезаности међузависности процена, планова и мера заштите, контроле њиховог доношења и примене. Лица која исте одређују немају исто образовање нити су едуковани за ову врсту посла, немају иста и довољно функционална средства нити су сви финансијски опскрбљени за тај посао (Стајић, 2018, стр. 127).

Ради усаглашавања са прописима донетим на нивоу Европске уније, Закон је предвидео и постојање такозваног официра за везу. Реч је о лицу „које служи као контакт између оператора и Министарства (унутрашњих послова), које обезбеђује сталну контролу ризика и претњи, обавештава о променама у односу на критичну инфраструктуру, обавештава Министарство (унутрашњих послова) 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“ (Закон о критичној инфраструктури, 2018, члан 9). Начин и програм за полагање посебног стручног испита за добијање лиценце коју официр за везу мора поседовати, за сада деле исту судбину као и методологија за израду и садржај Безбедносног плана. Ни ове области нису уређене до данас.

Деловање официра за везу је колико реактивно толико и превентивно. Наиме, од значаја је одредба закона која одређује да „приликом израде планских докумената у области просторног и урбанистичког планирања, докумената из области националне безбедности и области смањења ризика и управљања ванредним ситуацијама, критична инфраструктура мора се третирати на посебан начин, нарочито у делу превентивних активности и активности везаних за одговор на ванредне ситуације у којима мора имати приоритет“ (Закон о критичној инфраструктури, 2018, члан 10). На овај начин, негује се проактивно поступање у области заштите.

У случају „угрожавања, ометања рада или уништења критичне инфраструктуре руковођење и координацију спровођења мера и задатака у наведеним околностима

предузима Републички штаб за ванредне ситуације“ (Закон о критичној инфраструктури, 2018, члан 11), а у складу са *Законом о смањењу ризика од катастрофа и управљању ванредним ситуацијама, Сл. гласник РС, бр. 87/2018*. Интересантно је међутим да се у Закону о смањењу ризика од катастрофа и управљању ванредним ситуацијама ни на једном месту не помиње критична инфраструктура или њена заштита. Међутим, на основу члана 17. став 10. Закона о смањењу ризика од катастрофа и управљању ванредним ситуацијама донето је *Упутство о Методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања, Сл. гласник РС, бр. 80/2019* из којег проистиче документ под насловом „Методологија израде и садржај процене ризика од катастрофа и плана заштите и спасавања“. У овој Методологији постоје одредбе које се односе на критичну инфраструктуру, а која мора да буде обухваћена Проценом ризика од катастрофа Републике Србије, аутономне покрајине и јединице локалне самоуправе. Критична инфраструктура дефинише се на начин на који је то учињено у Закону о критичној инфраструктури и наводе се следеће инфраструктуре (део I, А)2.):

1) „Енергетску инфраструктуру чине: термо и хидро електране, термоелектране – топлане и други објекти за производњу електричне енергије, као и електроенергетски водови, далеководи и трансформаторске станице; објекти за производњу електричне енергије из обновљивих извора; високе бране и акумулације напуњене водом; објекти за производњу и прераду нафте и гаса, производњу биогорива и биотечности.
2) Саобраћајну инфраструктуру чине: друмски, железнички, ваздушни саобраћај (ауто-пут, државни путеви I и II реда; категорисани и некатегорисани путеви, мостови, тунели, надвожњаци и аутобуске станице; железничка мрежа, железничке станице; аеродроми), речни пловни путеви, луке и гранични прелази.
3) Водопривредну инфраструктуру чине: изграђени системи активне и пасивне заштите на водотоковима I и II реда; снабдевање водом – међурегионални и регионални објекти водоснабдевања, постројења за припрему воде за пиће; регулациони радови за заштиту од великих вода градских подручја и руралних површина; хидрограђевински објекти на пловним путевима; пловни канали и бродске преводнице, који нису у саставу хидроенергетског система.
4) Снабдевање храном: погони и капацитети за производњу хране, складишта прехрамбених производа (силоси, хладњаче...), објекти и средства за дистрибуцију.
5) Здравствену критичну инфраструктуру чине: објекти на примарном нивоу (домови здравља, болнице, апотеке, заводи); објекти на секундарном нивоу (болница – општа и специјална); објекти на терцијарном нивоу (клиника, институт, клиничко-болнички центар, клинички центар) и здравствена делатност која се обавља на вишем нивоу (заводи).
6) Финансије: банкарство, берзе, инвестиције и систем осигурања.
7) Телекомуникациону и информациону критичну инфраструктуру чине: објекти система и средства електронских комуникација, који су међународног и магистралног значаја; пренос података; информациони системи; пружање аудио и аудио-визуелних медијских услуга.
8) Заштита животне средине: производња и складиштење опасних материја (хемијске материје, биолошки материјали, радиолошки материјали, нуклеарни материјали као и депоније).
9) Функционисање органа државне управе и хитних служби (полиција, хитна медицинска помоћ, ватрогасно-спасилачке јединице и др.).

10) Наука и образовање: установе науке и образовања, њихови објекти, људски и материјални ресурси“.

Методологија не садржи процену рањивости и отпорности критичних инфраструктура на све врсте претњи, као и мере повећања отпорности о чему се доста говори о новоусвојеној секторској директиви на нивоу Европске уније. С обзиром на настојање Републике Србије да буде усаглашена са прописима о европској критичној инфраструктури, остаје празан простор између ове Методологије, као и Закона о критичној инфраструктури и нове Директиве Европске уније о отпорности критичних субјеката.

Поред наведеног, на основу члана 31. став 2. Закона о смањењу ризика од катастрофа и управљању ванредним ситуацијама донета је *Одлука о одређивању субјеката од посебног значаја за заштиту и спасавање у Републици Србији, Сл. гласник РС, бр. 69/2019*. Овом одлуком одређују се привредна друштва и друга правна лица, која су од значаја за спровођење мера заштите и спасавања, а који уједно припадају секторима критичне инфрастурктуре. Ако се повуче паралела између ове Одлуке и раније наведене Одлуке о одређивању великих техничких система од значаја за одбрану уочава се да одређена привредна друштва и друга правна лица од посебног значаја за заштиту и спасавање уједно представљају и велике техничке системе од значаја за одбрану. Реч је о: „Телеком Србија” а.д. Београд; BELGRADE AIRPORT d.o.o. Beograd; ЈП „Пошта Србије” Београд; АД ’Србија Воз’ Београд; АД ’Србија Карго’ Београд; АД ’Инфраструктура железнице Србије’ Београд; ЈП „Електропривреда Србије” Београд; АД ’Електромрежа Србије’ Београд; НИС а.д. Нови Сад и његова зависна привредна друштва; ЈП „Србијагас“ Београд; ЈВП „Србијаводе” Београд; ЈВП „Воде Војводине” Нови Сад; Јавна медијска установа Радио-телевизија Србије Београд; ЈП „Србијашуме“ Београд; ЈП „Војводинашуме” Петроварадин.

На основу претходне анализе изводи се закључак да је идентификацији критичне инфраструктуре више пажње посвећено Законом о смањењу ризика од катастрофа и управљању ванредним ситуацијама него матичним (системским) законом који треба на свеобухватан начин да уреди ову област и на тај начин послужи као основа даљој регулативи области критичне инфраструктуре и њене заштите.

Закон о критичној инфраструктури директно је повезан са Законом о одбрани и Законом о војсци. Ова два закона, као што је већ наведено, односе се на заштиту, чување, коришћење, контролу и надзор критичне инфраструктуре која је у надлежности Министарства одбране и Војске Србије. *Закон о одбрани, Сл. гласник РС, бр. 116/2007, 88/2009, 88/2009, 104/2009, 10/2015, 36/2018*, издваја се на овом месту као значајан у погледу одређења објеката од посебног значаја за одбрану земље, чиме се уједно и врши идентификација критичне инфраструктуре. У ове објекте се убрајају следеће врсте објеката: велики техничко-технолошки системи, објекти у којима се производе, складиште или чувају предмети или врше услуге за потребе одбране, објекти у којима су смештени државни органи и правна лица од посебног значаја за одбрану земље, као и одређени инфраструктурни објекти (Закон о одбрани, 2007, члан 67). Изменама и допунама закона, прописано је да се мере заштите ових објеката предузимају кроз опште и посебне мере заштите предвиђене прописима којима се уређује тајност података (Закон о одбрани, 2007, члан 67а).[148]

Анализом Закона о одбрани и одлука које произилазе из њега, а које су представљене у претходном поглављу, добија се детаљнији списак критичне инфраструктуре од оног који је дат у матичном (системском) Закону о критичној инфраструктури. У вези са свиме наведеним, а узимајући у обзир ближе одређење објеката од посебног значаја за одбрану и великих техничких система од значаја за одбрану, одређени елементи критичне инфраструктуре уједно чине и објекте препознате и одређене као посебно значајне са

[148] Подзаконски акти донети на основу овог закона обрађени су у претходном поглављу, те се на овом месту неће разматрати.

аспекта одбране земље. Уз то, као што се види из до сада изложеног, уједно је реч и објектима од посебног значаја за заштиту и спасавање.

У *Закону о приватном обезбеђењу*, *Сл. гласник РС, бр. 104/2013, 42/2015, 87/2018* не постоје одредбе везане за критичну инфраструктуру, али се одредбама обухватају обавезно обезбеђени објекти. Реч је о објектима „од стратешког значаја за Републику Србију и њене грађане, као и објекте од посебног значаја чијим оштећењем или уништењем би могле наступити теже последице по живот и здравље људи или који су од интереса за одбрану земље, осим објеката чију заштиту обављају државни органи и објеката чија се заштита обавља сагласно прописима из области одбране. Под обавезно обезбеђеним објектима сматра се и простор на коме се налазе ти објекти и чине њихов саставни део, као и пратећи објекти који су у функцији тих објеката“ (Закон о приватном обезбеђењу, 2013, члан 4). На основу овог Закона, донета је *Уредба о ближим критеријумима за одређивање обавезно обезбеђених објеката и начину вршења послова њихове заштите, Сл. гласник РС, бр. 98/2016*. Њоме су били одређени објекти који се обавезно обезбеђују и начин вршења послова њихове заштите. Упркос томе што је ова Уредба имала свој ослонац у Закону о приватном обезбеђењу доношењем Закона о критичној инфраструктури ова Уредба је престала да важи. Као њен правни следбеник узима се Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије која не садржи ниједну одредбу која се односи на обавезно обезбеђене објекте. Тако, изузев дефиниције из Закона о приватном обезбеђењу, термин обавезно обезбеђени објекти остао је неодређен. Иако је један део ових објеката одређен као критична инфраструктура, други део објеката је изостављен и то из оправданих разлога због погрешно одређених одредаба. Конкретно, у ову другу групу убрајали су се: затворени објекти, дворане, хале и други објекти намењени за окупљање грађана капацитета смештаја 5000 грађана и више; отворени објекти, стадиони и други објекти намењени за окупљање грађана капацитета смештаја 20.000 грађана и више; и тржни центри отвореног и затвореног типа површине 10.000 m^2 и више.[149]

Закон о приватном обезбеђењу на овом месту неће бити предмет подробне анализе, међутим, могуће је издвојити активности приватног обезбеђења када је у питању заштита критичне инфраструктуре. Стајић наводи да приватно обезбеђење може да има значајну улогу у: изради безбедносних процена ризика и планова деловања; превенцији и смањењу ризика; раном упозоровању и мобилизацији; постављању и употреби средстава техничке заштите; садејству са другим органима на предузимању мера заштите; отклањању штета; ширењу безбедносне културе и обуци шире популације на заштити; заштити ширих зона непосредног ризика; заштити када је она у приватном власништву; учешћу у штабовима за ванредне ситуације; уступању сопствених средстава и људства (мобилизација) државним органима у заштити након проглашења ванредних ситуација; спровођењу мера личне заштите, евакуације, збрињавања, спасавања, пружања прве медицинске помоћи; асанацији терена и др. (Стајић, 2019, стр. 132).

Поред обавезно обезбеђених објеката, издвајају се објекти, као и лица која уживају посебну заштиту коју обезбеђују министарство надлежно за унутрашње послове, Безбедносно-информативна агенција, Војнобезбедносна агенција, Војна полиција и јединице Војске Србије, на начин како је то уређено *Уредбом о одређивању послова безбедносне заштите одређених лица и објеката, Сл. гласник РС, бр. 72/2010, 64/2013*. Доношењем прве верзије Закона о приватном обезбеђењу било је предвиђено да приватно обезбеђење може пружати услуге заштите свих објеката од стратешког и

[149] О обавезно обезбеђеним објектима видети више у: Уредба о ближим критеријумима за одређивање обавезно обезбеђених објеката и начину вршења послова њихове заштите. (2016). *Сл. гласник РС*, бр. 98/2016, члан 2.

посебног значаја. Ипак, изменама закона из 2015. године искључена је та могућност (Радивојевић, 2019, стр. 217). *Законом о полицији, Сл. гласник РС, бр. 6/2016, 24/2018, 87/2018,* Министарство унутрашњих послова овлашћено је да врши безбедносну заштиту одређених личности и објеката (члан 3), као и да поступа у стању повећаног ризика по стање јавне безбедности, као и угрожавања безбедности људи или имовине у већем обиму (члан 29). У првом случају, полиција врши обезбеђивање објеката одређене критичне инфраструктуре, док у другом случају може да поступа када је критична инфраструктура угрожена.

На овом месту вреди помена и *Закон о информационој безбедности, Сл. гласник РС, бр. 6/2016, 94/2017, 77/2019*. У овом Закону, појам критичне информационе инфраструктуре се не помиње као такав, али се препознају ИКТ (информационо-комуникациони) системи од посебног значаја који обављају различите делатности међу којима су и оне од општег интереса. С тим у вези, у обављању делатности од општег интереса одређени су ИКТ системи у областима енергетике, саобраћаја, здравства, банкарства и финансијских тржишта, дигиталне инфраструктуре и другим областима попут електронске комуникације, производње и промета наоружања и војне опреме или комуналних делатности (Закон о информационој безбедности, 2016, члан 6). Значај овог Закона огледа се у чињеници да оваквим одређењем ИКТ система од посебног значаја недвосмислено указује на то да многи од препознатих ИКТ система представљају критичну инфраструктуру. Овакав исказ поткрепљује одредба Стратегије развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године, Сл. гласник РС, бр. 86/2021, по којој су „ИКТ системи од посебног значаја или тзв. критична информациона инфраструктура дефинисани Законом као посебни и значајни, јер је неопходно одржавати њихово несметано функционисање будући да ометање, престанак или уништење ових система могу имати значајне последице у случајевима када се односе на велики број корисника, велики део територије или јавну безбедност“ (3, Мера 3.2.).

Поред наведених закона и подзаконских аката, постоји још читав низ секторских закона у областима попут тајности података, вода, безбедности хране, просторном планирању, заштити од пожара, заштити животне средине, јавно-приватном партнерству, који не помињу децидно термин критична инфраструктура, али који кроз своје одредбе обухватају поједине сегменте критичне инфраструктуре и њихову заштиту.[150]

На крају овог поглавља, оправдано је указати и на *Уредбу о условима испоруке и снабдевања електричном енергијом, Сл. гласник РС, бр. 84/2023.*[151] У Уредби се наводи да се купцима за објекте чији би прекид рада довео до непосредне опасности по живот и здравље људи и за објекте од посебног интереса за привреду и живот људи и одбрану Републике Србије не може обуставити испорука електричне енергије. У ове објекте спадају здравствене установе у складу са законом којим се уређује здравствена заштита, изузев апотека; објекти водовода и канализације (за производњу, пречишћавање и транспорт воде, за функционисање канализације); кухиње за снабдевање дечјих установа и установа социјалне заштите; системи даљинског грејања; хидрометеоролошки и сеизмолошки заводи; рудници угља за снабдевање термоелектрана; војни објекти; објекти установе јавног радиодифузног сервиса у складу са законом којим се уређују електронске комуникације; предшколске, школске и високошколске установе; објекти полиције у складу са законом и прописима којима се

[150] Видети исто у: Трбојевић, Милован. (2018). Заштита критичних инфраструктура-искуства транзиционих земаља. *Политичка ревија* 56 (2), стр. 99-118; Мићовић, Д. Марија. (2020). *Специфичности критичне инфраструктуре у Републици Србији*. Београд: Криминалистичко-полицијски универзитет.

[151] Видети у вези са текстом и: Уредба о условима испоруке и снабдевања природним гасом. (2022). *Сл. гласник РС*, бр. 49/2022, 32/2023, 97/2023, члан 35.

уређује рад полиције; објекти ватрогасне службе у складу са законом којим се уређује заштита од пожара; објекти јавне телекомуникационе мреже у складу са законом којим се уређују електронске комуникације; објекти за издржавање заводских санкција у складу са законом којим се уређује извршење кривичних санкција; објекти органа државне управе у којима се обављају стручни и са њима повезани извршни послови у области метрологије; сопствена потрошња енергетских објеката и пословних објеката енергетских субјеката лиценцираних за обављање енергетске делатности, који су у функцији управљања, експлоатације и одржавања електроенергетског система (члан 57). У случају опште несташице, испорука електричне енергије се не може обуставити и следећим објектима: објектима и исправљачким станицама јавног саобраћаја (аеродроми, железничке станице, трамваји, тролејбуси, станице сигнализације за јавни саобраћај и централне гараже јавног саобраћаја); амбасадама, конзулатима и резиденцијама амбасадора и конзула; топлим погонима, пећима за топљење, погонима петрохемије и базне хемије, хладњачама и пумпним станицама за одводњавање; објектима за производњу нафте и природног гаса; објектима за производњу деривата нафте, нафтоводима, продуктоводима, објектима за складиштење нафте и деривата нафте; објектима за транспорт, дистрибуцију и складиштење природног гаса; објектима у којима су смештени државни органи; студентским, ученичким домовима и установама социјалне заштите (геронтолошки центри, домови за стара лица, домови за децу са сметњама у развоју); претоварним капацитетима речног, железничког и другог саобраћаја (члан 58).

На основу одредаба у наведеној Уредби, уочава се начињен избор по питању објеката чија је делатност од виталног интереса како за потребе одбране тако и за функционисање друштва у мирнодопским условима. Неулазећи у детаљнију анализу, значај овог избора огледа се и у томе што поред објеката који се карактеришу као критична инфраструктура, препознају се и други објекти који би могли да добију тај атрибут.

5. ДИСКУСИЈА

Поглавље је посвећено презентацији синтезе налаза добијених спровођењем експертског интервјуа, а у складу са дефинисаним предметом и циљевима истраживања. Како је наведено у методолошком делу дисертације, испитивање је спроведено са експертима – менаџерима безбедности, односно лицима која су запослена на руководећим пословима (корпоративне) безбедности у великим техничким системима од значаја за одбрану (критична инфраструктура). Експертски интервју треба да допуни одговоре на постављена истраживачка питања: у првом реду, на помоћно истраживачко питање првог нивоа *П2: У којој мери заштита критичне индраструктуре омогућава разумевање доприноса корпоративне безбедности на националну безбедност Републике Србије?* укључујући помоћна истраживачка питања другог нивоа која су обухваћена овим истраживачким питањем.

У првом делу поглавља, представљање резултата истраживања организовано је у неколико целина чији је редослед одређен тако да се постигне једна смислена дискусија. Након тога су предложене препоруке које би могле да кроз заштиту критичне инфраструктуре допринесу развоју улоге корпоративне безбедности у циљу унапређења националне безбедности. У последњем делу поглавља истакнута су ограничења дисертације, након чега следи закључно поглавље.

5.1. Допринос корпоративне безбедности националној безбедности Републике Србије са аспекта заштите критичне инфраструктуре

С обзиром на главно истраживачко питање *Који је допринос који корпоративна безбедност кроз заштиту критичне инфраструктуре може да пружи националној безбедности Републике Србије?*, у овој дисертацији биће разматране са једне стране организација и функције корпоративне безбедности у великим техничким системима од значаја за одбрану (у даљем тексту: системи) који су узети као објекти критичне инфраструктуре и са друге стране допринос те безбедности систему и стању националне безбедности.[152] Како би се добио што систематичнији увид у синтезу добијених налаза, текст који следи подељен је у неколико целина.

[152] Област корпоративне безбедности у Републици Србији још увек није достигла потребан ниво развоја. Још увек како у научним круговима, тако и у области праксе корпоративна безбедност није потпуно препозната као посебна област која завређује посебну пажњу. Иако су сви испитаници врло добро знали шта је приватно обезбеђење/безбедност (као нека врста корена корпоративној безбедности), неколико испитаника је требало објашњење шта је то корпоративна безбедност и шта се под њом подразумева. Овакав став проистиче не из незнања испитаника већ из неколико других разлога. Најпре, нигде се у званичним документима не помиње термин корпоративна безбедност. Поред тога, наука још увек није успела да дистрибуира знања о корпоративној безбедности, те су сазнања из ове области остала ограничена на оне који се њоме и сличним појавама баве. На крају, у пракси, у зависности од индустрије, власничке структуре правних лица, као и личних преференција зависи да ли ће лице имати одређена знања о корпоративној безбедности или не, као и у ком обиму ће та знања имати уколико их има. Важно је напоменути још једном да лица која немају сазнања о корпоративној безбедности не значи да нису стручна и професионална у обављању својих послова из области безбедности, већ да се у свом раду нису суочавала са овим концептом и његовом садржином. Након објашњења овог концепта, ти испитаници су исти прихватили и признали као валидан, те је разговор настављен.

1. Организација и функционисање корпоративне безбедности великих техничких система од значаја за одбрану (критична инфраструктура)

Испитаници су сагласни да су организација и функције корпоративне безбедности у систему где су запослени успостављени на основу закона и подзаконских аката области које спадају у корпус корпоративне безбедности, као и на основу интерне регулативе и међународних и националних стандарда. У највећем броју случајева, односно код највећег броја система који су били посматрани, не постоји кровни документ из области корпоративне безбедности. Целокупна област уређена је најпре актом о организацији или систематизацији (где се утврђују на пример, организациона структура, опис послова, број запослених, квалификације запослених, нивои плаћања), а потом и нижим актима које чине интерну регулативу по областима и то су најпре упутства, процедуре, правилници. Такви нижи документи могу бити и овлашћења директора. Дакле, у највећем броју посматраних система не постоји један документ који би сублимирао све, већ постоје парцијални који обухватају све послове и активности из сфере безбедности.

Наредно значајно питање јесте однос корпоративне безбедности као организационе целине (или организационих целина које обухватају област корпоративне безбедности, јер има и таквих случајева) са 1) главним менаџментом, односно генералним или извршним директором и 2) са другим организационим целинама. Питање односа са менаџментом или руководством значајно је јер директна подређеност, комуникација и одговорност су далеко ефикасније од посредничког односа организационе целине према руководству. Посматрани системи нису уједначени када је реч о директној повезаности организационе јединице и руководства. У неким системима постоји повезаност са извршним или генералним директором, док у неким системима се организационе целине корпоративне безбедности налазе тек на четвртом нивоу хијерархије. Као главни проблем који се јавља када не постоји директна повезаност издвојен је спор рад који свакако да успорава и радне процесе. Када је реч о односу са другим органоизационим целинама, било која организациона целина у области безбедности остварује сарадњу са другим организационим целинама, а нарочито оним целинама које из одређеног, али не и адекватног, разлога обављају послове из делокруга безбедности. Један од испитаника истакао је значај позиције и улоге менаџера безбедности. Сумирано, неопходно је усвојити и имати нормативни оквир такав да се организациона целина корпоративне безбедности постави да буде директно одговорна врху организације, да сарадња и комуникација са другим организационим целинама буде без преседана, те да се нормативно уреди позиција и делокруг послова менаџера безбедности. Менаџер безбедности треба да познаје цео систем, да успостави добру сарадњу са свим организационим целинама, да омогући и обезбеди да се и те целине упознају са улогом и сврхом корпоративне безбедности, као и да знају своје обавезе у погледу корпоративне безбедности.

Од значаја је и да ли ће се, или још боље, колико ће се издвајати и улагати у успостављање, одржавање и развој безбедности. Иако су испитаници у највећој мери сагласни по питању свести које руководство њихових система има по питању улагања у безбедност, као и по питању спремности да се уложи у безбедност, било је и оних испитаника који су указали на то да таква пракса није заступљена у њиховим системима. У сваком случају, у мере које су прописане законима и другим правним актима, као и међународним и националним стандардима улагање није смело да изостане. У случају изостанка, то би значило кршење прописаних норми или неизвршавање „обавеза“ из стандарда на које су се системи обавезали. Неки испитаници су скренули пажњу на то да улагања доста зависе не само од свести и спремности руководства, да ли они улагање виде као трошак или не, већ и од власничке структуре система. Сумирано, тамо где не постоји или постоји смањена свест и спремност за улагањем у безбедност неопходно је

исту развити или унапредити. Ова два елемента – свест и спремност су један од основних предуслова подизања нивоа безбедности са једне стране и увођења и унапређења корпоративне безбедности са друге стране. У основи сваке свести обично се налазе користи које, у овом случају, правно лице може да има од успостављене и функционалне корпоративне безбедности.

Системи у којима руководство има свест о потреби и бенефитима улагања у безбедност, то се чини континуираним развојем интерне регулативе и њеном потпуном применом, сталном едукацијом запослених како у области корпоративне безбедности, тако и у систему (кроз унапређивање бизнис процеса, улагања у кадрове). Један од испитаника је издвојио посебно едукацију запослених у процесу производње изневши став да уколико је он добро обучен, он ће добро, контролисано и одговорно водити свој процес, а ако дође до акцидента, он је обучен и први ће реаговати.

Испитаници су сагласни да су организација и функције корпоративне безбедности засновани на законима, подзаконским актима и интерној регулативи. Ипак, у већини посматраних система не постоји јединствен документ који обухвата све аспекте безбедности, већ докумената (правилници, процедуре, упутства) која покривају појединачне области безбедности. Када је реч о односу организационе целине корпоративне безбедности са менаџментом и другим организационим целинама, у неким системима, корпоративна безбедност има директну повезаност са менаџментом, док у другим постоји посреднички однос. Испитаници наглашавају да је неопходно да однос са менаџментом буде директан, јер побољшава комуникацију и процесе рада. Сарадња са другим организационим целинама препозната је као значајан сегмент у свим испитиваним системима. Сумирано, за успешну функцију корпоративне безбедности, неопходно је јасно дефинисати организациону структуру, успоставити директну повезаност са менаџментом, развијати сарадњу са другим организационим целинама и уз све то улагати у континуиран развој функције и едукацију запослених.

2. Функције корпоративне безбедности великих техничких система од значаја за одбрану (критична инфраструктура)

Када је реч о функцијама корпоративне безбедности, на основу добијених одговора, изводи се закључак да се у свим посматраним системима спроводе функције корпоративне безбедности. Реч је о следећим:

- безбедност на радном месту – безбедност запослених (безбедност и здравље на раду, заштита од насиља и мобинга);
- физичка и техничка заштита лица, имовине и пословања (ангажовање службеника обезбеђења и имплементација техничке заштите);
- прикупљање, провера, заштита и безбедност података и информација;
- надзор и контрола (проактивно деловање ради спречавања штетног догађаја: надзор и контрола над пословањем одређених сектора, процесних радњи у производњи, магацинских процеса (улаз/излаз робе, полупроизвода или сировина), надзор и контрола над спровођењем интерне регулативе);
- унутрашње истраге (спровођење интерних истрага у случају штетног догађаја унутар организације); заштита од пожара; заштита животне средине;
- процена, контрола и управљање ризиком;
- управљање кризама (кризни менаџмент);
- континуитет пословања.

Поред наведених функција, у неким системима постоје и друге попут економске безбедности, осигурања имовине, ауторизованог надзора, контролисања садржаја који се пласира у медије, а све то због специфичне делатности којој систем припада.

Поједине функције, и са њима повезани послови, су обавезни у складу са законима, док се функције надзора и контроле, унутрашњих истрага, управљања ризицима, кризни менаџмент и континуитет пословања спроводе како кроз друге наведене функције безбедности, тако и кроз друге сегменте рада правног лица (система). Неке од наведених функција не носе назив који је на овом месту наведен, али су препознате као функције које се спроводе у посматраним системима.

У одређеном броју посматраних система, функције корпоративне безбедности нису груписане под једну организациону целину, већ су распоређени у неколико, међу којима су и оне целине које немају додирних тачака са безбедношћу. На пример, безбедност и здравље на раду је у неким системима у сектору људских ресурса, док је у неким системима у правном сектору или чак у сектору „коришћења"; физичко-техничка заштита у правном сектору, информациона (ИКТ) безбедност у сектору развоја. У одређеним системима је корпоративна безбедност подељена на две или више грана које се баве пословима искључиво безбедносног карактера. На пример, постоје област/функција ХСЕ (безбедност и здравље на раду, индустријска безбедност и реаговање у ванредним ситуацијама и заштита животне средине) и област/функција корпоративне заштите (економска безбедност, безбедност информација, верификација кандидата за запошљавање, информациона аналитика, одбрамбене припреме). Или чак неколико јединица: Сектор заштите од пожара и безбедности и здравља на раду, Сектор безбедности и заштите животне средине, Сектор информационе технологије, Интерна ревизија – служба ИМС – управљање ризиком, Функција за финансијско економске послове, Функција за правне послове. У одређеним системима постоји једна организациона целина која може носити различите називе. То може бити сектор корпоративне безбедности, сектор безбедности или служба безбедности и заштите. Ове организационе целине у свом саставу могу имати ниже целине по називу одељење, служба, департмент или дирекција који обављају одређен делокруг послова из области корпоративне безбедности. Закључно, на шта је и део испитаника указао, корпоративна безбедност треба да буде посебна функција која ће имати своју организациону структуру – кровна организација која ће се бавити свим пословима безбедносног карактера. Као таква, она би била самостална и уз генералог директора, а кроз интерну регулативу имплементира на све организационе целине. Оваква организациона целина може имати ниже јединице у свом саставу, али би на овај начин, јасно били одређени надлежности и одговорности ове организационе јединице, њени сегменти, њени запослени, послови који се обављају, као и ланац руковођења. Дакле, све од наведених функција у неким системима спроводе се у оквиру једне организационе целине, док се у неким системима спроводе у оквиру две или више организационих целина које могу али не морају имати карактер „безбедносних" целина попут сектора људских ресурса.

У посматраним системима, корпоративна безбедност обухвата различите функције наведене у ранијим пасусима. Неке функције су обавезне према закону, док се друге функције успостављају на основу интерне регулативе, а у циљу заштите правних лица, у овом случају критичне инфраструктуре. У неким системима, све функције безбедносног карактера су интегрисане у једну организациону целину, док су у другим распоређене у више организационих целина или сектора. Конкретније, неколико система има једну целину за корпоративну безбедност која обавља све послове у области безбедности.

3. Приватно обезбеђење у великим техничким системима од значаја за одбрану (критична инфраструктура)[153]

Када је реч о служби обезбеђења, поједини системи имају сопствену службу обезбеђења, односно регистровани су за самозаштитну делатност, с тим да за одређене послове

[153] Поглавље се односи на ставове испитаника о примени одредаба Закона о приватном обезбеђењу.

обезбеђења користе услуге регистрованих правних лица за приватно обезбеђење. Системи попут ових, који поред самозаштитне делатности користе услуге регистрованих правних лица за приватно обезбеђење, имају такозвану комбиновану службу обезбеђења. Поједини системи искључиво изнајмљују услуге регистрованих правних лица за приватно обезбеђење, те се за њихове службе обезбеђења може рећи да су изнајмљене. Потенцијални проблем који се може јавити када је реч о изнајмљивању услуга приватног обезбеђења, а нарочито је изражен код безбедности критичне инфраструктуре, у основи се заснива на страном капиталу у власничкој структури правних лица за приватно обезбеђење. Наиме, добар део правних лица за приватно обезбеђење чије се услуге обезбеђења користе има бар удео страног власништва. Када би та правна лица из неког разлога добила забрану пословања на територији Републике Србије, то би значило престанак пружања услуга клијентима, као и необезбеђеност објеката које су до тада обезбеђивали. То би као последицу даље имало повећање изложености и рањивости објеката који су штићени, а посебно објеката критичне инфраструктуре.

Код њих се као главни разлог изнајмљивања ових услуга наводи се недовољност сопствених ресурса који би се користили за ову врсту послова. У неким случајевима је проблем број службеника које је потребно обезбедити, нарочито у оним системима где је флуктуација посетилаца велика, док је у другим случајевима у питању обученост и знање за обављање ових послова. Код система који искључиво изнајмљују услуге регистрованих правних лица за приватно обезбеђење као главни разлог због којег се не размишља о увођењу самозаштитне делатности наводи се неоправданост потребне инвестиције и исхода који би се постигли. У суштини, уложена средства не би дала жељене резултате, што значи да би добитак био мање вредан од почетног улагања. Код обе групе правних лица, разлог неувођења или неразвијања самозаштитне делатности у основи је најчешће новац, односно обим улагања новчаних средстава. Томе међутим треба додати и непостојање развијене или постојање недовољно развијене свести о свим предностима које самозаштитна делатност има упркос улагањима која свакако да постоје и да нису занемарљива. С обзиром на исплативост улагања у самозаштитну делатност на дугорочном плану, а и с обзиром на карактер објеката о којима је реч, важност који имају за државу и друштво, сматра се и више него оправданим размишљати у правцу развоја ове делатности. Самозаштита се намеће као квалитетније решење, јер, како сматра један од испитаника, добија се бољи квалитет услуга, обуке су квалитетније, већа је мотивисаност, већа је свеукупна контрола делатности.

Када је систем регистрован за обављање самозаштитне делатности, то га овлашћује и да под испуњеним условима врши „за себе“ (интерно), послове процене ризика у заштити лица имовине и пословања (Закон о приватном обезбеђењу, члан 45). Предност обављања послова процене ризика интерно налази се под претпоставком да лице запослено у систему за који се врши процена поред потребне лиценце има мултидисциплинарна знања и стручност, као и потребан ниво познавања процеса и активности система које га чине компетентнијим за обављање ове врсте посла од екстерног лиценцираног лица. Међу појединим испитаницима постоји слагање у погледу ризика „цурења информација“ када се послови ове врсте поверавају екстерним правним лицима. Поверљива информација оног тренутка када се преда престаје да буде поверљива. Овакав став доводи до питања да ли се екстерним правним лицима чине доступним све информације које су тражене ради израде процене ризика?! Следи питање, уколико се не доставе потпуне информације, да ли је и у којој мери процена ризика квалитетна?! С обзиром на то да се на основу ове процене израђују и друга документа попут планова (физичког и техничког) обезбеђења, квалитет процене ризика пренео би се и на квалитет тих других докумената. То би проузроковало упитност

квалитета и применљивости свих аката који се израђују на основу акта о процени ризика. Иако се испитаници у великој мери слажу око тога да лиценцирана лица за израду процене ризика имају одређена знања у погледу ове врсте посла, сматрају да је много боље да процену ризика ради лице које је запослено у систему за који се процена врши. На том основу се међутим долази до другог потенцијалног проблема, а то је стварна стручност овог лица (поред тога што има лиценцу), као и евентуални притисци руководства система да се процена изради тако да се добије „оно што се жели“, а не „оно што је реално стање ствари“. Чињеница је да се процена ризика израђује на основу прикупљених података, знања и искуства лица које исту израђује. Све од наведених елемената може бити упитно, те је неопходно одговорно приступити доношењу одлуке у вези са израдом документа овог типа. Уз то, према неким испитаницима, лица запослена у Министарству нису стручна да прегледају и оцењују те процене. Поменуте планове обезбеђења треба да раде запослени. Проблем се јавља што правна лица која пружају услуге обезбеђења могу да траже целокупне планове или делове из планова, чиме се ствара могућност да до планова дођу и лица која нису овлашћена, на пример, страни власници правних лица за обезбеђење. То, нарочито за критичну инфраструктуру, може бити велики проблем.

За разлику од послова процене ризика у заштити лица имовине и пословања и послова техничке заштите који се у веома малом броју система обављају интерно, најчешће изнајмљивана услуга приватног обезбеђења јесте вршење послова службеника обезбеђења (са или без оружја). Да би се обављала ова врста посла, као и код других послова приватног обезбеђења, неопходно је да лица која исте врше поседују лиценцу. У вези са наведеним, неки од испитаника сматрају да би било пожељно увести посебну лиценцу за службенике обезбеђења који послове приватног обезбеђења обављају у објектима или на локацијама који су идентификовани као критична инфраструктура.

Међу испитаницима постоје подељена мишљења када је у питању њихово задовољство квалитетом пружених услуга. У појединим системима, службеници обезбеђења извршавају своје послове на веома завидном нивоу, те нису идентификовани проблеми (нарочито не у погледу обучености, која за одређене послове мора бити испуњена). У једном од система указано је на то да нису идентификовани проблеми с обзиром на то да су прописани ниво сарадње и комуникације, одређена је опрема коју правна лица за приватно обезбеђење треба да обезбеде, као и да је дефинисана обавеза надокнаде штете која настаје уколико службеник обезбеђења направи пропусте у свом раду. Са друге стране, у појединим системима добијени одговори указују на незадовољство радом службеника обезбеђења. Међу проблемима који су уочени у раду службеника издвајају се: 1) немотивисаност, 2) старосна структура, 3) обученост и оспособљеност и 4) образовна структура.

Главни разлог немотивисаности лежи у чињеници да је реч о професији која је одувек плаћана минимално, што је чини се континуиран, као и тренутни тренд. Пракса показује да се велики део новчаних средстава која корисник улуга плати пружаоцу услуга задржава од стране пружаоца услуга, док се мањи део (најчешће је то законска минимална зарада или она предложена за ову врсту улуга) исплаћује службенику обезбеђења. Немотивисаност може бити проузрокована и лошим условима рада. Поједини испитаници су указали на то да се овај посао мало вреднује, па је и тешко наћи људе који ће задовољавати услове. На крају, чак и када службеници обезбеђења раде коректно свој посао, тешко је очекивати од њих какву заинтересованост за осматрање, опажање, указивање на догађаје који су потенцијално безбедносно значајни за систем.

Проблем старосне структуре огледа се у великом броју пензионисаних лица који су лиценцирани и запослени као службеници обезбеђења. Ставови су да лица одређених година не могу бити довољно спремни и приправни (и физички и психички) за

обављање ове врсте посла. Овај проблем се додатно усложњава на радним местима где се ради са оружјем. Узимајући у обзир степен потенцијалне угрожености система о којима је овде реч, намеће се као неопходно прописивање старосних услова када се расписује тендер за изнајмљивање услуга вршења послова службеника обезбеђења, а посебно са оружјем. Испитаници из система који припадају јавном сектору указали су на ограничења у погледу састављања тендера за изнајмљивање услуга приватног обезбеђења која намеће Закон о јавним набавкама. Са једне стране, тржиште услуга приватног обезбеђења није на завидном нивоу, док са друге стране проблем са јавним набавкама јесте тај што је један од критеријума избора најнижа понуда („најнижа понуђена цена"), а упитно је какав је квалитет тих услуга и какву заштиту они који су изабрани могу да пруже. Један од испитаника је издвојио као проблем доста споре процесе јавних набавки који би могли да се убрзају једино изменама одређених одредаба. Тржиште је и даље недовољно регулисано, те постоји простор за малверзације и намештање тендера. Такође, део испитаника је указао и на ограничена буџетска средства за ову врсту услуга (што у одређеној мери ограничава и квалитет услуга који се добије). Овај проблем немају они системи чије је руководство спремно да уложи значајна средства у ова питања, какви су обично системи чија су средства одвојена од државног буџета или системи који прате ниво безбедности који њихова организација има на међународном нивоу.

Када је реч о обучености, сва лица пролазе обуку пре добијања лиценце. Међутим, квалитет те обуке је упитан. Као резултат тога, добијају се лиценцирани службеници обезбеђења који једноставно нису обучени за посао који треба да обављају. Зато, неки испитаници су указали на релативно ниске критеријуме за полагање за лиценце за приватно обезбеђење. Уз то, испитаници указују на то да правна лица која изнајмљују услуге приватног обезбеђења не улажу довољно у обуку службеника обезбеђења, што додатно угрожава тржиште услуга приватног обезбеђења. На тај начин, системи који изнајмљују ову врсту услуга приморани су да поред специфичних обука (које морају да спроводе, како би се службеници упознали са активностима и пословима у конкретном систему) понављају и оне ствари које је требало службеници да науче и усвоје на основној обуци (за добијање лиценце). Према ставовима дела испитаника, додатни проблем односи се на законску одредбу да и Министарство унутрашњих послова може да спроводи обуку. Поставља се питање оправданости двојаке улоге коју ово Министарство има у вези са овим питањем. Зашто би овај субјекат вршио и обуку и спроводио стручни испит? Да ли је могуће да се оваквом одредбом створи простор за малверзације приликом полагања испита код оних лица која су обуку имала у поменутом Министарству? Такође, поставља се питање компетенције лица која би у Министарству спроводила ову врсту обуке?

Образовна структура је код неких испитаника такође препозната као разлог лошег квалитета услуга. Тренутно, Закон о приватном обезбеђењу прописује најмање средње образовање које лице мора да има да би могао да добије лиценцу. Међутим, одређени испитаници су изразили бојазан став према предлозима о изменама и допунама Закона где се овај степен спушта на нижи и прописује најмање основно образовање које лице мора да има да би могао да добије лиценцу. Питање је колико је лице способно да по питању знања савлада обуку за стицање лиценце, и уопште, колико је способно да обавља ову врсту послова с обзиром на године. Веома је тешко, можда и неизводљиво, постићи професионалност као једно од начела функционисања система националне безбедности прописивањем оваквих услова. Правна лица, предузетници и физичка лица која врше послове приватног обезбеђења јесу саставни елемент система националне безбедности и тиме њихова професинализација јесте неодвојива од професионализације целог система. Прописивањем да лица која врше послове приватног обезбеђења треба да имају најмање средње образовање, а нарочито основно образовање делује као активност чији је смер потпуно супротан оном којем се тежи у највишем стратешком акту државе. За неке

испитанике никако није адекватно да лица са средњом стручном спремом процењују ризике у системима од значаја за државу. Они сматрају да се захтеви овако озбиљног акта са оваквом стручном спремом не могу задовољити. У сваком случају, требало би прописати и посебне услове у погледу степена стручне спреме, тако да се постигне да лица на извршним пословима не могу имати вишу стручну спрему од руководиоца.

На крају, образовање је непосредно везано за професионализам и развој безбедносне културе. Безбедносна култура не само да је механизам за управљање системима и организацијама, већ њена улога лежи и у остваривању стратешких интереса. У том смислу, поставља се питање зашто се у предметном закону нигде не помиње Кодекс професионалне етике приватног обезбеђења Удружења за приватно обезбеђење Привредне Коморе Србије, као што је то урађено са Кодексом полицијске етике у Закону о полицији (члан 45)? Иако се у Кодексу професионалне етике приватног обезбеђења наводи да су само чланови Удружења у обавези да исти поштују, требало би нормативно уредити да сва правна лица и предузетници за приватно обезбеђење исти примењују, баш како је то учињено са Кодексом полицијске етике. У сваком случају, неопходно је поред континуираног обучавања, радити на подизању свести и нивоа безбедносне културе службеника обезбеђења. Тек са изградњом безбедносне културе могуће је говорити о развоју сарадње и партнерства између приватне и јавне безбедности.

У анализираним системима, уочавају се два модела организовања службе обезбеђења: 1) комбинована служба и 2) изнајмљена служба обезбеђења. Као главни разлог коришћења екстерних услуга приватног обезбеђења наводе се финансијска ограничења у погледу развоја или проширивања и унапређења сопствене службе. Квалитет услуга приватног обезбеђења варира. У неким системима, обезбеђење функционише на високом нивоу, док у другим постоје проблеми са мотивацијом, старосном структуром, обученошћу запослених и њиховим степеном образовања. Закључује се да професионализација система приватног обезбеђења захтева боље услове, улагање у обуку, као и повећање безбедносне културе. Сходно томе, Републици Србији требају законодавне и организационе промене које би побољшале квалитет и ефикасност приватног обезбеђења.

4. Сарадња организације корпоративне безбедности великих техничких система од значаја за одбрану (критична инфраструктура) са другим субјектима система националне безбедности

По питању сарадње корпоративне безбедности у критичној инфраструктури са другим субјектима система националне безбедности, испитаници нису били потпуно сагласни. Добијени одговори конрадикторни су, и пре свега зависе од области сарадње.

Досадашњу сарадњу са Министарством унутрашњих послова већина испитаника је оценила у основи позитивно – као солидну, добру, одличну, веома адекватну, на завидном нивоу. Ипак, како сматрају неки испитаници, могуће је да је сарадња адекватна јер је реч о специфичним делатностима, односно делатностима које су од значаја за функционисање државе. Овде се мисли на то да је сарадња неопходна за очување безбедности што је постављено за примарни задатак органима безбедности. Оваква оцена је делимично и претпостављена с обзиром на то да је Законодавац уредио бројне области у којима је сарадња овог Министарства или неке његове јединице са другим субјектима прописана и обавезна (области приватног обезбеђења, заштите од пожара и ванредних ситуација). Како је ово Министарство надлежно за остваривање и унапређивање безбедности грађана и имовине сарадња се остварује и у области сузбијања криминалитета, од спречавања корупције, идустријске шпијунаже, преко случајева отуђивања материјално-техничких средстава и друге имовине до случајева отицања тајних докумената, еколошких акцидената, процесуирања и осуде лица.

Сарадња се остварује и у односу на размену података, размену искустава, сталне саветодавне и практичне помоћи, спровођењем едукација или заједничким семинарима, пружањем материјално-физичке помоћи, донација. Један од испитаника подвукао је значај сарадње у организацијама које имају странце на одговорним местима, а од значаја су за функционисање државе.

Ипак, испитаници су идентификовали и неке недостатке са аспекта сарадње. На пример, поступци издавања лиценци за приватно обезбеђење могу бити доста дуги. Организација Министарства унутрашњих послова на локалном нивоу је у појединим сегментима рада таква да проузрокује такође одуговлачење поступака (логистички проблеми). Томе су додали и могућу смањену мотивисаност за рад или нестручност лица што такође проузрокује кашњења у административним поступцима. Неки испитаници су препознали као проблеме стручност запослених лица, као и њихову (не)информисаност. „Крутост“ у раду испољена кроз једноставно утврђивање постојања докумената који су обавезни, попуњавање „чек листа“ шта постоји а шта не, чиме систем располаже а чиме не, доводи до проблема за системе попут тога да се битно ремети модел организације. За неке испитанике сарадња чак и није довољног обима, јер Министарство унутрашњих послова „даје задатке и обавезе“, али не нуди помоћ у њиховом извршавању, те је некада од веће помоћи „комуникација са колегама из струке“, а често је и извршавање задатака „осуђено на самосналажење“. Према ставовима појединих испитаника Министарство унутрашњих послова нема контролну и надзорну функцију какву треба да има, што је повезано са недостатком кадрова у инспекцијским структурама.

Поједини испитаници су као посебан проблем издвојили и приступ који запослени у Министарству унутрашњих послова и службама безбедности имају према службеницима обезбеђења. Као објашњење, дата је ситуација када припадници јавне безбедности дођу на лице места на којем се налази службеник обезбеђења, а где је дошло до неког штетног догађаја. Уместо да се службеник обезбеђења третира као партнер, он се најчешће третира као „сметња” или „ризик”. Овакав проблем, сматра ова група испитаника, проистекла је можда и из неадекваних одредаба Закона о приватном обезбеђењу по питању услова које службеник обезбеђења треба да испуњава за добијање лиценце, а о чему је већ било речи.

На овакав став указује и Радивојевић у својој докторској дисертацији (2019, стр. 235). Недостатак обостраног поштовања полиције и приватне безбедности велики је проблем и препрека у остваривању јавно-приватног партнерства. У том међусубном односу, полиција себе види као субјекта безбедности са доста ексклузивнијом улогом. Истина је да су овлашћења полицијских службеника доста шира и озбиљнија. Истина је исто тако и да службеници обезбеђења имају извесне обавезе према полицијским службеницима, полицији или Министарству унутрашњих послова, те да полиција интервенише у извесним случајевима након интервенције службеника обезбеђења. Иако је Законодавац предвидео одређене линије њихове међусобне комуникације, уређујући ту комуникацију није користио терминологију која ће поспешити ту исту комуникацију. На пример, како овлашћени полицијски службеник може да „изда наређење“ службенику обезбеђења, Законодавац је већ једног службеника ставио у подређенији положај. Тако, сектор приватног обезбеђења остао је у подређеном положају у односу на полицију (Радивојевић, 2019, стр. 238).

Министарство унутрашњих послова није једини субјекат система националне безбедности за који су испитаници указали на ефикасну сарадњу. Како је реч о субјектима од значаја за државну критичну инфраструктуру, сарадња се остварује и са Министарством одбране укључујући Војску Србије и Војнообавештајну и Војнобезбедносну агенцију, као и са Безбедносно-информативном агенцијом, и ова

сарадња је оцењена као веома добра. Сарадња постоји и са другим министарствима, и то према функцијама корпоративне безбедности. У области заштите тајних података сарадња се остварује са министарством надлежним за правосуђе, у области безбедности и здравља на раду министарством надлежним за послове рада и министарством надлежним за послове здравља, у области заштите животне средине у првом реду са министарством надлежним за послове заштите животне средине. Закључно, сарадња се остварује са свим свим министарствима, органима и службама који имају додира са пословима корпоративне безбедности. Таква сарадња је у оквирима који су прописани законима и подзаконским актима, те су испитаници сагласни око тога да постоји простор да се та сарадња унапреди. С тим у вези, оно што је неопходно јесте допунити правни оквир конкретним одредбама о сарадњи.

Неки од испитаника су као пример који показује недовољну „бригу о критичној инфраструктури“ навели постављање центра за азил. Наиме, упитна је оправданост организовања прихватног центра, сада центра за азил, за мигранте у Обреновцу у непосредном окружењу ТЕНТ-а, као једног од највећих термоелектрана у Републици Србији, као и избегличког центра поред водовада (станица за пумпе и агрегате) у београдском насељу Борча.

Сарадња корпоративне безбедности критичне инфраструктуре са другим субјектима система националне безбедности није једнако оцењена од стране испитаника. Са једне стране, сарадња са Министарством унутрашњих послова у основи се сматра позитивном, међутим, са друге стране, издвајају се критике као што су дуги поступци издавања лиценци за приватно обезбеђење, нестручност запослених и одуговлачење административних процедура. Уз то, значајна је и критика која се односи на начин на који се полицијски службеници односе према службеницима обезбеђења, што је са једне стране последица неадекватне законске регулативе, док са друге стране ствара проблеме у развоју партнерства између полиције и приватног обезбеђења (службеника обезбеђења). Иако је и сарадња са другим субјектима система националне безбедности у основи оцењена као добра испитаници сматрају да постоји простор за унапређење сарадње кроз допуну правног оквира, и то са конкретним одредбама о сарадњи.

5. Нормативна уређеност области корпоративне безбедности и заштите критичне инфраструктуре

Уређеност области корпоративне безбедности посматра се у односу на функције корпоративне безбедности. Поједини испитаници сагласни су у ставу да је потребно увести концепт корпоративне безбедности у нормативни оквир. Део испитаника је указао на то да треба да постоји организациона целина на пример, у Министарству одбране, Министарству унутрашњих послова или чак Министарству привреде, попут Координационог тела које би се бавило успостављањем корпоративне безбедности у објектима критичне инфраструктуре, или бар оним објектима и системима који представљају државну имовину, а спадају у критичну инфраструктуру.

Испитаници су сагласни да су поједине области као што су безбедност и здравље на раду, поступање са тајним подацима, поступање са пословном тајном, заштита од пожара, заштита животне средине веома добро уређене позитивноправним оквиром. Иако постоје пропусти које Законодавац може да отклони у циљу унапређења рада и сарадње субјеката који су дужни да исту имају, испитанци сматрају да је регулаторни оквир у овим областима доста напредовао током времена и да је сада на сасвим завидном нивоу. Са друге стране, мишљења у вези са облашћу приватне безбедности нису толико позитивна. Поједини испитаници су истакли да је „физичко-техничка заштита била скрајнута“. Доношењем закона у овој области започело се са уређивањем ове области, уведен је нормативни оквир и успостављен је ред. Као и у претходном случају, и у овом

увек има простора за доградњу. Као главни проблеми препознати су услови за стицање лиценце за службеника обезбеђења који су исти за све врсте лиценци, а посебно питање потребног нивоа образовања. Код неких испитаника као проблем препозната је обавеза која проистиче из Закона о оружју и муницији, а тиче се плаћања пореза на оружје са којим службеници обезбеђења раде у одређеним системима и на одређеним пословима. Ови испитаници сматрају да је оружје „средство за рад“ и да би системи као објекти од значаја за државу који су регистровани за самозаштитну делатност и имају интерне службе обезбеђења које врше послове са оружјем требало да буду изузети од ове обавезе. Поред тога, један од испитаника поставио је питање добијања статуса овлашћеног службеног лица за службеника обезбеђења који ради са оружјем. Препознат је и проблем у вези са методологијом за израду акта о процени ризика у заштити лица, имовине и пословања (методологија из српског стандарда СРПС А.Л2.003:2025: Безбедност и отпорност друштва – Процена ризика – Захтеви и упутство за оцењивање усаглашености) која је опширна, неадекватна и веома често неприменљива. На пример, неке области овог акта су већ веома добро регулисане посебним регулативама, па се поставља питање „понављања већ реченог“.

Испитаници немају нарочито позитивна мишљења ни у вези са Законом о критичној инфраструктури. Као један од проблема који је уочен на основу добијених одговора издваја се чињеница да је Закон преписан и донет, по њима, ради испуњавања одређених политичких захтева. Постоји велико кашњење у примени закона, доношењу подзаконских аката и испуњењу других обавеза које проистичу из Закона. Поред проблема временског карактера – кашњења у вези са доношењем регулативе, испитаници су као проблеме истакли и извесне нејасноће које постоје у вези са идентификацијом критичне инфраструктуре, одређивањем официра за везу и садржајем безбедносног плана оператора. Још увек није јасно која организациона јединица Министарства унутрашњих послова треба да се бави заштитом и другим питањима у вези са критичном инфраструктуром. Неки испитаници сматрају да ови послови треба да остану у надлежности овог министарства с обзиром на то да не виде ко би се други бавио овим питањима. Њихови ставови су подељени по питању организационе целине која би требало да се бави овим питањима – једни сматрају да то треба да буде посебна организациона целина ван Сектора за ванредне ситуације, док други смратрају да је довољно да се формира посебна организациона целина у оквиру Сектора за ванредне ситуације. Неки испитаници су са друге стране, указали на то да је по њиховом мишљењу адекватније формирати посебно тело (министарство, агенција) која би се бавила искључиво питањима критичне инфраструктуре. Можда је најбоље следити најбоље праксе других држава по питању организовања надзора, контроле и координације заштите критичне инфраструктуре. Према неким испитаницима, министарства надлежна за критичну инфраструктуру по областима нису довољно заинтересована, те је неопходно најпре код њих пробудити свест о неопходности укључивања у целокупан систем заштите критичне инфраструктуре. Уз то, без обзира на то која би организациона целина вршила надзор, контролу и координацију, неопходно је да постоји спрега, сарадња и координација између тог субјекта (те организације) и објеката критичне инфраструктуре, као што и онај ко ради на терену мора знати који су објекти критичне инфраструктуре и које су њихове локације. Испитаници сугеришу да је неопходна измена Закона, усклађивање овог Закона са другим законима који дотичу ту област, а посебно са законима који се односе на рад Министарства унутрашњих послова, Министарства одбране, области управљања ванредним ситуацијама. Уз то, акценат треба ставити на идентификацију и анализу ризика, установити систем секторских мерила, дефинисати поверљиве податке који се односе на националну критичну инфраструктуру, прецизно одредити основ надзора, контроле и координације и инспекцијски надзор у области критичне инфраструктуре. Један од испитаника је чак

изразио став да би најбоље било „враћање на систем општенародне одбране“. Додатно, концепти и системи безбедности и заштите који су некада постојали оцењени су као и више него адекватни, нарочито од стране оних испитаника који су радили у таквим системима.

Иако је допринос законских прописа из области корпоративне безбедности на њен рад и функционалност неспоран, према неким испитаницима, објекти од значаја за државу нису адекватно законски третирани. Постоје бројни закони и подзаконски акти, али су они „несинхронизовани, нехармонизовани и неусаглашени“. Највећи број испитаника дели став да је неопходно даље развијати законски оквир, увести хармонију у тај законски оквир и обезбедити његову ефикаснију примену. Неопходно је исто тако примењивати прописано и реализовати задатке који су одређени, дати посебне задатке организацији корпоративне безбедности и то кроз њене функције под претпоставком да је раније таква организација прописана или бар успостављена. Неки испитаници одлазе корак даље сматрајући да постоји мали број закона и правних норми који се бави још увек недовољно истраженом облашћу корпоративне безбедности, док у области критичне инфраструктуре треба донети нови закон. Уз све то, неопходно је што пре напустити, сада већ честу, праксу спорог доношења подзаконских аката.

Када је реч о области корпоративне безбедности, испитаници се слажу да је потребно увести овај концепт у нормативни оквир, те су предложили формирање посебног тела које би се бавило корпоративном безбедношћу у објектима од значаја за функционисање државе. Испитаници деле мишљење да су многе области као што су безбедност на раду, заштита животне средине и заштита од пожара добро уређене, али област попут приватног обезбеђења још увек има проблеме, попут лиценцирања или обавезе плаћања пореза на оружје које су препознали као средство за рад. Закон о критичној инфраструктури такође има своје недостатке, као што су кашњења у примени и нејасноће у вези са идентификацијом и заштитом критичне инфраструктуре. Коначно, испитаници предлажу унапређивање појединачних закона кроз измене и допуне, и то посебно у областима приватног обезбеђења и критичне инфраструктуре, те њихово међусобно усаглашавање, као и усаглашавање са другим нормативним актима. Ово би поставило основе за потпуно правно и институционално уређење ових области, као и бољу координацију и сарадњу свих субјеката заинтересованих за заштиту критичне инфраструктуре.

6. Место и улога корпоративне безбедности великих техничких система од значаја за одбрану (критична инфраструктура) у систему националне безбедности

Улога корпоративне безбедности у систему националне безбедности различито је интерпретирана од стране испитаника. Неки испитаници истичу да је регулисана већ стратегијом, где се помиње као субјекат. У основи оваквог одговора пре је поистовећивање корпоративне безбедности са приватном безбедношћу или приватним обезбеђењем. Ипак, корпоративна безбедност није само физичко обезбеђење, већ су то све снаге правног лица које би реаговале у случају инцидената. Према другим испитаницима, корпоративна безбедност се ослања на приватну безбедност, али се за сада њена улога свела на сама правна лица, на индивидуалне одлуке руководиоца и одговорних лица. Један од испитаника је указао на неке од кључних фактора од којих зависи улога, попут величине система, степена достигнутости организовања корпоративне безбедности у систему, као и од послова корпоративне безбедности који се организују.

Испитаници су сагласни да је корпоративна безбедност неодвојив део система националне безбедности, јер је безбедност правних лица од великог утицаја на безбедност заједнице. Што су организација и функције корпоративне безбедности ефикасније то је већа и улога корпоративне безбедности у систему националне

безбедности, јер стабилност мањег система увек условљава стабилност већег. Успостављањем корпоративне безбедности утицало би се позитивно на заштиту критичне инфраструктуре, а тиме и на заштиту националних интереса. Ипак, постоји сагласност и око недостатка јединственог става шта је корпоративна безбедност и шта се под њоме убраја, око неинформисаности и код људи из струке и ван ње, што доводи до тога да су неки сегменти иако законски регулисани ипак остављени „на сналажење" приликом примене (активности иако законски регулисане за примену захтевају претходна знања, стручност и добру праксу). Сумирано, реч је о битном али још увек недовољно дефинисаном делу система националне безбедности. Концепт корпоративне безбедности још увек није препознат у Републици Србији, те у том контексту је неопходно више едукације, више приче о њеним бенефитима како у научним и стручним круговима тако и у широј јавности путем медија, веће афирмисање људи у власти који ће се бавити овим концептом и његовом имплементацијом.

Испитаници су сагласни у ставу да успостављена у организацији корпоративна безбедност може бити, треба да буде и јесте партнер Министарству унутрашњих послова и конкретније полицији у остваривању јавне, а потом и националне безбедности. У вези са партнерством организације корпоративне безбедности и других субјеката безбедности, испитаници су такође сагласни да партнерство треба и мора да постоји и на тим аспектима. Приликом успостављања партнерства неопходни су обострана свест и воља да се другој страни помогне и буде партнер, као и континуирана двосмерна комуникација и сарадња. Партнерство је један аспект који „захтева мала улагања, а даје значајне резултате".

Заправо, управо је партнерство један од предуслова пуног признања корпоративне безбедности у систему националне безбедности. Партнерство постоји, али га треба унапредити. Оно треба да буде развијано и унапређивано и са Министарством унутрашњих послова, али и са другим министарствима, органима, службама безбедности. У вези са наведеним значајан корак треба учинити у правцу елиминисања досадашње праксе да сви субјекти у систему „гледају само себе и раде само за себе".

Улога корпоративне безбедности у систему националне безбедности различито се интерпретира међу испитаницима. Неки је поистовећују са приватном безбедношћу, док други сматрају да зависи од самих правних лица, односно степена до којег је успостављена у правним лицима. Испитаници се слажу да је корпоративна безбедност важан део националне безбедности, јер стабилност критичне инфраструктуре где је успостављена корпоративна безбедност увек утиче на стабилност друштва и државе. У том контексту, подвлаче партнерство и континуирану сарадњу између сектора корпоративне безбедности критичне инфраструктуре и других субјеката система националне безбедности. Тренутно стање је такво да корпоративна безбедност није у потпуности препозната и призната у Републици Србији. То поставља захтеве за едукацијом о корпоративној безбедности, њеном промоцијом у стручним и ширим круговима што ће даље произвести не само њено признавање, успостављање и функционисање, већ и јачање система националне безбедности директно и кроз партнерства са другим субјектима кључним за стање безбедности државе.

7. Мишљење струке као предуслов унапређења стања безбедности

На крају, испитаници тренутно јесу или су били чланови професионалних или стручних удружења, или других стручних тела, те су и учествовали у различитим формама дијалога (састанцима и скуповима, јавним расправама на предложене законе, на научним и стручним конференцијама, семинарима, округлим столовима) који су били посвећени унапређењу приватне и корпоративне безбедности, као и заштите критичне инфраструктуре. Расправе које се воде на овим састанцима и скуповима углавном се

односе на тренутно стање. Под знаком питања је да ли се расправа води и по питању унапређења стања, као и да ли се дају конкретни предлози. У вези са тим, мала је могућност побољшања тренутног стања. Реч је о форумима где се размењују мишљења, предлажу допуне закона и других аката, дају други предлози од значаја за унапређење рада. Чињеница је да ова тела немају законодавну моћ, те једино могу да дају предлоге. Иако се долази до квалитетних закључака, често те расправе буду „јалове“, и све „остане на нивоу приче“. Неки испитаници су као предлог изнели чешће и редовније организовање састанака.

Са друге стране, неки испитаници су изразили врло позитивна мишљења у вези са резултатима ових састанака и скупова навевши да се „увек се ради на решењу, и увек се нађе решење“ или уважи предлог. Разлика у оваквим ставовима се међутим може приписати различитим делатностима у којима испитаници раде и у вези са тим врсти састанака и скупова, као и различитим областима у којима се расправе воде. У првом случају, постоје расправе које се воде по питању унапређења, а постоје и расправе које се воде у вези са неким проблемом те је тада и неопходно донети решење. У другом случају, испитаници су истакли да у области самозаштите, односно приватног обезбеђења расправа није напредовала много, док се у другим областима попут противпожарне заштите, безбедности и здравља на раду „чује реч и уважи предлог“.

Из добијених одговора, закључује се да је струка укључена у дијалоге који се баве унапређењем приватне и корпоративне безбедности и заштитом критичне инфраструктуре. Ипак, дијалози често не резултирају конкретним предлозима, а и када се до конструктивних закључака дође, они неретко остају на нивоу тих дијалога. И на овом месту, уочава се разилажење у ставовима испитаника у вези са доприносом који ови дијалози могу и треба да имају. На шта је већ указано, расправе у области самозаштите и приватног обезбеђења напредују спорије, док у другим областима као што су противпожарна заштита и здравље на раду постоји већа размена мишљења и реализација предлога.

5.1.1. Сумирани налази истраживања кроз помоћна истраживачка питања другог нивоа

У делу дисертације који се односи на коришћене методе истраживања, наведено је да се експертски интервју спроводи како би се добила сазнања која су од значаја за давање одговора првенствено на помоћно истраживачко питање првог нивоа *П2: У којој мери заштита критичне индраструктуре омогућава разумевање доприноса корпоративне безбедности на националну безбедност Републике Србије?.* Због своје комплексности, ово питање је рашчлањено на три додатна помоћна истраживачка питања, чији одговори су представљени у тексту који следи.

П2.1: На који начин је организован систем националне безбедности Републике Србије и у каквом је односу према корпоративној безбедности?

Систем националне безбедности Републике Србије организован је тако да се састоји од управљачког и извршног дела. Извршни део између осталих чине и субјекти приватне безбедности (правна лица, предузетници и физичка лица која врше послове приватног обезбеђења). Овако одређен у највишем стратешком акту државе – Стратегији националне безбедности, систем националне безбедности не препознаје корпоративну безбедност као засебни субјекат система. Одређење система националне безбедности уједно је и одредба са којом се отишло најдаље када је реч о препознавању концепта корпоративне безбедности у домаћој правној регулативи и то једино уколико се пође од тврдње да је корпоративна безбедност део приватне безбедности.

П2.2: *На који начин је корпоративна безбедност правно регулисана у Републици Србији и које су евентуалне мањкавости тренутног позитивноправног регулисања ове материје?*

Један од основних предуслова на основу којих корпоративна безбедност може да оствари своју улогу у систему националне безбедности јесте њена правна уређеност. Тренутно, Република Србија нема правни оквир којим ће се децидно уредити област корпоративне безбедности. Прецизније, како је већ наглашено, Законодавац још увек на простору Републике Србије није препознао и усвојио концепт корпоративне безбедности. Постоји низ, не потпуно хармонизованих, законских и других аката којима су уређене функције корпоративне безбедности, али појединачно. Одредбе тих нормативних аката омогућавају обављање послова корпоративне безбедности што је од суштинске важности за било које правно лице, а нарочито системе и објекте који су од значаја за функционисање државе и друштва.

Међутим, сматра се да би бољи резултати проистекли из обједињавања свих ових послова под окриљем једне целине. Увођење функција корпоративне безбедности у правни оквир Републике Србије био би први корак у успостављању функција корпоративне безбедности. На тај начин, сви субјекти националне безбедности развили би свест о новом концепту чија имплементација може да произведе бројне погодности. Уједно, и субјекти корпоративне безбедности (правна лица која су успоставила ову организацију) би постали свесни своје улоге у остваривању националне безбедности.

Још један предуслов, али не и мање важан јесте признавање улоге приватног обезбеђења у остваривању националне безбедности. То је у последње две деценије делимично учињено усвајањем Закона о приватном обезбеђењу 2013. године и пратећих подзаконских аката. У пракси још увек није у потпуности приватно обезбеђење прихваћено као део система националне безбедности. У извесној мери и због неадекватног законског оквира, о чему је било речи у раду, држава и полиција као традиционални субјекат јавне (унутрашње) безбедности не виде приватно обезбеђење као сарадника или партнера на плану остваривања националне безбедности. Тек када се то промени, и у потпуности прихвати приватно обезбеђење као равноправни субјекат са полицијом у систему националне безбедности, могуће је говорити о увођењу и уређењу области корпоративне безбедности тако да њена улога у остваривању националне безбедности буде призната.

П2.3: На који начин се критична инфраструктура Републике Србије штити и која је улога корпоративне безбедности у тој заштити?

Република Србија је релативно касно приступила системском нормативном регулисању заштите критичне инфраструктуре усвојивши Закон о критичној инфраструктури као матични закон у овој области тек 2018. године. До сада, по питању примене овог Закона није урађено пуно. Нису извршени идентификација и одређивање критичне инфраструктуре по секторима, нису одређени оператори критичне инфраструктуре, није одређен официр за везу у сваком оператору, нису усвојени Безбедносни планови оператора за управљање ризиком. Разлог неизвршавања одређених одредаба из Закона непознат је, и проузрокован је неиспуњавањем обавеза које је Законодавац прописао. Након више од пет година од ступања на снагу овог Закона, донесена је једино Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије.

Споведена анализа указује на то да у већини случајева, терминолошки, концепт корпоративне безбедности није препознат и усвојен као такав. Из тог разлога, изузев у малом броју случајева, тешко је говорити о улози корпоративне безбедности у заштити организација уопште, па тиме и у заштити критичне инфраструктуре. Са друге стране, није немогуће сусрести се са ситуацијом у којој у организацији овај концепт није

усвојен, али се примењује мањи или већи број њених функција. Тада, у зависности од функција које се примењују и њихове ефикасности достигнута безбедност може бити оптимална, истог нивоа као и безбедност која се постиже имплементацијом концепта корпоративне безбедности.

Функције корпоративне безбедности, у већој или мањој мери, активно се реализују у објектима критичне инфраструктуре, што применом закона, подзаконских аката и стандарда, што применом интерне регулативе које су обично донесене засебно за сваку функцију. Међутим, усвајањем концепта корпоративне безбедности са друге стране, обезбеђује се укупност свих функција безбедности у организацији, њихова планска и координисана примена чиме се уједно обезбеђује много већа успешност у области безбедности и укупном пословању.

5.2. Препоруке за развој доприноса корпоративне безбедности националној безбедности са акцентом на заштиту критичне инфраструктуре

У овом делу рада фокус је стављен на начине на које је могуће унапредити допринос корпоративне безбедности националној безбедности, са посебним нагласком на заштиту критичне инфраструктуре. У том контексту, дато је неколико препорука које је могуће разврстати на следећи начин:

1) израда званичних докумената из области безбедности који ће препознати корпоративну безбедност као субјекат система безбедности,
2) формирање посебних тела са координирајућом улогом у областима критичним за националну безбедност, као што је област заштите критичне инфраструктуре,
3) успостављање функционалне саветодавне групе у области корпоративне безбедности, укључујући и секторе корпоративне безбедности у критичној инфраструктури,
4) размена искустава између представника власти и представника из сектора корпоративне безбедности, укључујући и секторе корпоративне безбедности у критичној инфраструктури,
5) формирање центра за прикупљање и размену информација о могућим ризицима,
6) развијање свести о неопходности успостављања и спровођења корпоративне безбедности у организацијама,
7) унапређење сарадње и комуникације са свим заинтересованим субјектима по питању корпоративне безбедности уопште, па и по питању корпоративне безбедности успостављене у критичној инфраструктури.

Приликом израде званичних докумената из области безбедности потребно је посветити пажњу увођењу корпоративне безбедности и система који ће је подржавати. Корпоративна безбедност треба да обухвати све функције безбедности који се обављају у организацији укључујући и планирање континуитета пословања. Процес израде званичних докумената из области безбедности треба учинити таквим да се обезбеди што шире учешће свих заинтересованих субјеката, и плодоносним са што више решења и предлога. Поред тога, неопходно је постојање свести свих заинтересованих субјеката о потребама за безбедност и заштиту, као и воље за сарадњу и комуникацију, размену информација. Потребно је одредити надлежности и одговорности, као и успоставити основ за изградњу међусобног поверења. Проблем који се јавља у пракси јесте непотпуно разумевање могућности и ограничења државе као носиоца функције националне

безбедности, са једне стране и правних лица као носиоца функције корпоративне безбедности, са друге стране. Оно што је неопходно јесте да обе стране признају да и једна и друга страна имају значајну улогу и функцију у систему националне безбедности.

У оквиру министарства надлежног за унутрашње послове, било би од изузетне користи да се успостави организациона целина која ће бити одговорна за обезбеђивање, пренос информација о ризицима по националну безбедност и подршку индустрији у разумевању нових безбедносних питања. Посебно се препорука односи на безбедност критичних инфраструктура, те би та организациона целина вршила координацију над секторима безбедности објеката критичне инфраструктуре, односно над секторима корпоративне безбедности успостављених у овој групи правних лица.[154] Генерално, потребно је да постоји посебно тело или орган на координирајућем нивоу менаџмента у овој области који ће обухватити представнике управљачког и извршног дела система заштите критичне инфраструктуре.[155]

На оперативном нивоу, потребно је да постоји саветодавна група која би се састојала од менаџера из области корпоративне безбедности (попут менаџера безбедности, управљања ризицима), као и организација попут Српске асоцијације менаџера корпоративне безбедности и Удружења за приватно обезбеђење и остале услужне делатности, а посебно Групације за физичко обезбеђење, Групације за техничко обезбеђење, Групације за самозаштитну делатност (критичну инфраструктуру). Саветодавну групу би чиниле стручне организације и, још важније, стручна лица која добро познају начин функционисања, проблеме, као и простор за унапређење корпоративне безбедности.

Потребно је организовати форуме или радне групе о националној безбедности којима би присуствовали одговорна лица од стране извршне власти и руководиоци сектора корпоративне безбедности. Руководиоци сектора корпоративне безбедности треба да осигурају да се на тим форумима „чује“ глас непосредних извршиоца као лица која се током свог рада остварују најближи сусрет са проблемима у спровођењу функција корпоративне безбедности. Наведено је могуће постићи и тако што ће непосредни извршиоци присуствовати овим форумима или радним групама.

Потребно је да постоји програм упућивања владиних представника или представника из министарстава у објекте критичне инфраструктуре и њихове секторе корпоративне безбедности, како би се директно упознали са функционисањем корпоративне безбедности и проблемима са којима се суочава. Супротни правац јесте обезбеђивање учешћа представника из сектора корпоративне безбедности у вежбама које се односе на све аспекте националне безбедности, укључујући борбу против тероризма, ванредне ситуације, војну спремност и сајбер безбедност. Тако се јачају безбедносни аранжмани организација, укључујући увежбаност и ажурирање планова реаговања на инциденте и слично.

Потребно је формирати центар за прикупљање и размену информација о могућим ризицима. Центар може бити формиран за различите врсте ризика посебно или

[154] На пример, у Аустралији, формиран је Центар за сајбер безбедност и безбедност (критичне) инфраструктуре и налази се у оквиру Одељења унутрашњих послова. Овај центар ради у партнерству са владом, индустријом и широм заједницом на идентификацији и управљању ризицима националне безбедности за критичну инфраструктуру, и одговоран је за спровођење Закона о безбедности критичне инфраструктуре (Bergin, Williams and De Wilde, 2019, p. 3).

[155] На пример, у Аустралији постоји Поуздана мрежа за размену информација, у САД постоје координациона тела на нивоу сектора и на међусекторском нивоу, у Уједињеном Краљевству постоји Секретаријат за цивилне послове, у Канади координацију врши Национални међусекторски форум, у Шпанији постоји Национални сектор за заштиту критичне инфраструктуре (Стајић, Мирковић и Радивојевић, 2020, стр. 966).

обједињен за све врсте). То би требало да буде заједнички центар јавне и корпоративне безбедности, са двосмерном комуникацијом, анализом и планирањем у вези са различитим безбедносним ризицима. Центар треба да буде формиран на националном нивоу. Он може да обухвати различите области које захтевају заштиту, попут заштите критичне инфраструктуре. Центар који би био формиран у области заштите критичне инфраструктуре био би центар за прикупљање и размену информација у области или систему заштите критичне инфраструктуре. Информације које су суштинске за безбедност не треба да се задржавају како од стране владе и других државних органа тако ни од организација. Неопходна је обострана спремност и да се прича и да се слуша, те да се у другој страни увек види саговорник и партнер, а не неко ко захтева информације (обично су то држава и њене службе) или неко ко је у обавези да исте пружи (правна лица, посебно у приватном сектору, а посебно се могу издвојити, с обзиром на предмет рада, правна лица у приватном сектору безбедности). Неулазећи у све потенцијалне разлоге, постоји могућност задржавања релевантних информација и једне и друге стране проузроковано неповерењем, које опет може бити оправдано или не. Разлог за развој неповерења на пример може бити недовољан законски оквир заштите информација или раније искуство које је проузроковало повреду права на заштиту информација. Зато, доносиоци одлука треба нормативно да уреде формалне канале комуникације, како би осигурали двосмерни проток релевантних информација по националну безбедност, и тиме бар умањили, ако не и елиминисали неформалне токове. Иако је неформално долажење до информација некада лакши и бржи начин долажења до сазнања, а некада и једини могући, и иако је некада од неупитног значаја за безбедност, оно се може институционализовати и формализовати. Чињеница је да одсуство размене поузданих, тачних и правовремених информација оставља негативне последице по систем заштите критичне инфраструктуре. Често се међутим заборавља обим информација којим располажу организације, а која се могу користити као значајан ресурс за потребе националне безбедности.[156] Кадрови ових организација могу бити значајан извор експертизе за потребе националне безбедности. Када доносиоци одлука у једној држави „забораве“ на овакве ствари, онда не бива створена правна основа, а потом ни амбијент у којем ће се ресурси организација регулисано користити за потребе националне безбедности. Постојање правне основе некада није довољно, већ је неопходно уредити је тако да задовољава интересе обе стране, и државе и правних лица. Свакако, решење није да држава искоришћава ресурсе организација, док она издвајају огромне напоре за набавку, одржавање и коришћење истих. Такође, да би оваква интеракција била функционална, неопходно је да влада добро зна које организације могу да обезбеде ресурсе и који су то ресурси који могу бити обезбеђени. Са друге стране, организације треба да познају владине структуре и такође знају од кога могу тражити информације и на који начин.

Руководство организација треба да разуме да губици који настају услед недовољног степена безбедности њихових организација не утиче само на њихово пословање, већ утиче и на националну безбедност. Односно руководство организација треба да разуме да улагање у властиту безбедност значи улагање и у националну безбедност. Са друге стране, профитабилност приватног сектора ипак зависи од стања националне безбедности, те он не треба да буде орјентисан само на улагање у безбедност за себе, већ и на улагање у националну безбедност. Руководство организација треба да разуме потребу за успостављањем и спровођењем корпоративне безбедности која ће бити самостална целина, одговорна директно највишем руководству. Успостављање

[156] Треба следити фразу „усуди се да поделиш“ усвојену од стране правних лица у Аустралији, а која се заснива на заједничкој посвећености правног лица и владе побољшању партнерства у размени безбедносних информација (Bergin, Williams and De Wilde, 2019, p. 10).

корпоративне безбедности укључује и израду регулативе, спровођење едукације, вођење база података о ризицима по сопствену и националну безбедност. Регулатива обезбеђује основ за сваку даљу активност, едукација подиже степен свести о ризицима и заштити, као и степен безбедносне културе, док прикупљени подаци стварају основу за рад корпоративне безбедности, као и основ за сарадњу са другим субјектима укључујући надлежне органе у оквиру јавно-приватног партнерста у области заштите критичне инфраструктуре. На сва три начина, руководство организација доприноси безбедности државе.

Руководство организација треба да разуме потребу за сарадњом и комуникацијом како са другим организацијама јавног и приватног сектора, тако и са телима и представницима извршне власти, те узме учешће на заједничким форумима, радним групама, формираним телима или у заједничким вежбама. Иако се питања сарадње и комуникације могу дефинисати различитим стандардима, програмима или другим неформалним начинима, адекватан нормативни оквир би могао да произведе много боље и квалитетније резултате.

У основи, препоруке о којима је реч на овом месту за развој корпоративне безбедности (видети Табелу 10) и за развој заштите критичне инфраструктуре (видети Табелу 11) могуће је у основи разврстати у следеће:

- Унапређивање нормативног оквира;
- Јачање институционалних и стручних капацитета;
- Развијање и континуирана примена процедура и
- Унапређивање сарадње на националном и међународном нивоу.

Уколико се мере посматрају кроз призму три нивоа менаџмента, онда је могуће говорити о мерама на стратегијском, оперативном и тактичком нивоу. Стратегијски ниво у теорији и пракси има највиши ниво научне заснованости, а на овом месту ће се посматрати на највишем нивоу општости. Као такав, стратегијски ниво даје основне смернице за поступање без њихове разраде за примену. Оперативни ниво чини основне смернице стратегијског нивоа спремнијим за примену јер представља спону између теорије (стратегијског нивоа) и праксе (тактичког нивоа). Тактички ниво чини реализацију и материјализацију смерница могућим у пракси. Могуће је последња два нивоа схватити као операционализацију препорука те су табеле које следе организоване тако да се у првој колони налазе препоруке (стратегијски ниво), које се операционализују прво на ниво један (оперативни ниво), а потом на ниво два (тактички ниво).

Табела 10: Препоруке за развој корпоративне безбедности (Ауторка)

ПРЕПОРУКА	ОПЕРАЦИОНАЛИЗАЦИЈА	
	Ниво 1	**Ниво 2**
1. Унапређивање нормативног оквира	1.1. Континуирано развијати нормативни оквир корпоративне безбедности укључујући и њено препознавање као елемент система националне безбедности	Нормативни оквир корпоративне безбедности треба сагледати кроз нормативни оквир функција корпоративне безбедности. Самим тим, континуиран развој нормативног оквира функција корпоративне безбедности подразумева редовне измене и допуне тренутно важећих нормативних аката. Уз то, корпоративна безбедност треба да добије неопходну подршку и ресурсе за примену што у пракси значи обезбедити помоћ организацијама да ефикасно имплементирају нормативни оквир и раде у складу са истим. Интеграција корпоративне безбедности у систем националне безбедности зависи од неколико предуслова: 1) препознавање корпоративне безбедности као једне од кључних компоненти ширег система националне безбедности и 2) промовисање, развијање свести и разумевање улоге корпоративне безбедности у систему националне безбедности. Интеграцијом се признаје значајан утицај безбедности појединачних корпорација на националну безбедност у целини.
	1.2. Организовати размену знања и искустава о корпоративној безбедности у научним и стручним круговима	Окупљањем стручњака из области релевантних за корпоративну безбедност обезбеђује се комуникација и размена идеја, као и прикупљање различитих увида и долажење до препорука за унапређивање нормативног оквира функција корпоративне безбедности. Сходно томе, треба уважавати ставове стручне јавности утемељене на позитивним праксама и закључке који су проистекли из научних истраживања.
	1.3. Континуирано вршити надзор и контролу над применом нормативног оквира који уређује функције корпоративне безбедности	Надзор и контрола треба да омогуће континуирано праћење примене правних прописа чиме се осигурава њихова примена. То укључује: 1) редовно преиспитивање и процену начина на који се ови прописи примењују у организацији, 2) праћење међусобне усаглашености нормативног оквира са интерном регулативом и 3) идентификовање евентуалних проблема или пропуста у примени како би се исти кориговали. На овај начин, проактивно се обезбеђује правно усаглашено пословање, као и правовремено реаговање у случају пропуста или кршења норми. За интерну регулативу, од значаја су редовне ревизије и ажурирања. Обука запослених у примени правних прописа издваја се као предуслов одржавања интегритета регулаторног оквира.

Табела 10: наставак

ПРЕПОРУКА	Ниво 1	Ниво 2
2. Јачање институционалних и стручних капацитета	2.1. Успоставити организацију и функционисање корпоративне безбедности	Успостављање организације корпоративне безбедности подразумева креирање наменске безбедносне структуре унутар структуре организације који би био одговоран за континуирано управљање безбедношћу у организацији и систематично решавање проблема безбедносне природе. Успостављање правилног функционисања корпоративне безбедности могуће је једино кроз успостављање функција корпоративне безбедности.
	2.2. Обезбедити адекватну попуњеност, обученост и опремљеност кадрова организације корпоративне безбедности	Након успостављања организације корпоративне безбедности, да би се ефикасно реализовале активности и задовољиле њене функције неопходно је: 4) обезбедити и осигурати довољан број квалификованих лица за обављање послова безбедности, 5) набавити и одржавати опрему (на пример, средства техничке заштите) и средства за рад (средства која запослени користе за обављање послова из свог делокруга рада) који омогућавају што ефикасније обављање послова и извршавање активности функције корпоративне безбедности и 6) реализовати основну обуку како би запослени адекватно могли да одговоре на захтеве функција корпоративне безбедности.
	2.3. Обезбедити континуирану обуку и усавршавање, који треба да допринесу даљој професионализацији струке и јачању капацитета целокупног система корпоративне безбедности	Континуираним улагањем у едукацију кадра корпоративне безбедности, подиже се ниво његове обучености и оспособљености. Самим тим, јача се струка корпоративне безбедности и доприноси се јачању капацитета целокупног система безбедности. У циљу унапређења процеса обучавања и усавршавања треба унапређивати програме едукације и спроводити евалуације ради идентификовања области за побољшање.
	2.4. Интегрисати процедуре корпоративне безбедности у процесе менаџмента организације и свакодневну активност	Процедуре корпоративне безбедности у ширем смислу (процедуре које обезбеђују правилно обављање функција корпоративне безбедности од стране свих запослених) треба да буду усаглашене са општим циљевима организације. Тек тада је могуће исте укључити у процесе управљања и то кроз безбедносне процедуре. Овим се осигурава да се безбедност не третира као засебна или секундарна компонента, већ као интегрална компонента укупног функционисања и успеха организације. Адекватна безбедносна култура омогућава постојање свести која даље доприноси усвајању и имплементацији процедура. Примена процедура у свакодневним активностима доприноси позитивном размишљању о безбедности у организацији. Циљ наведених активности јесте створити безбедније окружење рада.

Табела 10: наставак

ПРЕПОРУКА	Ниво 1	Ниво 2
3. Развијање и континуирана примена процедура	3.1. Унапређивати начин поступања интерних субјеката корпоративне безбедности, а посебно интерних субјеката у ужем смислу	Да би се унапредио начин поступања интерних субјеката корпоративне безбедности, неопходно је обезбедити следеће: 7) јасно дефинисати улоге и одговорности, 8) осигурати приступ ресурсима неопходним за рад, 9) развијати и ажурирати јасне и детаљне процедуре рада, 10) дефинисати стандарде понашања или усвајити кодекс понашања, 11) подстицати побољшану комуникацију и координацију и 12) развијати посебне програме обуке који неће имати само функцију едукације већ и подизања свести.
	3.2. Неговати проактивни приступ	Негујући проактивни приступ, организације умањују вероватноћу угрожавања и нарушавања безбедности доприносећи тиме безбеднијем интерном и екстерном окружењу. Да би био делотворан, проактивни приступ треба да буде имплементиран у стратегије и политике организације, чиме се обезбеђује и његова доследна примена у пракси.
	3.3. Унапређивати оквир за прикупљање, дељење и заштиту података и информација у функцији доношења одлука	Прикупљање, дељење и заштита података и информација у основи зависи од систематизације радних места и процедуре рада оних који по систематизацији имају право и обавезе у вези прикупљањем, дељењем и заштитом података и информација. Заштита је неизоставни елемент руковања подацима и информацијама. Она обухвата неколико сегмената: 1) Нормативне мере (правне, организационе и кадровске), 2) Свест запослених о потреби за безбедност у вези са подацима и информацијама, 3) Физичко-техничке мере (физичка заштита, техничка заштита, физичко-техничка заштита или контрола приступа и процедуре рада) и 4) Едукација. Развијањем и унапређењем оквира који обезбеђује доступност, интегритет и поверљивост података побољшава се квалитет истих који се користе у доношењу одлука.
	3.4. Унапређивати оквир идентификације и процене ризика	Један од предуслова функционисања организације јесу идентификација и процена ризика. Побољшањем оквира за идентификацију и процену ризика, организације постају спремније да правовремено открију ризик и у складу са проценом делују према ризику обезбеђујући континуитет пословања.
	3.5. Остварити надзор и контролу над спровођењем процедура	Да би се обезбедио квалитетан процес надзора и контроле неопходно је најпре сачинити план надзора, односно контроле. Суштина ове две активности јесте пре свега унапредити примену прописаних процедура, и по потреби ревидирати исте у циљу унапређења рада и професионалнијег обављања активности прописаних процедурама.

Табела 10: наставак

ПРЕПОРУКА	Ниво 1	Ниво 2
4. Унапређивање сарадње на националном и међународном нивоу	4.1. Унапређивати комуникацију између корпоративне безбедности и екстерних субјеката корпоративне безбедности, односно других субјеката система националне безбедности	Због значаја који има, важно је да корпоративна безбедност оствари и континуирано унапређује комуникацију са екстерним субјектима корпоративне безбедности, односно са другим субјектима система националне безбедности (системи корпоративне безбедности других правних лица, државне институције попут Министарства унутрашњих послова, тужилаштва и судства, органи локалне самоуправе, научно-истраживачке институције, струковна удружења). Адекватна комуникација предуслов је за сарадњу и међусобну размену знања и искустава.
	4.2. Унапређивати сарадњу и подстицати размену знања и искуства на националном нивоу	Јачање сарадње и координације између организација корпоративне безбедности и екстерних субјеката корпоративне безбедности, односно других субјеката система националне безбедности по правилу доприноси изградњи партнерстава на националном нивоу. Даље, ова парнерства доприносе изградњи интегрисаног и кохезивног безбедносног окружења које је у стању да понуди ефикасније одговоре на претње и изазове, и на крају, допринесе сигурнијем окружењу. Сарадња би омогућила благовремено информисање о новим појавним облицима угрожавања, па и деловала едукативно и проактивно. Подстицање размене знања и искустава међу заинтересованим субјектима на националном нивоу омогућило би формирање информисаног окружења које је заинтересовано за сарадњу и погодно тло за унапређење безбедносних или других релевантних питања.
	4.3. Унапређивати сарадњу и подстицати размену знања и искуства на међународном нивоу	Под претпоставком да страни капитал постане већински власник правног лица (у овом случају система или објекта критичне инфраструктуре) неопходно је развијати сарадњу и неговати размену знања и искустава и на међународном нивоу. У првом реду размена знања би укључила сазнања и искуства у вези са облицима и носиоцима угрожавања, те мерама и добрим праксама које су дале позитивне резултате у проактивном и реактивном деловању система корпоративне безбедности.

Табела 11: Препоруке за развој заштите критичне инфраструктуре (Ауторка)

ПРЕПОРУКА	ОПЕРАЦИОНАЛИЗАЦИЈА	
	Ниво 1	**Ниво 2**
1. Унапређивање нормативног оквира	1.1. Континуирано развијати нормативни оквир заштите критичне инфраструктуре	Континуиран развој нормативног оквира заштите критичне инфраструктуре на овом месту би подразумевао измене и допуне постојећих, те усвајање нових нормативних аката којима ће се прописати обавеза увођења свих функција корпоративне безбедности у критичну инфраструктуру. Дакле, на националном нивоу, треба прописати обавезу критичних инфраструктура да имплементирају све функције корпоративне безбедности. То би значило, да функције корпоративне безбедности које нису уређене као обавезне, треба уредити као такве.
	1.2. Организовати размену знања и искустава о заштити критичне инфраструктуре у научним и стручним круговима	Окупљањем стручњака из области заштите критичне инфраструктуре обезбеђује се комуникација и размена идеја, као и прикупљање различитих увида и долажење до препорука за унапређивање нормативног оквира заштите критичне инфраструктуре. Сходно томе, треба уважавати ставове стручне јавности утемељене на позитивним праксама и закључке који су проистекли из научних истраживања.
	1.3. Континуирано вршити надзор и контролу над применом нормативног оквира заштите критичне инфраструктуре	Надзор и контрола треба да омогуће континуирано праћење примене правних прописа чиме се осигурава њихова примена. То укључује: 13) редовно преиспитивање и процену начина на који се ови прописи примењују у организацији, 14) праћење међусобне усаглашености нормативног оквира са интерном регулативом и 15) идентификовање евентуалних проблема или пропуста у примени како би се исти кориговали. На овај начин, проактивно се обезбеђује правно усаглашено пословање, као и правовремено реаговање у случају пропуста или кршења норми. За интерну регулативу, од значаја су редовне ревизије и ажурирања. Обука запослених у примени правних прописа издваја се као предуслов одржавања интегритета регулаторног оквира.
2. Јачање институционалних и стручних капацитета	2.1. Обезбедити адекватну попуњеност, обученост и опремљеност кадрова организационих целина и лица који се баве заштитом критичне инфраструктуре	Да би се обезбедила заштита критичне инфраструктуре неопходно је: 1) обезбедити и осигурати довољан број квалификованих лица за обављање послова безбедности, 2) набавити и одржавати опрему (на пример, средства техничке заштите) и средства за рад (средства која запослени користе за обављање послова из свог делокруга рада) који омогућавају што ефикасније обављање послова и извршавање активности функције корпоративне безбедности и 3) реализовати основну обуку како би запослени адекватно могли да одговоре на захтеве функција корпоративне безбедности.

Табела 11: наставак

ПРЕПОРУКА	Ниво 1	Ниво 2
2. Јачање институционалних и стручних капацитета – наставак	2.2. Обезбедити континуирану обуку и усавршавање, који треба да допринесу унапређењу заштите критичне инфраструктуре	Континуираним улагањем у едукацију кадра задуженог за заштиту критичне инфраструктуре, подиже се ниво његове обучености и оспособљености. Самим тим, не доприноси се само професионализацији лица која се баве заштитом критичне инфраструктуре, већ се индиректно јачају и капацитети целокупног система безбедности. У циљу унапређења процеса обучавања и усавршавања треба унапређивати програме едукације и спроводити евалуације ради идентификовања области за побољшање.
	2.3. Интегрисати процедуре заштите критичне инфраструктуре у процесе менаџмента организације и свакодневну активност	Процедуре којима се регулише област заштите критичне инфраструктуре треба да буду саставни део менаџмента. На тај начин, обезбеђује се да заштита критичне инфраструктуре буде третирана као интегрална компонента укупног функционисања критичне инфраструктуре, што она и јесте.
3. Развијање и континуирана примена процедура	3.1. Унапређивати начин поступања организационих целина и лица који се баве заштитом критичне инфраструктуре (унутар организације)	Да би се унапредио начин поступања лица који се баве заштитом критичне инфраструктуре, неопходно је обезбедити следеће: 1) јасно дефинисати улоге и одговорности, 2) осигурати приступ ресурсима неопходним за рад, 3) развијати и ажурирати јасне и детаљне процедуре рада, 4) дефинисати стандарде понашања или усвајити кодекс понашања, 5) подстицати побољшану комуникацију и координацију и 6) развијати посебне програме обуке који неће имати само функцију едукације већ и подизања свести. Када су лица која се баве заштитом критичне инфраструктуре спремна да ефикасно поступају у циљу заштите критичне инфраструктуре, тада су и организационе целине у којима та лица извршавају своје радне задатке такође спремна. На менаџменту јесте да јасно дефинише улоге и одговорности релевантних организационих целина, као и унапреди њихову међусобну комуникацију и координацију.
	3.2. Неговати проактивни приступ	Негујући проактивни приступ, критичне инфраструктуре умањују вероватноћу угрожавања и нарушавања безбедности доприносећи тиме безбеднијем интерном и екстерном окружењу. Да би био делотворан, проактивни приступ треба да буде имплементиран у стратегије и политике критичне инфраструктуре, чиме се обезбеђује и његова доследна примена у пракси.

Табела 11: наставак

ПРЕПОРУКА	Ниво 1	Ниво 2
3. Развијање и континуирана примена процедура – наставак	3.3. Унапређивати оквир за прикупљање, дељење и заштиту података и информација у функцији доношења одлука	Прикупљање, дељење и заштита података и информација у основи зависи од систематизације радних места и процедуре рада оних који по систематизацији имају право и обавезе у вези прикупљањем, дељењем и заштитом података и информација. Заштита је неизоставни елемент руковања подацима и информацијама. Она обухвата неколико сегмената: 1) Нормативне мере (правне, организационе и кадровске), 2) Свест запослених о потреби за безбедност у вези са подацима и информацијама, 3) Физичко-техничке мере (физичка заштита, техничка заштита, физичко-техничка заштита или контрола приступа и процедуре рада) и 4) Едукација. Развијањем и унапређењем оквира који обезбеђује доступност, интегритет и поверљивост података побољшава се квалитет истих који се користе у доношењу одлука.
	3.4. Унапређивати оквир идентификације и процене ризика	Један од предуслова функционисања критичне инфраструктуре јесу идентификација и процена ризика. Побољшањем оквира за идентификацију и процену ризика, критичне инфраструктуре постају спремније да правовремено открију ризик и у складу са проценом делују према ризику обезбеђујући континуитет пословања.
	3.5. Остварити надзор и контролу над спровођењем процедура	Да би се обезбедио квалитетан процес надзора и контроле неопходно је најпре сачинити план надзора, односно контроле. Суштина ове две активности јесте пре свега унапредити примену прописаних процедура, и по потреби ревидирати исте у циљу унапређења рада и професионалнијег обављања активности прописаних процедурама.
4. Унапређивање сарадње на националном и међународном нивоу	4.1. Унапређивати комуникацију између оператора критичне инфраструктуре и других субјеката система националне безбедности	Због значаја који има за државу, важно је да оператори критичне инфраструктуре континуирано унапређују комуникацију међусобно, као и са другим субјектима система националне безбедности. Адекватна комуникација предуслов је за сарадњу и међусобну размену знања и искустава. * Према важећој законској регулативи, официр за везу представља контакт између оператора критичне инфраструктуре и министарства надлежног за унутрашње послове. У том контексту, он би био адекватан посредник у комуникацији и сарадњи.

Табела 11: наставак

ПРЕПОРУКА	Ниво 1	Ниво 2
4. Унапређивање сарадње на националном и међународном нивоу – наставак	4.2. Унапређивати сарадњу и подстицати размену знања и искуства на националном нивоу	Јачање сарадње и координације између критичне инфраструктуре и других субјеката система националне безбедности по правилу доприноси изградњи партнерстава на националном нивоу. Даље, ова парнерства доприносе изградњи интегрисаног и кохезивног безбедносног окружења које је у стању да понуди ефикасније одговоре на претње и изазове, и на крају, допринесе сигурнијем окружењу. Сарадња би омогућила благовремено информисање о новим појавним облицима угрожавања, па и деловала едукативно и проактивно. Подстицање размене знања и искустава међу заинтересованим субјектима на националном нивоу омогућило би формирање информисаног окружења које је заинтересовано за сарадњу и погодно тло за унапређење безбедносних или других релевантних питања.
	4.3. Унапређивати сарадњу и подстицати размену знања и искуства на међународном нивоу	Под претпоставком да страни капитал постане већински власник система или објекта критичне инфраструктуре неопходно је развијати сарадњу и неговати размену знања и искустава и на међународном нивоу. У првом реду размена знања би укључила сазнања и искуства у вези са облицима и носиоцима угрожавања, те мерама и добрим праксама које су дале позитивне резултате у заштити критичне инфраструктуре.

5.3. Ограничења дисертације и могућности за даља истраживања

Функције корпоративне безбедности условљене су важећим законским и другим одредбама у свакој држави. То значи да стање нормативне уређености корпоративне безбедности у овој дисертацији је ограничено на подручје за које је анализа рађена, дакле за Републику Србију. Исто ограничење постоји и када је реч о анализи нормативне уређености заштите критичне инфраструктуре која је такође посматрана за Републику Србију.

За узорак експертског интервјуа узети су велики технички системи од значаја за одбрану посматрани као критична инфраструктура. Критична инфраструктура је много више од тога, али због непостојања листе објекта и локација који су одређени као критична инфраструктура, ауторка је ограничила узорак на већ поменуте велике техничке системе. Сходно томе, само део ових система је био посматран. У вези са наведеним, налази истраживања су условљени оваквим избором узорка, па је у будућим истраживањима могуће проширити узорак на више или све овакве системе под условом да се добије њихова сагласност за посматрање, односно учешће у истраживању. Такође, дефинисањем посебних критеријума могуће је листу критичне инфраструктуре проширити и на објекте који не представљају велике техничке системе од значаја за одбрану.

Интервју је обављен са лицима који су на руководећим пословима у области (корпоративне) безбедности, те се добијени налази заснивају на њиховим мишљењима и ставовима, односно на њиховом искуству. Уз то, испитаници као запослени у системима који су од значаја за функционисање државе и друштва могли су да дају део

података који није осетљив и на било који начин заштићен. У вези са тим, упитник је формулисан тако да не задире у степеноване документе правног лица, те је могуће да су неке предметно интересантне области изостављене, односно да су поједини одговори условљени.

У будућим истраживањима, постоји неколико могућности за истраживање које би могле да побољшају разумевање корпоративне безбедности, њене улоге у заштити критичне инфраструктуре и уопште у систему националне безбедности доприносећи кроз своју улогу и самој националној безбедности. Један од потенцијалних приступа јесте анализа начина на који се организује корпоративна безбедност, начина на које се њоме управља, начина њеног функционисања у различитим типовима организација, укључујући ту и објекте критичне инфраструктуре. То би чак могло и да омогући поређења између различитих организација и сектора, нудећи свеобухватнији поглед на динамику корпоративне безбедности у различитим контекстима. Када се сагледа и разуме концепт корпоративне безбедности на нивоу организација истог, али још боље, различитог карактера, могуће је извести закључке о постојању и степену имплементираности овог концепта на државном нивоу, наравно, у зависности од састава узорка. Један од потенцијалних приступа био би и анализа улоге појединачних функција корпоративне безбедности у заштити критичне инфраструктуре. На крају, будућа истраживања би могла да буду планирана са проширивањем узорка што је могуће извршити у два правца. Први правац односио би се на проширивање узорка тако да он обухвати већи број индивидуалних стручних (експертских) интервјуа, док би се други правац односио на формирање разноврснијег узорка који би поред категорије учесника који су били укључени у ово истраживање обухватио и друге категорије које су релевантне за предмет истраживања. Већи и репрезентативнији узорак дао би свеобухватнији увид у предмет истраживања.

Проширени приступ истраживања свакако да би као резултат имао богатији корпус нових сазнања на основу којег би било могуће развијати делотворније стратегије и препоруке. Такав корпус сазнања допринео би и бољем разумевању испитиваних феномена омогућавајући идентификовање проблема и потенцијалних решења, као и простора за изналажење најбољих пракси деловања и даљи развој. С тим у вези, као најделотворнији потенцијални истраживачни приступ издваја се комбинација експертског интервјуа и добро структурисане анкете.

6. ЗАКЉУЧНА РАЗМАТРАЊА

Корпоративна безбедност јесте пословна функција успостављена у организацији. Она је условљена законским оквиром државе у којој се успоставља, међународном регулативом, стандардима, добром праксом запослених на пословима корпоративне безбедности, као и интерним прописима организације. Поред тога, на корпоративну безбедност утичу свест о потреби за заштитом, расположиви финансијски ресурси и идентификоване кључне вредности. Као функција успостављена у организацији, она је независна од других функција. Усмерена је на остваривање циљева заштите и подршку постизању циљева организације што се остварује управо заштитом лица, имовине и пословања организације. Корпоративна безбедност организује се као организациона целина за себе, па је могуће рећи и да има сопствен систем. Следећи поставке Теорије система, о систему корпоративне безбедности је могуће говорити као о друштвеном, динамичном и отвореном систему. Као систем, корпоративна безбедност са једне стране обухвата правне, економске, социјалне, информационе и друге области који се налазе у узајамној интеракцији унутар система, док са друге стране, припада вишем пословном систему организације, као и вишим системима државе попут система приватне безбедности и система националне безбедности. Дакле, као елемент система приватне безбедности или субјекат приватног, недржавног секора безбедности, она припада систему безбедности државе.

Корпоративна безбедност има двоструку улогу у систему националне безбедности. Прво, штитећи организације доприноси стању безбедности у окружењу тих организација. Друго, индиректним јачањем економске безбедности помаже у одржавању друштвено-политичке стабилности и безбедности шире заједнице и државе. Унапређење безбедности организација и њиховог окружења и допринос економској безбедности остварује се управо кроз функције корпоративне безбедности. Дакле, корпоративна безбедност препозната је као елемент система националне безбедности.

Сваки аспект безбедности организације има вишеструки допринос. Тај допринос се пре свега огледа у позитивном утицају на свеукупну безбедност организације, а потом и безбедност шире заједнице. Када би се сви аспекти безбедности организације објединили под кровну организацију као што је она која одговара концепту корпоративне безбедности, обезбедио би се један свеобухватан, целовит и комплетан правац деловања на националну безбедност. У њој су обједињене све функције безбедности у организацији и у привредном систему. Обављајући основну делатност, корпоративна безбедност директно доприноси остваривању безбедности правних лица, њихове имовине и пословања, па тиме и широј безбедности државе. Функције корпоративне безбедности остварују се како проактивним тако и реактивним активностима у зависности од облика и извора угрожавања. Спроводе их запослени као интерни субјекти корпоративне безбедности. Из улоге корпоративне безбедности произилази и њена сврха, да допринесе остваривању циљева организације, као и националној безбедности.

Значај корпоративне безбедности у систему националне безбедности нарочито је важан када се у обзир узму организације чије функционисање обезбеђује основне производе и услуге које су од суштинског значаја за опстанак и дугорочни развој државе и друштва. Реч је о системима, као и свим објектима и локацијама који су одређени и идентификовани као критична инфраструктура. Наиме, национална критична инфраструктура није ништа мање но део система националне безбедности. Од ње зависи здравље и живот људи, имовина, животна средина, безбедност грађана, економска стабилност. Дакле, национална безбедност, као и свеукупно функционисање државе и

друштва зависни су од критичне инфраструктуре. Тако, један од предуслова националне безбедности и оптималног функционисања државе јесте управо заштита критичне инфраструктуре. Заштита критичне инфраструктуре један од примарних задатака било које државе јер она подупире физичке и логичке системе неопходне за подршку безбедности државе и чини могућим континуирано пружање предвиђених услуга заједници. У раду је заштита сагледана кроз јачање отпорности са једне стране, и остваривање и унапређење безбедности инфраструктуре са друге стране. То би значило постизање таквог степена отпорности критичне инфраструктуре да издржи и опорави се од поремећаја, односно имплементацију активности и мера за смањење вероватноће и утицаја криминалних и терористичких акција.

Циљ рада је да укаже на то да би најефикасније резултате у заштити критичне инфраструктуре обезбедила безбедност организована у посебној форми каква је корпоративна безбедност. Улога корпоративне безбедности у системима и објектима критичне инфраструктуре наиме двоструко доприноси националној безбедности. Са једне стране, обезбеђује услове за задовољавање основних потреба државе и друштва (пружање основних услуга или производа) одржавајући безбедно стање и континуитет радних процеса. Са друге стране, даје подршку функцији безбедности на националном нивоу за деловање у мирнодопским условима, а посебно за деловање у случају ратног или ванредног стања.

Резултати добијени екпертским интервјуом потврђују теоријски изнете ставове да је корпоративна безбедност баш као и критична инфраструктура значајни елемент система националне безбедности. Оне доприносе одржавању и унапређењу стања националне безбедности и уопште функционисању државе. Ипак, тренутно стање у ове две области није на адекватном нивоу.

О корпоративној безбедности не постоје документа правне снаге националног карактера. У пракси се она појављује тек у организацијама у којима су руководство и запослени препознали њен значај и бенефите, док се ефикасно имплементира у још мањем броју организација. Добра вест за теоретичаре и практичаре корпоративне безбедности јесте да још увек „има наде“ за развој и ширу имплементацију овог концепта. Иако не постоји терминолошки као „корпоративна безбедност“, у многим организацијама постоје безбедносне активности које су прописане интерним документима и које се спроводе. Иако су често ови документи, понекад и недовољно јасно написани, ограничени на активности које регулишу, њихово постојање представља добар почетак у спровођењу безбедносних активности јер их институционализује. Тако, уместо једног кровног документа о безбедносним активностима организације постоји неколико њих. Подељеност у односу на интерну регулативу проблем је који се сусреће и у односу на организациону целину која се бави безбедносним активностима. Тако, уместо једне организационе целине која се бави безбедносним активностима организације постоји неколико њих. Последица тога јесте подељеност и у односу на послове и активности безбедносног карактера који једноставно нису обједињени под једну кровну функцију.

Организације чији је кадар свестан предности које могу да проистекну из имплементираног концепта корпоративне безбедности на добром су путу да тај концепт имплементирају и развију. Ипак, неопходан предуслов за тако нешто свакако је свест и подршка менаџмента организације, као и улагања у развој система безбедности организације (система корпоративне безбедности). Системи у којима је менаџмент свестан важности корпоративне безбедности имају тенденцију да постижу боље резултате кроз континуирани развој интерних прописа, едукацију запослених и унапређење пословних процеса.

Дакле, не постоји организација која не спроводи безбедносну активност. Питање је које су те активности које спроводи, како су оне регулисане и на који начин се спроводе. Одговор на ова питања указује на степен развоја имплементираности безбедносних активности што индиректно може служити за извођење закључка о евентуалној усвојености и примени концепта корпоративне безбедности. Свакако, у Републици Србији мањка свест о овом концепту. Законодавство не препознаје потребу да функције корпоративне безбедности треба да буду обавезујуће за критичну инфраструктуру. Нико не наводи да ће се стање безбедности организације или друштва и државе погоршати уколико се овај концепт не усвоји. Циљ је био указати на његове карактеристике и добити које би запослени и организације, односно друштво и држава, могли да имају његовом имплементацијом. Дакле, у овом раду се наводи да би концептом корпоративне безбедности рад запослених на пословима безбедности у организацијама био уређенији са нормативног, организационог и функционалног аспекта и засигурно ефикаснији дајући боље резултате.

О заштити критичне инфраструктуре интензивније се говори тек једну деценију. Доношење регулативе из ове области поприлично заостаје, док се о имплементацији исте још теже може говорити. Управо због недостатака у одређењу објеката критичне инфраструктуре, за потребе истраживања узети су у обзир велики технички системи од значаја за одбрану, те су се закључци истраживања изводили из научног разговора обављеног са запосленима на руководећим пословима безбедности управо у тим објектима.

Корпоративна безбедност, односно њене функције могу и треба да буду предмет националног законодавног оквира, посебно у области заштите критичне инфраструктуре. Исто је и са заштитом критичне инфраструктуре као посебне области. Критична инфраструктура је основ функционисања државе и њеног становништва. Стога, уместо садашњег матичног закона који је неадекватан и недоследан, са политичким утицајем на његову израду, одложеном применом и нејасноћама у вези са његовим кључним аспектима релевантни органи треба уз саветовање са струком да предузму кораке ка ефикаснијем регулисању ове области заштите критичне инфраструктуре. То би био предуслов за постизање веће уређености ове области што повлачи са собом и већу безбедност критичне инфраструктуре.

На крају, могуће је закључити да корпоративна безбедност кроз заштиту критичне инфраструктуре може да допринесе националној безбедности Републике Србије неколико начина.

Прво, корпоративна безбедност имплементирана у објектима критичне инфрастуктуре директно утиче на то да ове инфраструктуре буду заштићене од различитих облика и носиоца угрожавања. Када је реч о угрожавању споља, у првом реду се издвајају спољашњи носиоци угрожавања и облици угрожавања попут тероризма и диверзије, док када је реч о угрожавању изнутра могли би да се издвоје облици попут саботаже или корупције. Услед развоја информационо-комуникационих технологија, све се више као облик угрожавања издвајају и сајбер напади. Интегрисана као свеобухватни систем у објектима критичне инфрастуктуре, она не само да штити од претњи, већ и омогућава наставак функционисања инфраструктуре у случају било каквих поремећаја. На тај начин, корпоративна безбедност имплементирана у објектима критичне инфрастуктуре последично подржава националну безбедност спречавањем поремећаја који би могли њу да наруше.

У заштити критичне инфраструктуре велику улогу имају Министарство унутрашњих послова и Министарство одбране као два министарства задужена за безбедност државе. Сходно томе, заштита критичне инфраструктуре захтева блиску координацију са овим органима и њиховим службама. Корпоративна безбедност, у овом контексту, може

помоћи да се премости јаз између субјеката приватног сектора који поседују или управљају критичном инфраструктуром, а данас их је све више, и државе, обезбеђујући благовремену размену информација и ефикасан одговор у случају безбедносних претњи.

Друго, корпоративна безбедност имплементирана у објектима критичне инфрастуктуре помаже у изградњи отпорности унутар критичне инфраструктуре применом стратегија управљања ризиком, креирањем планова за ванредне ситуације и обезбеђивањем брзог опоравка у случају инцидента. На тај начин, када се јача отпорност виталних објеката јача се и отпорност државе и друштва чији су то витални објекти. Последично, јачање отпорности критичне инфраструктуре доприноси да национална безбедност не буде угрожена током криза, односно да и у кризним временима буде способна да одржи бар минимални, а још боље оптимални ниво производње и пружања услуга становништву.

Треће, стабилност привреде директно зависи од заштите критичне инфраструктуре, јер било какви поремећаји у функционисању ових система могу да имају катастрофалне последице по економију. Стабилност привреде зависи и од могућности националне безбедности да обезбеди сигурност кључних економских средстава. У том контексту, корпоративна безбедност је спона између економије и државе. Односно како је економска безбедност основа националној безбедности, тако је корпоративна безбедност спона између економије и економских интереса и националне безбедности.

И четврто, функције корпоративне безбедности могу и треба да буду предмет нормативног регулаторног оквира, нарочито оног којим се функције корпоративне безбедности одређују као неопходне у заштити критичне инфраструктуре. На тај начин, обезбедило би се да корпоративна безбедност као елемент система националне безбедности буде од користи у идентификацији рањивости критичне инфраструктуре и буде субјекат заштите критичне инфраструктуре чиме би допринела укупној безбедности државе.

Коначно, корпоративна безбедност, кроз заштиту критичне инфраструктуре, директно доприноси одржавању националне безбедности обезбеђивањем континуитета у пружању основних производа и услуга, повећањем отпорности, заштитом економских средстава и обезбеђивањем координисаног одговора на претње.

7. БИБЛИОГРАФИЈА

„Council Directive 2008/114/EC of 8 Decembar 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" Official Journal of the European Union L, pp. 345-375, 23.12.2008.

„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" Official Journal of the European Union L, pp. 164–198, 27.12.2022.

9/11 Commission Report. (2004). Washington DC: National Commission on Terrorist Attacks Upon the United States.

Abrahamsen, Rita, and Williams, C. Michael. (2011). „Power and governance: Global assemblages and the security field". In: *Security Beyond the State: Private Security in International Politics* (pp. 89-121). Cambridge: Cambridge University Press.

Abrahamsen, Rita, and Williams, C. Michael. (2007). Securing the city: private security companies and non-state authority in global governance. *International relations* 21 (2), pp. 237-253.

Action Plan for Chapter 24. (2015). Доступно на: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eupregovori.bos.rs/progovori-o-pregovorima/uploaded/Akcioni%20plan%20za%20poglavlje%2024%20od%2023.%20januara%202015_1.pdf.

Adams, K. Thomas. (1999). The new mercenaries and the privatization of conflict. *Parameters* 29 (2), pp. 103-116.

Adams, Kevin, Hester, Patrick, and Bradley, Joseph. (2013). „A Historical Perspective of Systems Theory". In: A. Krishnamurthy and W. K. V. Chan (Eds.). *Proceedings of the 2013 Industrial and Systems Engineering Research Conference* (pp. 4102-4109).

Adams, M. Kevin, Hester, T. Peggy, Bradley, M. Joseph, Meyers, J. Thomas and Keating, B. Charles. (2014). Systems theory as the foundation for understanding systems. *Systems Engineering* 17 (1), pp. 112-123.

Addicted to food. (2019, 27. фебруар). NAPAD NA BEOGRADSKI VODOVOD! Akcija "Raduša '72". Доступно на: https://www.addictedtofood.me/napad-na-beogradski-vodovod-akcija-radusa-72/.

Alcaraz, Cristina, and Zeadally, Sherali. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection* 8, pp. 53-66.

Alexander, E. David. (2013). Resilience and disaster risk reduction: an etymological journey. *Natural Hazards and Earth System Sciences* 13, pp. 2707-2716.

Amin, Massoud. (2000). National infrastructures as complex interactive networks. *Automation, Control, and Complexity: An Integrated Approach* 3, pp. 263-286.

Aradau, Claudia. (2010). Security that matters: critical infrastructure and objects of protection. *Security Dialogue* 41 (5), pp. 491-514.

ASIS Foundation. (2009). *Compendium of the ASIS Academic/Practitioner Symposium, 1997–2008*. Virginia: ASIS Foundation.

ASIS International. (2024, February 26). *ASIS International and Security Industry Association Release "Complexities in the Global Security Market: 2024 Through 2026"*. ASIS International.

Доступно на: https://www.asisonline.org/publications--resources/news/press-releases/asis-and-sia-release-complexities-in-the-global-security-market-2024-through-2026/.

ASIS International. (n.d.). Доступно на: https://www.asisonline.org/.

Atanacković, Zoran. (1986). *Uvod u teoriju politike i političkih sistema*. Beograd: Naučna knjiga.

Avant, Deborah. (2004). The privatization of security and change in the control of force. *International Studies Perspectives* 5 (2), pp. 153-7.

Avant, Deborah. (2005). *The Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press.

Bajagić, Mladen. (2011). Razumevanje bezbednosti od antičkih vremena do savremenih pristupa. NBP. *Nauka, bezbednost, policija* 16 (2), str. 39-55.

Baker, H. George. (2005). „A vulnerability assessment methodology for critical infrastructure sites". In *DHS symposium: R and D partnerships in homeland security*. Institute for infrastructure and information assurance.

Бакић, Војислав (Ур.). (1976а). Друштвена самозаштита као теорија, политика и пракса заштите нашег друштва и његових вредности. *Анали Правног факултета у Београду* XXIV (1-2), стр. 19-46.

Бакић, Војислав (Ур.). (1976б). Друштвена самозаштита и друштвено-политички систем Југославије. *Анали Правног факултета у Београду* XXIV (1-2), стр. 47-59.

Baldwin, A. David. (1997). The Concept of Security. *Review of International Studies* 23 (1), pp. 5-26.

Baumeister, F. Roy, and Leary, R. Mark. (1997). Writing narrative literature reviews. *Review of general psychology* 1 (3), pp. 311-320.

Bayley, H. David, and Shearing, D. Clifford. (2001). *The New Structure of Policing. Description, Conceptualization, and Research Agenda*. Washington: U.S. Department of Justice, National Institute of Justice.

Beck, Ulrih. (2001). *Rizično društvo: u susret novoj moderni*. Beograd: Filip Višnjić.

Beck, Ulrih. (2011). *Svetsko rizično društvo: u potrazi za izgubljenom sigurnošću*. Novi Sad: Akademska knjiga.

Becker, M. Theodore. (1974). The place of private police in society. An area of research for the social sciences. *Social Problems* 21 (3), pp. 438-453.

Београдски водовод и канализација. (н.д.). *Корисни савети за коришћење воде у домаћинству*. Доступно на: https://www.bvk.rs/edukativni-sadrzaj/#av-tab-section-1-1-link.

Београдски водовод и канализација. (н.д.). Основни подаци. Доступно на: https://www.bvk.rs/osnovni-podaci/.

Bergin, Anthony, Williams, Donald, and De Wilde, Rhys. (2019). *From board room to situation room: Why corporate security is national security*. Australian Strategic Policy Institute.

Berkes, Fikret. (2007). Understanding uncertainty and reducing vulnerability: lessons from resilience thinking. *Nat. Hazards* 41 pp. 283-295.

Berle, A. Adolf, and Means, C. Gardiner. (1991). *The modern corporation and private property*. Nev Brunsvick; London: Transaction publishers.

Berzina, Ieva. (2020). From 'Total' to 'Comprehensive' National Defence: the Development of the Concept in Europe. *Journal on Baltic Security* 6 (2), pp. 1-9.

Beyani, Chaloka, and Lilly, Damian. (2001). *Regulating Private Military Companies*. London: International Alert.

Biringer, Betty, Vugrin, Eric, and Warren, Drake. (2013). *Critical Infrastructure System Security and Resiliency*. Boca Raton: CRC Press.

Blanchard, S. Benjamin, and Blyler, E. John. (2012). *System Engineering Management.* New Jersey: John Wiley & Sons.

Bogner, Alexander, and Menz, Wolfgang. (2009). In: A. Bogner, B. Littig and W. Menz (Eds.). *Interviewing Experts* (pp. 43-80). London: Palgrave Macmillan.

Boin, Arjen, and McConnell, Allan. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of contingencies and crisis management* 15, pp. 150-159.

Boin, Arjen, and Smith, Denis. (2006). Terrorism and Critical Infrastructures: Implications for Public-Private Crisis Management. *Public Money and Management* 26 (5), pp. 295-304.

Borodzicz, P. Edward, and Gibson, D. Stevyn. (2006). Corporate security education: towards meeting the challenge. *Security Journal* 19, pp. 180-195.

Bošković, Mićo, i Bošković, Dejan. (2011). „Neki aktuelni problemi od značaja za bezbednost i zaštitu korporacija". U: *Zbornik radova: „Razvoj sistema bezbjednosti i zaštita korporacija"* (10-22). Banja Luka.

Bošković, Mićo. (2006). *Osnovi detektivske delatnosti*. Novi Sad: Fakultet za pravne i poslovne studije.

Бошковић, Милица. (2017). *Индустријска безбедност и заштита*. Београд: Универзитет у Београду, Факултет безбедности.

Boulding, E. Keneth. (1985). Systems research and the hierarchy of world systems: General systems in special chaos. *Systems Research* 2 (1), pp. 7-11.

Boulding, E. Kenneth. (1956). General systems theory – the skeleton of science. *Management Science* 2, pp. 197-208

Brooks, Doug. (2000). Messiahs or mercenaries? The future of international private military services. *International Peacekeeping* 7 (4), pp. 129-144.

Brooks, G. Stephen. (2005). *Producing Security: Multinational Corporations, Globalization, and the Changing Calculus of Conflict*. New Jersey: Princeton University Press.

Brooks, J. David, and Corkill, D. Jeffrey. (2014). „Corporate Security and the Stratum of Security Management". In: K. Walby and R. K. Lippert (Eds.). *Corporate Security in the 21st Century* (pp. 216-235). Hampshire: Palgrave Macmillan.

Brooks, J. David. (2010). What is security: Definition through knowledge categorisation. *Security Journal*, 23 (3), pp. 225-239.

Brooks, J. David. (2013). Corporate Security: Using Knowledge Construction to Define a Practising Body of Knowledge. *Asian Journal of Criminology* 8 (2), pp. 89-101.

Brown, R. Lester. (1986). Redefining National Security. *Challenge* 29 (3), pp. 25-32.

Buckley, Walter. (1998). *Society – A Complex Adaptive System: Essays in Social Theory*. Amsterdam: Overseas Publishers Association.

Bures, Oldrich, and Carrapico, Helena. (2017). Private security beyond private military and security companies: exploring diversity within private-public collaborations and its consequences for security governance. *Crime Law Soc Change* 67, pp. 229-243.

Burnstein, Harvey. (1978). Beyond cops and robbers: a note on corporate security. *University of Michigan business review* 30 (2), pp. 30-32.

Burstein, Harvey. (1999). *Introduction to Security*. New York: Prentice Hall.

Button, Mark and George, Bruce. (2001). Government regulation in the United Kingdom private security industry: The myth of non-regulation. *Security Journal* 14 (1), pp. 55-66.

Buzan, Barry, Wæver, Ole, and de Wilde, Jaap. (1998). *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers.

Buzan, Barry. (1983). *People, States, and Fear: The National Security Problem in International Relations*. Brighton: WHEATSHEAF BOOKS LTD.

Buzan, Barry. (1991). *People, States and Fear. An Agenda for International Security Studies in Post-Cold War Era*. New York: Harvester Wheatsheaf.

Cabric, Marko. (2015). *Corporate security management: Challenges, risks, and strategies*. Oxford: Butterworth-Heinemann is an imprint of Elsevier.

Calder, D. James. (1987). New corporate security: The autumn of crime control and the spring of fairness and due process. *Journal of Contemporary Criminal Justice* 3 (4), pp. 1-34.

Čaleta, Denis. (2012). „The role of geopolitics and geoeconomics in providing corporate security". In: D. Čaleta (Ur.). *Corporate Security in Dynamic Global Environment - Challenges and Risks* (pp. 85-9). Ljubljana: Institute for Corporative Security Studies.

Caparini, Marina. (2006). „Applying a Security Governance Perspective to the Privatisation of Security". In: Alan Bryden and Marina Caparini (Eds.). *Private Actors and Security Governance* (pp. 263-284). LIT & DCAF.

Cardona, D. Omar. (2004). The Need for Rethinking the Concept of Vulnerability and Risk from a Holistic Perspective: A Necessary Review and Criticism for Effective Risk Management. In: G. Bankoff, G. Hilhorst, Dorothea (Eds.), *Mapping Vulnerability, Disasters, Development and People* (pp. 37-51). London: Earthscan.

Carley, M. Kathleen, and Gasser, Les. (1999). „Computational organization theory". In: G. Weiss (Ed.). *Multiagent systems: A modern approach to distributed artificial intelligence* (pp. 299-330). Massachusetts, London: MIT Press.

Carroll, B. Archie. (1979). A three-dimensional conceptual model of corporate performance. *Academy of Management Review* 4 (4), pp. 497-505.

Carroll, B. Archie. (2016). Carroll's pyramid of CSR: taking another look. *International journal of corporate social responsibility* 1 (3), pp. 1-8.

Centar za civilno-vojne odnose. (2008). *Privatne bezbednosne kompanije u Srbiji – prijatelj ili pretnja?.* Beograd: Centar za civilno-vojne odnose.

Chappuis, Fairlie. (2021). *Toolkit for Security Sector Reporting – Media, Journalism and Security Sector Reform*. Geneva: Geneva Centre for Security Sector Governance.

Chertoff, Michael. (2006). *National Infrastructure Protection Plan [NIPP]*. Homeland Security.

Chesterman, Simon and Lehnardt, Chia (eds). (2009). *From Mercenaries to Market: The Rise and Regulation of Private Military Companies*. Oxford: Oxford University Press.

Činčalová, Simona and Prokop, Martin. (2019). How is Corporate Social Responsibility Meant: Analysis of 100 Definitions. *Hradec Economic Days* 9 (1), pp. 112-120.

Claesens, Stijn. (2003). *Global Corporate Governance Forum*. Vashington DC: The World Bank.

Coaffee, Jon. (2009). Protecting the urban: The dangers of planning for terrorism. *Theory, Culture & Society 26* (7-8), pp. 343-355.

Cockayne, James. (2006). *Commercial security in humanitarian and post-conflict settings: an exploratory study*. New York: International Peace Academy.

CoESS. (2016). *Critical Infrastructure Security and Protection: The Public-Private Opportunity*. Belgium: Confederation of European Security Services.

Collective, C. A. S. E. (2006). Critical approaches to security in Europe: A networked manifesto. *Security dialogue* 37 (4), pp. 443-487.

Collier, J. Stephen, and Andrew, Lackoff. (2008). „The vulnerability of vital systems: how'critical infrastructure' became a security problem". In: M. Dunn and K. S. Kristensen (Eds.), *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation* (pp. 17-39). Routledge.

Commission of the European Communities. (2001). *GREEN PAPER: Promoting a European framework for Corporate Social Responsibility.* European Union.

Commission of the European Communities. (2006). *Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM/2006/0786 final*.

Cooper, M. Harris. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in society* 1 (1), pp. 104-126.

Crawford, Adam. (2006). „Policing and security as 'club goods': The new enclosures?" In: J. Wood and B. Dupont (Eds.). *Democracy, Society and the Governance of Security* (pp. 111-138). Cambridge: Cambridge University Press.

Crawford, Adam. (2012). „Plural policing in the UK: policing beyond the police". In: T. Newburn (Ed.). *Handbook of policing,* Second edition (pp. 175-209). Devon: Willan Publishing.

Cubbage, Christopher, and Brooks, David J. (2012). *Corporate Security in the Asia Pacific Region: Crisis, Crime, Fraud and Misconduct*. Boca Raton, FL: Taylor and Francis.

Cunningham, William C., and Todd H. Taylor. (1985). *The Hallcrest Report: Private Security and Police in America*. Portland, Oregon: Chancellor.

Dahlsrud, Alexander. (2008). How corporate social responsibility is defined: an analysis of 37 definitions. *Corporate social responsibility and environmental management* 15 (1), pp. 1-13.

Dalton, R. Dennis. (2003). *Rethinking Corporate Security in the Post 9/11 Era*. New York: Butterworth-Heinemann.

Damjanović, Dalibor, i Ristić, Aleksandar. (2022). „Zaštita i upravljanje kritičnom infrastrukturom, teorijska razmatranja sa osvrtom na međunarodna iskustva". U: L. Gostimirović i G. Maksimović (Ur.). *Diskurs o kritičnoj infrastrukturi* (str. 169-180). Doboj: Visoka poslovno tehnička škola; Banja Luka: Bezbjednosni istraživački centar.

Даничић, Милан, и Стајић, Љубомир. (2008). *Приватна безбједност*. Бања Лука: Висока школа унутрашњих послова.

Davidović, Dušan, Kešetović Želimir, and Pavićević, Olivera. (2011). „National Critical Infrastructure Protection in Serbia: The Role of Private Security". In: D. Čaleta and P. Shemella (Eds.). *Counter terrorism challenges regarding the process of critical infrastructure protection* (pp. 201-209). Institute for Corporative Security Studies - ICS; Center for Civil-Military Relations.

Давидовић, Душан. (2011). Приватна безбедност у Србији. У: В. Н. Цветковић (Ур.), *Ризик, моћ, заштита – Увођење у науке безбедности* (стр. 452-467). Службени гласник и Универзитет у Београду, Факултет безбедности.

Davidson, C. H. (1989). Towards a new discipline of security management: the need for security to stand alone as a management science. *Security Management* 1 (1), pp. 3.

DCSINT. (2006). *Handbook No. 1.02 Critical Infrastructure Threats and Terrorism*. Fort Leavenworth: US Army Training and Doctrine Command.

De Bruijne, Mark, and van Eeten, Michel. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. *Journal of contingencies and crisis management* 15 (1), pp. 18-29.

De Nevers, Renée. (2009). Private security companies and the laws of war. *Security dialogue* 40 (2), pp. 169-190.

De Waard, Jaap. (1999). The private security industry in international perspective. *European journal on criminal policy and research* 7, pp. 143-174.

Dempsey, S. John. (2010). *Introduction to private security*. Belmont: Wadsworth Cengage Learning.

Дирекција полиције. (2017а). *Стратешка процена јавне безбедности*. Министарство унутрашњих послова.

Дирекција полиције. (2017б). *Стратешки план полиције за период од 2018-2021. године – јавна верзија*. Министарство унутрашњих послова.

Dorussen, Han, Lenz, Hartmut, and Blavoukos, Spyros. (2005). Assessing the Reliability and Validity of Expert Interviews. *European Union Politics* 6 (3), pp. 315-337.

Драгишић, Зоран, и Радојевић, Кристина. (2014). *Безбедносни менаџмент*. Београд: Универзитет у Београду, Факултет безбедности.

Драгишић, Зоран. (2009). Систем националне безбедности – покушај дефинисања појма. *Војно дело* 61 (3), стр. 162-176.

Драгишић, Зоран. (2011). *Систем националне безбедности Републике Србије*. Београд: Универзитет у Београду, Факултет безбедности.

Драгишић, Зоран. (2013). Безбедност, стратегија, политика и систем. *Политика националне безбедности* 1/2013, стр. 109-125.

Драговић, Соња. (2013). Утицај корпоративизма на национални идентитет. *Култура полиса* 22, стр. 209-218.

Duffield, Mark. (2011). Total War as Environmental Terror: Linking Liberalism, Resilience, and the Bunker. *South Atlantic Quarterly* 110 (3), pp. 757-769.

Đukić, Anđelija, i Vuletić, Dejan. (2023). Organizacija sistema odbrane prema konceptu totalne odbrane na primeru Švajcarske, Švedske i Srbije. *Medjunarodni problemi* 75 (4), str. 621-647.

Ђукић, Станимир. (2018). Менаџмент у корпоративној безбедности и безбедност индустријских објеката–физичко техничка заштита. *Војно дело* 70 (2), стр. 220-239.

Ђукић, Станимир. (2019). Нарушавање јавног реда и мира као облик угрожавања унутрашње безбедности. *Војно дело* 71 (1), стр. 70-84.

Dulanović, Živko, i Džinović, Milenko. (1995). *Osnovi organizacije*. Beograd: FON management.

Dulić, Tomislav, and Kostić, Roland. (2010). Yugoslavs in Arms: Guerrilla Tradition, Total Defence and the Ethnic Security Dilemma. *EuropeAsia Studies* 62 (7), pp. 1051-1072.

Дуловић, Љубомир. (2019). *Становништво Републике Србије као чинилац система националне безбедности у условима глобалних економских процеса* (Докторска дисертација). Београд: Универзитет одбране, Војна академија.

Dunn Cavelty, Myriam. (2007). Critical Information Infrastructure: Vulnerabilities, Threats and Responses. *ICTs and International Security* 3, pp. 15-22.

Ђурић, Ђуро. (2016). *Корпоративно управљање, с посебним освртом на грађевинске компаније у Републици Србији* (Докторска дисертација). Београд: Универзитет Мегатренд, Факултет за пословне студије.

Ђурић, Слађана. (2010). Контрола квалитета квалитативних истраживања. *Социолошки преглед* 44 (4), стр. 485-502.

Ђурић, Слађана. (2013а). Квалитативни приступ у криминолошким истраживањима. *Теме-Часопис за Друштвене Науке* (03), стр. 1339-1359.

Ђурић, Слађана. (2013б). *Истраживање безбедности: квалитативни приступ*. Београд: Факултет безбедности.

Ђурић, Слађана. (2016). Интервјуисање експерата: специфичности и принципи примене. *Годишњак Факултета безбедности 2016*, стр. 11-28.

Dželetović, Milenko. (2020). Uvod u korporativno upravljanje i finansijsku funkciju poslovanja. Beograd: Inovacioni centar Fakulteta bezbednosti; Akademska misao.

Џигурски, Озрен. (2018). „Системско-структурни приступ у анализи и решавању безбедносних проблема корпорација – системски концепт". У: З. Кековић, И. Р. Димитријевић и Н. Шекарић (Прир.). *Корпоративна безбедност – хрестоматија* (стр. 253-276). Београд: Универзитет у Београду, Факултет безбедности.

Egan, Jude Matthew. (2007). Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems. *Contingencies and Crisis Management* 15 (1), pp. 4-17.

Ejdus, Filip. (2012). *Međunarodna bezbednost: teorije, sektori i nivoi*. Beograd: Službeni glasnik.

El Kalam, Abou Anas, Deswarte, Yves, Baina, Amine, and Kaâniche, Mohamed. (2009). PolyOrBAC: A security framework for Critical Infrastructures. *International Journal of Critical Infrastructure Protection* 2 (4), pp. 154-169.

ELCON. (2004). *The economic impacts of the August 2003 blackout*. Electric Consumers Resource Council.

ENISA. (2015). *Critical Information Infrastructures Protection approaches in EU*. ENISA.

ERR. (2019, October 28). *Storm shows Estonia not ready for crises yet*. ERR. Доступно на: https://news.err.ee/996815/storm-shows-estonia-not-ready-for-crises-yet.

EU-NATO Task Force on the Resilience of Critical Infrastructure. (2023). *Final Assessment Report*.

European Commission. (2020). *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities* (SWD/2020/358 final).

European Committee for Standardization. (2021). *Private security services - Protection of critical infrastructure - Part 1: General requirements* (EN 17483-1:2021). European Committee for Standardization.

European Union. (2023, August 23). *Disruption to Critical Infrastructure*. European Union. Доступно на: https://civil-protection-knowledge-network.europa.eu/eu-overview-risks/human-induced-risks/disruption-critical-infrastructure.

Farmer, D. Richard, Goett, Andrew, Musick, Nathan, Torregrosa, David, Hitchner, Roger, Moore, David, and Congressional Budget Office (US Congress). (2004*). Homeland Security and the Private Sector: A CBO Paper*. DTIC Document.

Fayol, Henri. (2016). *General and industrial management*. Ravenio Books.

Feaver, D. Peter. (2003). *Armed servants: Agency, Oversight, and Civil-Military relations*. Cambridge, MA: Harvard University Press.

Fekete, Alexander. (2011). Common Criteria for the Assessment of Critical Infrastructures. *International Journal of Disaster Risk Science* 2 (1), pp. 18-19.

Fischer, Robert, Halibozek, Edward and Walters, David. (2012). *Introduction to security* (10th edition). Butterworth-Heinemann.

Fisher, R. E., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Eaton, L. K., Haffenden, R. A., Hussar, N. E., Klett, M. S., Lawlor, M. A., Millier, D. J., Petit, F. D., Peyton, S. M., Wallace, K. E., Whitfield, R. G., and Peerenboom, J. P. (2010). *Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program* (No. ANL/DIS-10-9). Argonne: Argonne National Lab (ANL).

Fjäder, Christian. (2014). The nation-state, national security and resilience in the age of globalization. *Resilience* 2 (2), pp. 114-129.

Flynn, E. Stephen. (2015). *Bolstering Critical Infrastructure Resilience After Superstorm Sandy: Lessons for New York and the Nation*. Boston, Massachusetts: Northeastern University.

Форца, Божидар. (2019). Теоријско одређење функција система националне безбедности. *Безбедност* 61 (1), стр. 40-69.

Forca, Božidar. (2021). „Vrednosti, interesi i ciljevi u strategijama nacionalne bezbednosti“. U: Ž. Radosavljević (Ur.), *Pravo, ekonomija i menadžment u savremenim uslovima LEMiMA* (str. 421-448). Beograd: Univerzitet „Union – Nikola Tesla”.

Forst, Brian. (2000). The Privatization and Civilianization of Policing. *Criminal Justice* 2 (24), pp. 19-97.

Francis, Royce, and Bekera, Behailu. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab Eng Syst Saf* 121, pp. 90-103.

Гачић, Јасмина, и Шећеров, Прода. (2012). Ресурси Републике Србије у заштити критичне инфраструктуре од терористичких претњи. *Безбедност* 54 (3), стр. 160-176.

Гаћиновић, Радослав. (2017). Национална безбедност као кључни фактор у функционисању модерне државе. *Војно дело* 1/2017, стр. 87-97.

Гајић, Новак. (2020). Сложеност корпоративизма и тешкоће његовог разумевања и одређења. *Српска политичка мисао* (3), стр. 243-267.

Garcia, Mary Lynn. (2007). *Design and evaluation of physical protection systems*. Burlington: Elsevier.

George, Bruce and Kimber, Simon. (2014). „The History of Private Security and Its Impact on the Modern Security Sector“. In: G. Martin (Ed.). *The Handbook of Security* (pp. 21–40). London: Palgrave Macmillan.

Gerginova, Tatjana. (2016). „Role of corporate security“. In: G. Mesko and B. Lobnikar (Eds.). *Criminal Justice and Security in Central and Eastern Europe: Safety, Security, and Social Control in Local Communities* (pp. 490-497). Ljubljana: Faculty of Criminal Justice and Security.

Gerginova, Tatjana. (2017). The Term Corporation in Modern Global Conditions. *Proceeding of International University Travnik* VII (1), pp. 361-369.

Gerring, John. (1999). What Makes a Concept Good? A Criterial Framework for Understanding Concept Formation in the Social Sciences. *Polity* 31 (3), pp. 357-393.

Gill, Martin, and Hart, Jerry. (1997b). Private investigators in Britain and America: Perspectives on the impact of popular culture. *Policing: An International Journal of Police Strategies and Management* 20 (4), pp. 631-640.

Gill, Martin, and Hart, Jerry. (1997a). Exploring investigative policing: A study of private detectives in Britain. *The British journal of criminology* 37 (4), pp. 549-567.

Gjurovski, Marjan, and Alceski, Gjorgji. (2021). *The role of corporate security in the protection of critical infrastructure*. Repository of Ss. Cyril and Methodius University in Skopje.

Global Justice Now. (2016, September 12). *10 biggest corporations make more money than most countries in the world combined*. Global Justice Now. Доступно на: https://www.globaljustice.org.uk/news/10-biggest-corporations-make-more-money-most-countries-world-combined/.

Goddard, C. Scott. (2001). *Private military company: a legitimate international entity within modern conflict* (Doctoral dissertation). Fort Leavenworth, KS: US Army Command and General Staff College.

Gordon, Kathryn and Maeve Dion. (2008). *Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security*. OECD.

Graham, Stephen. (2009). The urban 'battlespace'. *Theory, Culture and Society* 26 (7-8), pp. 278-288.

Grizold, Anton. (1994). The concept of national security in the contemporary world. *International Journal on World Peace* 11 (3), pp. 37-53.

Grizold, Anton. (2000). Contemporary national security in the light of militarization and militarism. *Politička misao: časopis za politologiju* 37 (5), str. 128-143.

Haddaway, R. Neal, Bethel, Alison, Dicks, V. Lynn, Koricheva, Julia, Macura, Biljana, Petrokofsky, Gillian, Pullin, S. Andrew, Savilaakso, Sini, and Stewart, B. Gavin. (2020). *Eight problems with literature reviews and how to fix them. Nature Ecology & Evolution* 4 (12), pp. 1582-1589.

Hamidu, Ahmad, Haron, Md, and Amran, Azlan. (2015). Corporate social responsibility: A review on definitions, core characteristics and theoretical perspectives. *Mediterranean Journal of Social Sciences* 6 (4), pp. 83-95.

Harborne, Bernard, Dorotinsky, L. William, and Bisca, M. Paul. (2017). *Securing development: public finance and the security sector: a guide to public expenditure reviews in the security and criminal justice sectors.* Washington, DC: International Bank for Reconstruction and Development/The World Bank.

Hamada, Masanori. (2014). *Critical Urban Infrastructure Handbook*. Boca Raton: CRC Press.

Hart, Chris. (2001). *Doing a Literature Review: Releasing the Social Science Research*. London: SAGE Publications.

Hermann, F. Charles. (1982). Defining National Security. In John F. Reichart and Steven R. Sturm (Eds.). *American Defense Policy* (pp. 18-21). Baltimore: Johns Hopkins University Press.

Hess, Kären M. (2009). *Introduction to Private Security* (5th edition). Belmont: Wadsworth Cengage Learning.

Hobs, Tomas. (2004). *Levijatan*, preveo Borislav Mikulić. Zagreb: Naklada Jesenski i Turk.

Hofreiter, Ladislav, and Zvaková, Zuzana. (2017). „Theoretical Aspects of Critical Infrastructure Protection". In: A. Kravcov, E. Cherepetskaya, and V. Pospichal (Eds.). *Durability of Critical Infrastructure, Monitoring and Testing* (pp. 139-147). Singapore: Springer.

Holling, C. (1973). Resilience and stability of ecological systems. *Annual review of ecology and systematics 4*, pp. 1-23.

Holmqvist, Caroline. (2005). *Private security companies. The case for regulation*. SIPRI Policy Paper 9.

Homeland Security Council. (2007). *National Strategy for Homeland Security*.

IATA. (2010). *IATA Economic Briefing: The Impact of Eyjafjallajokull's Volcanic Ash Plume*. IATA.

Ietto-Gillies, Grazia. (2012). *Transnational corporations and international production: concepts, theories and effects*. Cheltenham, Northampton: Edward Elgar Publishing.

Илић, Предраг. (2012). О дефинисању и дефиницијама националне безбедности. *Војно дело* 64 (2), стр. 123-138.

Institute for Economics & Peace. (2013). *Global Peace Index 2013.* Sydney: Institute for Economics & Peace.

Institute for Economics & Peace. (2024). *Global Peace Index 2024: Measuring Peace in a Complex World.* Sydney: Institute for Economics & Peace.

International Convention against the Recruitment, Use, Financing and Training of Mercenaries, 4 December 1989 - Signatory States. (1989). International Committee of the Red Cross. https://ihl-databases.icrc.org/en/ihl-treaties/conv-mercenaries-1989/state-parties.

International Organization for Standardization. (2010). *Guidance on social responsibility* (ISO Standard No. 26000:2010).

International Security Ligue and CoESS. (2023). *Cyber-Physical Security and Critical Infrastructure*. Zollikofen: International Security Ligue; Brussels: CoESS.

ISO. (n.d.). Online Browsing Platform. Доступно на: https://www.iso.org/obp/ui#search

Иваниш, Жељко, Младеновић, Мирослав, и Драгишић, Зоран. (2006). *Политички систем*. Београд: Факултет цивилне одбране.

Ivanović, R. Aleksandar. (2017). Pojam i elementi nacionalne bezbednosti. *Pravne teme* 5 (9), str. 186-211.

Ivanović-Đukić, Maja. (2011). Podsticanje društveno odgovornog poslovanja preduzeća u funkciji pridruživanja Srbije EU. *Ekonomske teme* 1, str. 45-58.

Jackson, C. Mike. (1994). Critical systems thinking: beyond the fragments. *System Dynamics Review* 10 (2-3), pp. 213-229.

Jackson, Gregg. (1980). Methods for integrative reviews. *Review of Educational Research* 50 (3), pp. 438-460.

Jahier, Khan, Staff Officer Civil Protection Group, Civil-Military Planning and Support Section and Operations Division. (n.d.). *Critical Infrastructure Protection within NATO*. Brussels: Civil Military Planning and Support Section.

Јаковљевић, Владимир. (2010). Ресурси критичне инфраструктуре и њихов значај за управљање ванредним ситуацијама. *Годишњак факултета безбедности*, стр. 63-81.

Jakovljević, Vladimir, i Gačić, Jasmina. (2012). „Zaštita kritične infrastrukture u kriznim situacijama". U *Zbornik radova Međunarodna naučna konferencija Menadžment 2012, Mladenovac, 20-11. april 2012* (str. 280-286). Mladenovac: Fakultet za industrijski menadžment, ICIM plus-Izdavački centar za industrijski menadžment plus.

Jefferies, D. Ian. (2002). Private Military Companies – A Positive Role to Play in Today's International System. *Connections* 1 (4), pp. 103-125.

Јеличић, Горан, и Ковинић, Марина. (2017). Промене корпоративног управљања под утицајем процеса глобализације Међународне привреде – са освртом на Србију. *Култура полиса* XIV (33), стр. 433-449.

Joh, E. Elizabeth. (2005). Conceptualizing the Private Police. *Utah Law Review* 2005 (2), pp. 573-617.

Jones, Andrew. (2007). Critical infrastructure protection. *Computer Fraud & Security* (4), pp. 11-15.

Jones, Trevor and Newburn, Tim. (2002). The Transformation of Policing? Understanding Current Trends in Policing Systems. *British Journal of Criminology* 42, pp. 129-146.

Jones, Trevor, and Newburn, Tim. (2006). „Understanding plural policing". In: T. Jones and T. Newburn (Eds.). *Plural policing, a comparative perspective* (pp. 1-11). London: Routledge.

Jovanović, Milica. (2017). Korporativna društvena odgovornost kao determinanta održivosti. *Economics of Sustainable Development* 1 (1), pp. 93-107.

Jovanovic, S. Aleksandar, Chakravarty, Somik, and Jelic, Marjan. (2021). „Resilience and Situational Awareness in Critical Infrastructure Protection: An Indicator-Based Approach". In: V. Rosato and A. Di Pietro (Eds.). *Issues on Risk Analysis for Critical Infrastructure Protection* (Chapter 4). IntechOpen.

Јовић, Ц. Радован. (2000). Савремене концепције цивилне одбране у систему опште одбране, *Зборник Факултета цивилне одбране* 2, стр. 49-72.

Kakalik, S. James, and Wildhorn, Sorrel. (1971). *The Private Police Industry: Findings and Recommendations. Vol. I*. RAND Corporation study for the National Institute of Law Enforcement and Criminal Justice. Washington: Government Printing Office.

Kalesnikas, Rajmundas. (2003). Mesto i uloga privatnog obezbeđenja u policijskom radu država u tranziciji. *NBP. Nauka, bezbednost, policija* 8 (2), pp. 21-37.

Kalina, Iryna, Viktoriia Khurdei, Vira Shevchuk, Tetiana Vlasiuk, and Ihor Leonidov. (2022). Introduction of a Corporate Security Risk Management System: The Experience of Poland. *Journal of Risk and Financial Management* 15 (8), pp. 335.

Karagiannis, Georgios Marios, Cardarilli, Monica, Turksezer, Zehra Irem, Spinoni, Jonathan, Mentaschi, Lorenzo, Feyen, Luc, and Krausmann, Elisabeth. (2019a). *Climate change and critical infrastructure – storms*. European Union: Luxembourg.

Karagiannis, Georgios Marios, Turksezer, Zehra Irem, Alfieri, Lorenzo, Feyen, Luc, and Krausmann, Elisabeth. (2019b). *Climate change and critical infrastructure – floods*. European Union: Luxembourg.

Kast, E. Fremont, and Rosenzweig, E. James. (1972). General systems theory: Applications for organization and management. *Academy of management journal* 15 (4), pp. 447-465.

Kaufmann, Mariele. (2013). Emergent self-organisation in emergencies: resilience rationales in interconnected societies. *Resilience* 1 (1), pp. 53-68.

Кековић, Зоран, и Димитријевић, Иван. (2017). *Системи безбедности са системом безбедности Републике Србије*. Београд: Универзитет у Београду, Факултет безбедности.

Кековић, Зоран. (2011). *Системи безбедности*. Београд: Универзитет у Београду, Факултет безбедности.

Кековић, Зоран. (2018). „Појмовно одређење и садржај корпоративне безбедности". У: З. Кековић, И. Р. Димитријевић и Н. Шекарић (Прир.). *Корпоративна безбедност – хрестоматија* (стр. 13-37). Београд: Универзитет у Београду, Факултет безбедности.

Kempa, Michael, Carrier, Ryan, Wood, Jennifer and Shearing, Clifford. (1999). Reflections on the Evolving Concept of 'Private Policing'. *European Journal on Criminal Policy and Research,* 7 (2), pp. 197-224.

Кешетовић, Желимир, и Симоновић, Бранислав. (2009). Сектор корпоративне и приватне безбедности у Србији. *Годишњак Факултета безбедности*, стр. 147-171.

Kešetović, Želimir, Putnik, Nenad, and Rakić, Marko. (2013). „Possibilities of Improving Critical Infrastructure Protection in Countries in Transition". In: *National critical infrastructure protection regional perspective* (pp. 131-142). Belgrade: University of Belgrade, Faculty of Security Studies; Ljubljana: Institute for Corporative Security Studies.

Кешетовић, Желимир. (2008). *Кризни менаџмент*. Београд: Универзитет у Београду, Факултет безбедности.

Kesić, Zoran. (2009). *Privatni sektor u kontroli kriminaliteta*. Beograd: Dosije studio.

Кесић, Зоран. (2013). Популарни имиџ приватног детектива и његова демистификација. *Безбедност* 55 (2), стр. 84-105.

Kinsey, Christopher. (2005). Challenging international law: a dilemma of private security companies. *Conflict, Security and Development* 5 (3), pp. 269-293.

Kinsey, Christopher. (2006). *Corporate Soldiers and International Security: The Rise of Private Military Companies*. London: Routledge.

Kljajić, Zdenko, Mandžuka, Sadko, i Škorput, Pero. (2010). „Primjena ICT-a u upravljanju kritičnom infrastrukturom u tranzicijskim zemljama". U: *18. Telekomunikacioni forum TELFOR 2010* (str. 75-78). Beograd.

Кнежевић, Милош. (2016). Национална безбедност на темељу националних интереса: Просторне димензије националне безбедности Србије. *Политика националне безбедности* 2.2016, стр. 115-138.

Komazec, Nenad, i janković, Katarina. (2023). Kritična infrastruktura u kontekstu održivog razvoja: Izazovi i perspektive. U: *Naučno-stručna konferencija „Održivi razvoj-usklađivanje interesa ili nužna potreba"* (str. 21-32). Doboj: Visoka poslovno tehnička škola; Banja Luka: Bezbjednosni istraživački centar.

Koonce, M. Anthony, Apostolakis, G. E., and Cook, B. K. (2008). Bulk power risk analysis: Ranking infrastructure elements according to their risk significance. *International Journal of Electrical Power and Energy Systems* 30 (3), pp. 169-183.

Копања, Михајло. (2022). *Геополитички приступ утврђивању делотворности концепта велике стратегије обуздавања: студија случаја Сједињене Америчке Државе 1979-1989* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

Koubatis, Andrew, and Schonberger, Jorge Yerena. (2005). Risk management of complex critical systems. *International Journal of Critical Infrastructures* 1 (2/3), pp. 195-205.

Ковач, Митар. (2010). Основни документи националне безбедности. У: В. Н. Цветковић (Ур.), *Ризик, моћ, заштита – Увођење у науке безбедности* (стр. 170-199). Београд: Службени гласник и Универзитет у Београду, Факултет безбедности.

Ковачевић, Сретен. (1980). *Основи система Друштвене самозаштите*. Београд: Виша школа унутрашњих послова.

Kovacich, L. Gerald, and Halibozek, P. Edward. (Eds.). (2003). *The manager's handbook for corporate security: Establishing and managing a successful assets protection program*. Oxford: Butterworth-Heinemann.

Kozarev, Atanas. (2017). Relacije između korporativne bezbednosti u Republici Makedoniji i državnog bezbednosnog sektora. *Zbornik radova Internacionalnog univerziteta Travnik* V (9), str. 38-45.

Krahmann, Elke. (2009). *Private security companies and the state monopoly on violence: a case of norm change?* PRIF-Reports No. 88. Frankfurt am Main: Peace Research Institute Frankfurt.

Krstić, Ostoja. (2008). „Policija i privatni sektor bezbednosti". U: *Privatna bezbednost: stanje i perspektive: zbornik radova: prvi međunarodni skup* (str. 63-75). Novi Sad: Fakultet za pravne i poslovne studije.

Kruck, Andreas, and Spencer, Alexander. (2013). Contested stories of commercial security: self- and media narratives of private military and security companies. *Critical Studies on Security* 1 (3), pp. 326-346.

Лабовић, Дејан. (2015а). *Приватна безбедност – Правна и социјална димензија*. Београд: Иновациони центар Факултета безбедности.

Лабовић, Дејан. (2015б). *Приватна безбедност у Републици Србији-правни аспекти и компаративна искуства* (Докторска дисертација). Крагујевац: Универзитет у Крагујевцу.

Лалић, Велибор, Ћеранић, Предраг, и Сикимић, Милица. (2019). Приватна и/или корпоративна безбједност: Да ли постоје концептуалне сличности и разлике? *ЖУРНАЛ ЗА БЕЗБЈЕДНОСТ И КРИМИНАЛИСТИКУ* 1 (1), стр. 53-68.

Larkin, Brain. (2013). The politics and poetics of infrastructure. *Annual review of anthropology* 42, pp. 327-343.

Last, David M. (2007). „Evolution of Policing and Security: What it Means for Diverse Security Sectors". In: *Conference, Defending Democracy Accommodating Diversity in the Security Sector Queen's University School of Policy Studies November 1-3, 2007*.

Leander, Anna. (2004). *Eroding State Authority? Private Military Companies and the Legitimate Use of Force*. Soveria Mannelli: Rubbettino.

Lečić, Boriša. (2018). „Place and role of corporate security in the national safety system". In: D. Trivan (Ed.). *Contemporary concept of corporate security* (pp. 175-191). Belgrade: Faculty of Business Studies and Law, University „Union-Nikola Tesla", Wien: Austrian Institute for European and Security Policy/AIES, Ljubljana: Institute for Corporative Security Studies, ICS.

Lee, Elsa. (2008). *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection*. Boca Raton: Crc Press.

Leffler, P. Melvyn. (1990). National Security. *Journal of American History* 77 (1), 143-152.

Lewis, G. Ted. (2006). *Critical infrastructure protection in homeland security: defending a networked nation*. New Jersey: John Wiley and Sons.

Li, Hao, Rosenwald, W. Gary, Jung, Juhwan, and Liu, Chen-Ching. (2005). Strategic power infrastructure defense. *Proceedings of the IEEE* 93 (5), pp. 918-933.

Li, Wenjia, Kodeswaran, Palanivel, Jagtap, Pramod, Joshi, Anupam, and Finin, Tim. (2012). Managing and Securing Critical Infrastructure – A Semantic Policy and Trust-Driven Approach. In: Das, S. K., Kant, K. and Zhang, N. (Eds.). *Handbook on Securing Cyber-Physical Critical Infrastructure: Foundations and Challenges* (pp. 551-573). San Francisco: Morgan Kaufmann.

Липовац, В. Милан. (2016). *Национална безбедност Републике Србије у регионалном безбедносном поткомплексу Западни Балкан* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

Lippert, K. Randy, Walby, Kevin and Steckle, Rhys. (2013). Multiplicities of corporate security: Identifying emerging types, trends and issues. *Security Journal* 26 (3), pp. 206-221.

Lippert, K. Randy, and Walby, Kevin. (2014). „Critiques of corporate security: Cost, camouflage and creep". In: M. L. Gill (Ed.). *The handbook of security* (pp. 881-899). New York: Palgrave Macmillan.

Lippman, Walter. (1943). *U.S. Foreign Policy: Shield of the Republic*. Boston: Little, Brown and Company.

Litavski, Jan. (2012). Izazovi privatnog sektora bezbednosti u novom veku. *Novi vek, Tromesečnik Centra za evroatlantske studije*, novembar 2012.

Little, G. Richard. (2002). Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. *Journal of Urban Technology* 9 (1), pp. 109-123.

Loader, Ian, Goold, Benjamin and Thumala, Angélica. (2014). The moral economy of security. *Theoretical criminology* 18 (4), pp. 469-488.

Lok, Džon. (2002). *Dve rasprave o vladi*, preveli Kosta Čavoški i Nazifa Savčić. Beograd: Utopija.

Longstaff, Patricia. H., Armstrong, Nicholas J., Perrin, Keli, Parker, Whitney May, and Hidek, Matthew A. (2010). Building resilient communities: A preliminary framework for assessment. *Homeland security affairs* 6 (3), pp. 1-23.

Ludbey, Codee Roy, Brooks, David Jonathan, and Coole, Michael Patrick. (2017). Corporate security: identifying and understanding the levels of security work in an organisation. *Asian Journal of Criminology* 13 (2), pp. 109-128.

Luhmann, Niklas. (2001). *Društveni sistemi: osnovi opšte teorije.* Novi Sad: Izdavačka knjižarnica Zorana Stojanovića.

Luiijf, Eric, Nieuwenhuijs, Albert, Klaver, Marieke, van Eeten, Michael, and Cruz, Edite. (2008). „Empirical findings on critical infrastructure dependencies in Europe". In: *International Workshop on Critical Information Infrastructures Security* (pp. 302-310). Berlin, Heidelberg: Springer Berlin Heidelberg.

Lukas, Ludek, and Hromada, Martin. (2011). Resilience as main part of protection of critical infrastructure. *International journal of mathematical models and methods in applied sciences* 5 (6), pp. 1135-1142.

Lundborg, Tom, and Vaughan-Williams, Nick. (2011). Resilience, critical infrastructure, and molecular security: The excess of "life" in biopolitics. *International Political Sociology* 5 (4), pp. 367-383.

Magestro, Brandon. (2013). Transitional phase of a security manager: A closer look into the struggles and difficulties experienced during the transition into security management. *Journal of Applied Security Research* 8 (1), pp. 135-150.

Mandel, Robert. (2001). The Privatization of Security. *Armed Forces & Society* 28 (1), pp. 129-151.

Мандић, Горан Ј. (2020). „Корпоративна безбедност – пословна функција правног лица". У: В. Н. Цветковић (Прир.). *Науке безбедности – врсте и облици* (стр. 167-182). Београд: Универзитет у Београду, Факултет безбедности.

Мандић, Ј. Горан, и Станојевић, Петар. (2020). *Корпоративна безбедност*. Београд: Универзитет у Београду, Факултет безбедности.

Maogoto, Nyamuya Jackson and Sheehy, Benedict. (2006). Contemporary Private Military Firms Under International Law: An Unregulated «Gold Rush». *Adelaide Law Review* 26 (2), pp. 1-23.

Маринковић, Немања. (2016). *Однос спољне политике и националне безбедности* (Докторска дисертација). Београд: Универзитет у Београду, Факултет политичких наука.

Marjanović, Marjan, i Ćupić, Danilo. (2017). Korelacija korporativne i nacionalne bezbjednosti. *Kriminalističke teme – Časopis za kriminalistiku, kriminologiju i sigurnosne studije* XVII (5), str. 490-509.

Marjanović, Marjan. (2020). *Teorijski i normativni okvir zaštite kritične infrastrukture u Crnoj Gori* (Doktorska disertacija). Beograd: Univerzitet „Union – Nikola Tesla", Fakultet za poslovne studije i pravo.

Марковић, Јана. (2021). Континуитет пословања као функција корпоративне безбедности (Мастер рад). Београд: Универзитет у Београду, Факултет безбедности.

Марковић, Јана. (2023а). Стратегија националне безбедности и унутрашња безбедност – Анализа за Републику Србију. У: *Зборник радова са конференције Стратешки и нормативни оквир Републике Србије за реаговање на савремене безбедносне ризике* (стр. 76-92). Београд: Универзитет у Београду, Факултет безбедности.

Марковић, Јана. (2023б). Улога корпоративне безбедности у заштити критичне инфраструктуре Републике Србије. *Безбедност* 65 (2), стр. 197-214.

Марковић, Јана. (2023в). Безбедност информација у функцији управљања континуитетом пословања. *Савремене студије безбедности* 1 (2), стр. 11-28.

Марковић, Ратко. (2010). *Уставно право*. Београд: Правни факултет Универзитета у Београду и Службени гласник.

Marković, Slobodan. (2007). *Osnovi korporativne i industrijske bezbednosti*. Novi Sad: Fakultet za poslovne i pravne studije.

Marković, Slobodan. (2014). Filozofija korporativne bezbednosti. *CIVITAS* (7), str. 9-22.

Markusen, R. Ann. (2003). The case against privatizing national security. *Governance* 16 (4), pp. 471–501.

Mašić, Branislav, i Dželetović, Milenko. (2015). *Uvod u menadžment*. Beograd: Inovacioni centar Fakulteta bezbednosti; Akademska knjiga.

Maslow, H. Abraham. (1943). A theory of human motivation. *Psychological Review* 50 (4), pp. 370-396.

McFate, Sean. (2014). *The Modern Mercenary : Private Armies and What They Mean for World Order*. Oxford University Press.

Međunarodna finansijska korporacija. (2011). *Korporativno upravljanje – Priručnik*. Beograd: Međunarodna finansijska korporacija.

Merabti, Madjid, Kennedy, Michael, and Hurst, William. (2011). „Critical infrastructure protection: A 21 st century challenge“. In: *International Conference on Communications and Information Technology (ICCIT)*. IEEE.

Meyer, Claire. (2024, February 26). N*ew Report Measures Global Size, Economic Weight of Physical Security Industry.* ASIS International. Доступно на: https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2024/february/complexities-global-security-market-report/.

Мићовић, Марија Д. (2020). *Специфичности критичне инфраструктуре у Републици Србији*. Београд: Криминалистичко-полицијски универзитет.

Mihaljević, Branko. (2018). Protection of critical national infrastructure: challenges for the private security sector. *Annals of Disaster Risk Sciences* 1 (1), pp. 47-56.

Mijalković, Saša, i Milošević, Goran. (2011). Korelacija ekonomske, korporativne i nacionalne bezbednosti. *Megatrend revija* 8 (2), str. 479-96.

Мијалковић, Саша, и Милошевић, Горан. (2010). „Угрожавање корпоративне безбедности и последице по националну безбедност“. У: *Дани безбједности на тему „Корпоративна безбједност - ризици, пријетње и мјере заштите* (стр. 287-296). Бања Лука.

Мијалковић, Саша, и Поповић, Марија. (2015). *Увод у студије безбедности*. Београд: Криминалистичко-полицијска академија.

Мијалковић, Саша. (1998). Угрожавање безбедности државе. *Војно дело* 2, стр. 169-189.

Мијалковић, Саша. (2009). *Национална безбедност*. Београд: Криминалистичко-полицијска академија.

Мијалковић, Саша. (2015). *Национална безбедност.* Београд: Криминалистичко-полицијска академија.

Милковски, Вангел, и Божић, Сандра. (2023). Концепт тоталне одбране у стратегији одвраћања Републике Србије. *Српска политичка мисао* 80 (2), стр. 7-32.

Milenković, Dejan. (2019). *Savremene teorije i moderna uprava*. Beograd: Čigoja.

Милетић, Слободан, и Талијан, Момчило. (2011). *Јавна безбедност – послови и начини рада, организација и руковођење*. Нови Сад: Факултет за правне и пословне студије др Лазар Вркатић.

Miljević, Milan. (2007). *Metodologija naučnog rada*. Pale: Filozofski fakultet.

Millon, David. (1990). Theories of the Corporation. *Duke LJ*, pp. 201-262.

Милосављевић, Богољуб. (1997). *Наука о полицији*. Београд: Полицијска академија.

Milosavljević, Bogoljub. (2014). Prilog teorijskopravnom određenju pojma bezbednosti. *Pravni zapisi* V (1), str. 95-119.

Milosavljević, Branislav, and Štrbac, Katarina. (2024). The Concept of Total Defense Options of the Republic of Serbia. *Security science journal* 5 (1), pp. 43-59.

Милосављевић, Бранислав, и Вучинић, Драган. (2021). Однос према критичној инфраструктури у Републици Србији. *Војно дело* 73 (4), стр. 42-56.

Милосављевић, Бранислав. (2019). *Безбедносна процена као чинилац стратегије националне безбедности Републике Србије* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

Милосављевић, Славомир, и Радосављевић, Иван. (2013). *Основи методологије политичких наука*. Београд: Службени гласник.

Милошевић, М., и Младеновић, М. (2017). Управљање правним ризицима као елемент корпоративне безбедносне политике. *Српска политичка мисао* 24 (3), стр. 289-230.

Милошевић, Милан. (2001). *Систем државне безбедности*. Београд: Полицијска академија.

Milošević, Milan. (2017). Normativni okviri korporativne bezbednosti u Republici Srbiji: aktuelno stanje i perspektive razvoja. *Zbornik radova Internacionalnog univerziteta Travnik* V (9), str. 30-37.

Milošević, Nenad and Jukić, Jadranko. (2017). Private military and security companies: Legal, moral and social implications. *Vojno delo* 69 (7), str. 161-173.

Мишев, Гордана. (2022). *Фактори успешног развоја држава и њихове импликације на безбедност* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

Moesgaard, Christa. (2013). *Private military and security companies-from mercenaries to intelligence providers*. Danish Institute for International Studies.

Monks, Robert, and Minow, Nell. (2011). *Corporate Governance*. West Sussex: John Wiley & Sons.

Moteff, D. John, and Parfomak, Paul. (2004). *Critical Infrastructure and Key Assets: Definition and Ientification, Congressional Research Service*. Washington, DC: Congressional Research Service, Library of Congress.

Moteff, D. John, Copeland, Claudia, and Fischer, W. John. (2003). *Critical infrastructures: What makes an infrastructure critical?*. Washington, DC: Congressional Research Service, Library of Congress.

МУП РС. (2019). *Процена ризика од катастрофа у Републици Србији*. Министарство унутрашњих послова Републике Србије.

Murray, T. Alan, and Grubesic, H. Tony. (2012). Critical infrastructure protection: The vulnerability conundrum. *Telematics and Informatics* 29 (1), pp. 56-65.

Murray, Tonita, and McKim, Erica. (2003). Полиција и сектор приватне безбедности: шта доноси будућност. *Безбедност* 4, стр. 635-646.

Национална стратегија одрживог развоја. (2008). *Службени гласник РС*, бр. 57/2008.

Нацрт закона о критичној инфраструктури. (2018). Доступно на: https://www.paragraf.rs/dnevne-vesti/270418/270418-vest18.html.

Najman, Velizar. (1979). *Uređivanje društvene samozaštite: zakonodavstvo, teorija, praksa*. Šabac: Dragan Srnić.

Nalla, Mahesh and Morash, Merry. (2002). Assessing the scope of corporate security: Common practices and relationships with other business functions. *Security Journal* 15 (3), pp. 7-19.

Nalla, Mahesh and Newman, R. Graeme. (1990). *A primer in private security*. New York: Harrow and Heston.

National Counter Terrorism Security Office. (n.d.). *Guidance Project Griffin*. GOV.UK. Dostupno na: https://www.gov.uk/government/publications/project-griffin/project-griffin.

National Infrastructure Advisory Council. (2009). *Critical Infrastructure Resilience, Final Report and Recommendations.* Washington, DC: U.S. Department of Homeland Security.

National Strategy for Critical Infrastructure Protection (CIP Strategy). (2009). Federal Republic of Germany, Federal Ministry of the Interior.

NATO. (2016). NATO Summit Guide. Dostupno na: https://www.nato.int/cps/en/natohq/topics_134190.htm.

NATO. (2024, July 08). *Resilience, civil preparedness and Article 3*. NATO. Dostupno na: https://www.nato.int/cps/en/natohq/topics_132722.htm.

Neuman, W. Lawrence. (2012). *Basics of social research: qualitative and quantitative approaches* (Third Edition). London: Pearson Education Limited.

Newburn, Tim and Reiner, Robert. (2007). „Policing and the police". In: M. Maguire, R. Morgan, and R. Reiner (Eds.). *The Oxford Handbook of Criminology* (pp. 910-952). Oxford: OUP.

Nikač, Željko, i Pavlović, Gojko. (2012). *Pravo privatne bezbednosti*. Beograd: Kriminalističko-policijska akademija.

Nikač, Željko. (2013). *Privatna bezbednost i detektivska delatnost: novi zakonski propisi u Republici Srbiji*. Beograd: Poslovni Biro.

Nikolić, Milojko, i Sinkovski, Stevan. (2013). *Korporativna bezbednost: Osnove zaštite biznisa i preduzetništva*. Beograd: Banjac grafika.

Ninković, Vladimir M. (2021). Critical Infrastructure Resilience-National Approaches in the United States of America, the United Kingdom and Australia. *Зборник радова Правног факултета у Новом Саду* 4/2021, стр. 1205-1225.

Noll, A. Michael. (2015). *Memories: A Personal History of Bell Telephone Laboratories*. Michigan: Michigan State University, Quello Center.

Nossal, Kim Richard. (2001). Global governance and national interests: regulating transnational security corporations in the post-cold war era. *Melbourne Journal of International Law* 2 (2), pp. 459-476.

O'Brien, A. Kevin. (2009). „What should and what should not be regulated?". In: S. Chesterman and C. Lehnardt (Eds.). *From Mercenaries to Market: The Rise and Regulation of Private Military Companies* (pp. 29–48). Oxford: Oxford University Press.

Ocqueteau, Frédéric. (2011). Heads of corporate security in the era of global security. *Champ pénal/Penal field* 8.

Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности. (2019). *Сл. гласник РС,* бр. 45/2019-65, 112/2020.

Одлука о објектима од посебног значаја за одбрану. (2008). *Сл. гласник РС*, бр. 112/2008.

Одлука о одређивању производа и услуга од посебног интереса за одбрану земље. (1994). *Сл. лист СРЈ,* бр. 43/94, 28/96.

Одлука о одређивању производа и услуга од посебног интереса за одбрану земље. (2006). *Сл. лист СЦГ,* бр. 13/06.

Одлука о одређивању производа и услуга од посебног значаја за одбрану Републике Србије. (2008). *Сл. гласник РС,* бр. 58/2008, 26/2019.

Одлука о одређивању субјеката од посебног значаја за заштиту и спасавање у Републици Србији. (2019). *Сл. гласник РС*, бр. 69/2019.

Одлука о одређивању великих техничких система од интереса за одбрану земље. (1994). *Сл. лист СРЈ,* бр. 54/94, 58/94, 65/94, 10/97.

Одлука о одређивању великих техничких система од значаја за одбрану. (2014). *Сл. гласник РС*, бр. 41/2014, 35/2015, 86/2016, 53/2017, 26/2019, 94/2019, 67/2021, 62/2022.

Одлука о одређивању великих техничких система од значаја за одбрану. (2009). *Сл. гласник РС, бр.* 15/09, 54/10, 4/11, 58/11.

Одлука о одређивању војних и других објеката и рејона који су забрањени за осматрање снимање и приступ и о мерама за њихову заштиту. (1996). *Сл. гласник РС*, бр. СРЈ 11/1996, 42/2005.

Одлука о утврђивању Стандардних уговорних клаузула. (2020). *Сл. гласник РС*, бр. 5/2020.

OECD. (2011). *OECD Guidelines for Multinational Enterprises*. OECD Publishing.

OECD. (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*. Paris: OECD Publishing. Доступно на: https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

OECD. (2018a). *Assessing Global Progress in the Governance of Critical Risks*. Paris: OECD Publishing. Доступно на: https://www.oecd-ilibrary.org/governance/assessing-global-progress-in-the-governance-of-critical-risks_9789264309272-en.

OECD. (2018b). *Assessing the Real Cost of Disasters: The Need for Better Evidence*. Paris: OECD Publishing. Доступно на: https://www.oecd-ilibrary.org/governance/assessing-the-real-cost-of-disasters_9789264298798-en.

OECD. (2019). *Good Governance for Critical Infrastructure Resilience.* Paris: OECD Publishing. Доступно на: https://www.oecd-ilibrary.org/sites/76326acb-en/index.html?itemId=/content/component/76326acb-en.

Office Of Homeland Security. (2002). *National Strategy for Homeland Security*.

Organisation for Economic Co-operation and Development. (2015). Recommendation of the Council on Principles of Corporate Governance, OECD/LEGAL/0413. OECD.

Ortmeier, P. J. (1999). *Public safety and private security administration*. Woburn, MA: Butterworth-Heinemann.

Ostojić, Momir. (2008). „Naučni problem teorijske definicije bezbednosti kao osnove za definisanje privatne bezbednosti". U: *Privatna bezbednost: stanje i perspektive: zbornik radova: prvi međunarodni skup* (str. 181-201). Novi Sad: Fakultet za pravne i poslovne studije.

Ouyang, Min. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability engineering and System safety* 121, pp. 43-60.

Oxford Learner's Dictionary. (2010). *Oxford Advanced Learner's Dictionary*. Oxford: Oxford University Press.

Pal, Indrajit, Kumar, Anil, and Mukhopadhyay, Anirban. (2023). Risks to coastal critical infrastructure from climate change. *Annual Review of Environment and Resources* 48, pp. 681-712.

Papadakis, S. Ioannis, and Ziemba, T. William. (2001). „Derivative Effects of the 1999 Earthquake in Taiwan to U.S. Personal Computer Manufacturers". In: Kleindorfer, P.R. and M.R. Sertel, (Eds.). *Mitigation and Financing of Seismic Risks: Turkish and International Perspectives* (pp 261–276). NATO Science Series, vol 3. Dordrecht: Springer.

Parsons, Taltok. (2009). *Društveni sistem i drugi ogledi*. Novi Sad: Izdavačka knjižarnica Zorana Stojanovića.

Pavić, Milica, i Jokanović, Igor. (2021). Zakonodavstvo o kritičnoj infrastrukturi u Republici Srbiji, regionu i Evropskoj uniji. *Zbornik radova Građevinskog fakulteta* 37 (39), str. 17-28.

Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M. (2006). *Critical infrastructure interdependency modeling: a survey of US and international research*. Idaho: Idaho National Laboratory.

Pejanović, Ljubo, Stojanović, Stevan, and Komarčević, Miodrag. (2018). „Corporate and system coordinated integration of security services of state and private sector". In: D. Čaleta (Ed.). *Contemporary concept of corporate security* (pp. 237-254). Belgrade: Beopress.

Pendić, Zoran R., Pendić, Rajko Z., Jakovljević, Bojana B., Vujotić, Ljiljana. B. and Gajić, Lazar T. (2019). Where is the place of corporate security/safety in the organizational structure of an organization: An approach. *Tehnika* 74 (5), pp. 741-750.

Pescaroli, Gianluca, and Alexander, David. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards 82*, pp. 175-192.

Pesch-Cronin, A. Kelley, and Marion, E. Nancy. (2017). *Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective*. Boca Raton: Taylor and Francis Group.

Petersen, L. Karen. (2013). The Corporate Security Professional: A Hybrid Agent Between Corporate and National Security. *Security Journal,* 26 (3), pp. 222-235.

Petersen, L. Karen. (2014). The Politics of Corporate Security and the Translation of National Security. In: K. Walby and R. K. Lippert (Eds.). *Corporate Security in the 21st Century* (pp. 216-235). Hampshire: Palgrave Macmillan.

Petit, F., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., Fisher, R. E., Haffenden, R. A., Huttenga, A. A., Klett, M. S., Phillips, J. A., Thomas, M., Veselka, S. N., Wallace, K. E., Whitfield, R. G., and Peerenboom, J. P. (2013). *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience* (No. ANL/DIS-13-01). Argonne: Argonne National Lab (ANL).

Petit, F., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Haffenden, R. A., Klett, M. S., M. S., Phillips, J. A., Veselka, S. N., Wallace, K. E., Whitfield, R. G., and Peerenboom, J. P. (2013). *Protective Measures Index and Vulnerability Index: Indicators Of Critical Infrastructure Protection and Vulnerability* (No. ANL/DIS-13/04). Argonne: Argonne National Lab (ANL).

Petrakos, Nikolaos, and Kotzanikolaou, Panayiotis. (2019). Methodologies and Strategies for Critical Infrastructure Protection. In: D. Gritzalis, M. Theocharidou, and G. Stergiopoulos (Eds.). *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications* (pp. 17-33). Cham: Springer.

Petticrew, Mark and Roberts, Helen. (2006). *Systematic Reviews in the Social Sciences: A Practical Guide*. Malden, MA: Blackwell Publishing.

Polinpapilinho, F. Katina, and Hester, P. Thomas. (2012). Systemic determination of infrastructure criticality. *International Journal of Critical Infrastructures* 9 (3), pp. 211-225.

Поточар, Стане (1974). Концепција општенародне одбране – резултати и задаци. *Војно дело* 2, стр. 5-26.

Почуч, Владимир (Ур.). (2023). *Бела књига одбране Републике Србије*. Београд: Војна штампарија.

Powell, John. (2002). Bringing terrorism into the strategic debate: an expanded characterisation of strategic threats to firms. *Security Journal* 5 (3), pp. 26-35.

Правилник о ближем начину, трошковима и критеријумима за процену радне способности и могућности запослења или одржања запослења особа са инвалидитетом. (2010). *Сл. гласник РС*, бр. 36/2010, 97/2013.

Правилник о ближим условима, критеријумима и стандардима за спровођење мера и активности професионалне рехабилитације. (2009). *Сл. гласник РС*, бр. 112/2009.

Правилник о евиденцијама које воде правна лица и предузетници. (2016). *Сл. гласник РС*, бр. 3/2016.

Правилник о изради и спровођењу плана управљања ризицима од повреде принципа родне равноправности. (2022). *Сл. гласник РС*, бр. 67/2022.

Правилник о Листи опасних материја и њиховим количинама и критеријумима за одређивање врсте документа које израђује оператер севесо постројења, односно комплекса. (2010). *Сл. гласник РС*, бр. 41/2010, 51/2015, 50/2018.

Правилник о методологији за израду националног и локалног регистра извора загађивања, као и методологији за врсте, начине и рокове прикупљања података. (2010). *Сл. гласник РС*, бр. 91/2010, 10/2013, 98/2016, 72/2023.

Правилник о начину израде и садржају Плана заштите од пожара аутономне покрајине, јединице локалне самоуправе и субјеката разврстаних у прву и другу категорију. (2010). *Сл. гласник РС*, бр. 73/2010.

Правилник о начину израде и садржају Плана заштите од удеса. (2019). *Сл. гласник РС*, бр. 41/2019.

Правилник о начину праћења извршавања обавезе запошљавања особа са инвалидитетом и начину доказивања извршења те обавезе. (2016). *Сл. гласник РС*, бр. 101/2016.

Правилник о начину унутрашњег узбуњивања, начину одређивања овлашћеног лица код послодавца, као и другим питањима од значаја за унутрашње узбуњивање код послодавца који има више од десет запослених. (2018). *Сл. гласник РС*, бр. 49/2015, 44/2018.

Правилник о начину вођења Регистра привредних друштава и правних лица која рукују опасним супстанцама. (2019). *Сл. гласник РС,* бр. 34/2019.

Правилник о облику и садржају знака забране пушења и знака да је пушење дозвољено у одређеном простору, начину истицања тих знакова, обрасцу извештаја о повреди забране пушења, врсти потребних доказа о пушењу и начину на који се они прикупљају и на који се утврђује присуство дуванског дима у простору у коме је пушење забрањено, као и о обрасцу за наплату новчане казне на лицу места. (2010). *Сл. гласник РС*, бр. 73/2010, 89/2017.

Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности. (2019). *Сл. гласник РС*, бр. 40/2019.

Правилник о организовању заштите од пожара према категорији угрожености од пожара. (2021). *Сл. гласник РС*, бр. 6/2021.

Правилник о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја. (2020). *Сл. гласник РС*, бр. 9/2020.

Правилник о поступку издавања, изгледу и садржини образаца и исправа о оружју предвиђених Законом о оружју и муницији. (2016). *Сл. гласник РС*, бр. 16/2016.

Правилник о правилима понашања послодаваца и запослених у вези са превенцијом и заштитом од злостављања на раду. (2010). *Сл. гласник РС*, бр. 62/2010.

Правилник о просторно-техничким условима за безбедно смештање и чување оружја и муниције. (2016). *Сл. гласник РС*, бр. 9/2016, 106/2016, 50/2018.

Правилник о садржају и начину достављања Плана мера за отклањање или ублажавање неравномерне заступљености полова и годишњег извештаја о његовом спровођењу. (2010). *Сл. гласник РС*, бр. 89/2010.

Правилник о садржини обавештења о новом севесо постројењу односно комплексу, постојећем севесо постројењу, односно комплексу и о трајном престанку рада севесо постројења, односно комплекса. (2010). *Сл. гласник РС*, бр. 41/2010.

Правилник о садржини политике превенције удеса и садржини и методологији израде Извештаја о безбедности и Плана заштите од удеса. (2020). *Сл. гласник РС*, бр. 41/2010.

Правилник о садржини, начину успостављања и одржавања регистра ризика од катастрофа. (2019). *Сл. гласник РС*, бр. 78/2019.

Правилник о вођењу евиденције и извештавању о остваривању родне равноправности. (2022). *Сл. гласник РС*, бр. 67/2022.

Правилник о врсти и количини опасних супстанци на основу којих се сачињава План заштите од удеса. (2019). *Сл. гласник РС*, бр. 34/2019.

Привредна комора Србије. (2024, септембар 18). *Чадеж и Дачић: Држава и привреда сигурне и стабилне уз сарадњу приватног и јавног сектора безбедности*. Доступно на: https://pks.rs/vesti/cadez-i-dacic-drzava-i-privreda-sigurne-i-stabilne-uz-saradnju-privatnog-i-javnog-sektora-bezbednosti-10451.

Prieto, Robert. (2003). Business Community Views. *Technology in Society* 25 (4), pp. 517-522.

Prior, Tim. (2014). *Measuring Critical Infrastructure Resilience: Possible Indicators, Risk and Resilience Report 9*. Zürich: Center for Security Studies, ETH.

Pursiainen, Christer. (2009). The Challenges for European Critical Infrastructure Protection. *Journal of European Integration* 31 (6), pp. 721-739.

Радивојевић, Ненад. (2019). *Јавно-приватно партнерство у области јавне безбедности у развијеним земљама са посебним освртом на Републику Србију* (Докторска дисертација). Нови Сад: Универзитет у Новом Саду, Правни факултет у Новом Саду.

Radvanovsky, S. Robert, and McDougall, Allan. (2024). *Critical infrastructure: Homeland security and emergency preparedness*. Boca Raton: CRC press.

Rahman, Shafiqur. (2011). Evaluation of Definitions: Ten Dimensions of Corporate Social Responsibility. *World Review of Business Research,* 1 (1), pp. 166-176.

Rajnović, Ljiljana. (2016). Društveno odgovorno poslovanje u funkciji poboljšanja privrednog ambijenta u Republici Srbiji. *Ekonomski vidici* 21 (1), str. 1-13.

Ракић, М. Марко. (2015). *Кризни менаџмент у функцији заштите критичних инфраструктура у земљама у транзицији* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

Rakić, Mile. (2008). „Značaj privatne bezbednosti u sistemu bezbednosti ". U: *Privatna bezbednost: stanje i perspektive: zbornik radova: prvi međunarodni skup* (str. 157-167). Novi Sad: Fakultet za pravne i poslovne studije.

Rakić, Mile. (2008). Politika i ustav kao pretpostavka izgradnje savremenog sistema bezbednosti višeetničkih država. *Kriminalističke teme* 1-2, str. 247-255.

Ratner, R. Steven. (2001). Corporations and Human Rights: A Theory of Legal Responsibility. *The Yale Law Journal* 111 (3), pp. 443-545.

Rawlings, Philip. (2012). „Policing before the police". In: T. Newman (Ed.). *Handbook of policing* (pp. 75-99). Routledge.

RECIPE. (2015). *Resilience of Critical Infrastructure Protection – Guidelines*. European Commission – DG ECHO.

Reich, Leonard S. (1980). Industrial Research and the Pursuit of Corporate Security: The Early Years of Bell Labs. *The Business History Review* 54 (4), pp. 504–529.

Рељановић, Марио. (2020). „Заштита података о личности у радном односу". У: С. Андоновић, Д. Прља и А. Дилигенски (Ур.). Заштита података о личности у Србији (стр. 61-92). Београд: Институт за упоредно право.

Ridley, Gail. (2011). National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience. *Journal of Business Ethics* 103 (1), pp. 111-125.

Rinaldi, M. Steven, Peerenboom, P. James, and Kelly, K. Terrence. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21 (6), pp. 11-25.

Rinaldi, M. Steven. (2004). „Modeling and simulating critical infrastructures and their interdependencies". In: *Proceedings of the 37th Annual Hawaii International Conference on System Sciences* (pp. 20054a). California: IEEE.

Ruso, Žan Žak. (1993). *Društveni ugovor*, preveli Tihomir Marković, Radmila Stojanović i Mira Vuković. Beograd: Filip Višnjić.

Rosenthal, Uriel, Charles, T. Michael, and 't Hart. Paul. (1989). *Coping with Crises: The Management of Disasters, Riots and Terrorism*. C.C. Thomas.

Rothschild, Emma. (1995). What Is Security? *Daedalus* 124 (3), pp. 53-98.

Reuters. (2019, June 24). *Netherlands emergency services hit by major telecoms outage*. Euronews. Доступно на: https://www.euronews.com/2019/06/24/dutch-emergency-services-hit-by-major-telecoms-outage.

Ribeiro, Anna. (2023, July 25). *Data breach costs for critical infrastructure sector exceed $5 million, as time 'new currency' in cybersecurity*. Industrial Cyber. Доступно на: https://industrialcyber.co/reports/data-breach-costs-for-critical-infrastructure-sector-exceed-5-million-as-time-new-currency-in-cybersecuritydata-breach-costs-for-critical-infrastructure-sector-exceed-5-million-as-time-new/.

Saha, Sudip. (n.d.). *Private Security Market Outlook (2024 to 2034)*. Future Market Insights. Доступно на: https://www.futuremarketinsights.com/reports/private-security-market.

Salehyan, Idean. (2010). The delegation of war to rebel organizations. *Journal of Conflict Resolution* 54 (3), pp. 493-515.

Sarre, Rick and Prenzler, Timothy. (2009). *The Law of Private Security in Australia* (2nd ed.). Pyrmont: Thomson Lawbook.

Савић, Андреја. (2007). *Национална безбедност*. Београд: Криминалистичко-полицијска академија.

Савић, Андреја. (2006). *Обавештајне службе и национална безбедност*. Крагујевац: Правни факултет.

Savić, Andreja. (2008). „Privatna bezbednost u sistemu nacionalne bezbednosti“. U: *Privatna bezbednost: stanje i perspektive: zbornik radova: prvi međunarodni skup* (str. 15-23). Novi Sad: Fakultet za pravne i poslovne studije.

Савић, Сузана, Станковић, Миомир, и Јанаћковић, Горан. (2021). *Теорија система и ризика: системност у контексту менаџмента ризиком*. Београд: Академска мисао; Факултет заштите на раду у Нишу.

Scheimer, Michael. (2009). Separating Private Military Companies From Illegal Mercenaries in International Law: Proposing an International Convention for Legitimate Military and Security Support that Reflects Customary International Law. *American University International Law Review* 24 (3), pp. 609-646.

Schot, Jochan. (2003). *Transnational Infrastructures and the Rise of Contemporary Europe, Working Doc No. 1.*

Schreier, Fred and Caparini, Marina. (2005). *Privatising security: Law, practice and governance of private military and security companies* (Vol. 6). Geneva: DCAF.

Schultze, L. Charles. (1973). The economic content of national security policy. *Foreign Affairs* 51(3), pp. 529-535.

Schweikert, Amy, Nield, Lindsey, Otto, Erica, and Deinert, Mark. (2019). *Resilience and critical power system infrastructure: Lessons learned from natural disasters and future research needs*, Policy Research Working Paper 8900. World Bank.

Security Committee. (2017). *The Security Strategy for Society. Government Resolution*. Helsinki: Security Committee.

Sellevåg, R. Stig. (2022). *Modelling Total Defence Systems to Inform National Resilience Objectives – A Norwegian Case Study*. NATO Science and Technology Organization.

Setola, Roberto, Luiijf, Eric, and Theocharidou, Marianthi. (2016). „Critical infrastructures, protection and resilience“. In: R. Setola, V. Rosato, E. Kyriakides, E. Rome (Eds.). *Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach* (pp. 1-18). Springer International Publishing.

Shearing, Clifford. (2005). Nodal security. *Police Quarterly* 8 (1), pp. 57-63.

Shearing, D. Clifford, and Stenning, C. Philip. (1981). Modern private security: its growth and implications. *Crime and justice* 3, pp. 193-245.

Shearing, D. Clifford, and Stenning, C. Philip. (1983). Private security: Implications for social control. *Social Problems* 30, pp. 493-506.

Shearing, D. Clifford. (1992). The Relation between Public and Private Policing. *Crime and Justice* 15, pp. 399-434.

Shyra, Taras, Salyga, Kostiantyn, Derii, Vasyl, Prykhodko, Igor, and Shymkiv, Svitlana. (2021). The development of corporate security in the context of countering threats to doing business. *Business: Theory and Practice* 22 (1), pp. 211-221.

Šijan, Aleksandar, Karabašević, Darjan, i Rajčević, Dušan. (2019). Značaj opšte teorije sistema za savremeni svet. *Trendovi u poslovanju* 2 (14), str. 87-94.

Simić, Đorđe, i Arnautović, Omer. (1987). *Priručnik: fizičko-tehničko obezbeđenje i protivpožarna i civilna zaštita*. Beograd: Poslovna politika.

Simić, Slobodan. (2022). „Kompleksnost sistema zaštite kritične infrastrukture“. U: L. Gostimirović i G. Maksimović (Ur.). *Diskurs o kritičnoj infrastrukturi* (str. 1-9). Doboj: Visoka poslovno tehnička škola; Banja Luka: Bezbjednosni istraživački centar.

Симовић, Слободан, и Манић, Михајло. (2019). „Послови у надлежности функције корпоративне безбедности". У: С. Душанић (Ур.). *Зборник Међународна научна конференција Медији и економија* (стр. 205-230). Бања Лука: Бесједа.

Синдикат полиције Слога. (2021, Септембар 9). *Систематизација у МУП недоступна иако је информација од јавног значаја*. Доступно на: https://sindikatpolicije.org.rs/?p=4740#more-4740.

Singer, W. Peter. (2008). *Corporate Warriors: The Rise of the Privatized Military Industry.* Ithaca, NY: Cornell University Press.

Singh, Anne-Marie, and Light, Matthew. (2019). Constraints on the growth of private policing: A comparative international analysis. *Theoretical Criminology* 23, pp. 295-314.

Škero, Mirko i Ateljević, Vladimir. (2015). Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope 2008/114/ES. *Vojno delo* 3, str. 192-207.

Smith, Clifton, and Brooks, David J. (2012). *Security science: The theory and practice of security*. Butterworth-Heinemann.

Smith, N. Craig. (2003). Corporate social responsibility: whether or how?. *California management review* 45 (4), pp. 52-76.

Social Accountability International. (2014). *Social Accountability* (SAI Standard No. 8000:2014).

Sorensen, C. Theodore. (1990). Rethinking National Security. *Foreign Affairs* 69 (3), pp. 1-18.

South, Nigel. (1987). „Law, profit, and private persons: private and public policing in English history". In: Clifford D. Shearing and Philip C. Stenning (Eds.). *Private Policing* (pp. 73-109). California: Sage.

South, Nigel. (1994). Privatizing Policing in the European Marker: Some Issues for Theory, Policy, and Research. *European sociological review* 10 (3), pp. 219-233.

Sparrow, K. Malcolm. (2014). *Managing the boundary between public and private policing*. New Perspectives in Policing Bulletin. Washington, DC: U.S. Department of Justice, National Institute of Justice.

Spitzer, Stephen, and Scull, T. Andrew. (1977). Privatization and capitalist development: The case of the private police. *Social Problems* 25 (1), pp. 18-29.

Стајић, Љубомир, и Гаћиновић, Радослав. (2007). *Увод у студије безбедности*. Београд: Драслар партнер.

Стајић, Љубомир, и Лукић, Татјана. (2011). *Право приватне безбедности*. Нови Сад: Правни факултет, Центар за издавачку делатност.

Стајић, Љубомир, и Мандић, Ј. Горан. (2014). Неке контроверзе Закона о приватном обезбеђењу. *Зборник радова Правног факултета* 48 (2), стр. 131-150.

Стајић, Љубомир, и Радивојевић, Ненад. (2015). Закон о приватном обезбеђењу – стање и последице. У Р. Кеча (Ур.). *Хармонизација српског и мађарског права са правом Европске уније: тематски зборник. Књ. 3* (стр. 171-188). Нови Сад: Правни факултет.

Стајић, Љубомир, и Радивојевић, Ненад. (2016). Неки проблеми имплементације Закона о приватном обезбеђењу. У Љ. Стајић (Ур.). *Хармонизација српског и мађарског права са правом Европске уније: тематски зборник. Књ. 4* (стр. 153-169). Нови Сад: Правни факултет, Центар за издавачку делатност.

Стајић, Љубомир, и Радивојевић, Ненад. (2017). Полиција, комунална полиција и приватно обезбеђење – дивергентни или конвергентни субјекти јавне безбедности. У Љ. Стајић (Ур.). *Хармонизација српског и мађарског права са правом Европске уније:*

тематски зборник. Књ. 5 (стр. 151-173). Нови Сад: Правни факултет, Центар за издавачку делатност.

Стајић, Љубомир, Мијалковић, Саша, и Станаревић, Светлана. (2004). *Безбедносна култура*. Београд: Драганић.

Стајић, Љубомир, Мирковић, Владан, и Радивојевић, Ненад. (2020). Безбедносни менаџмент у области заштите критичне инфраструктуре у Републици Србији – стање и перспективе. *Зборник радова Правног факултета у Новом Саду* 54 (3), стр. 953-970.

Стајић, Љубомир, Мирковић, Владан, и Радивојевић, Ненад. (2021). Управљање системом заштите критичне инфраструктуре у Републици Србији. У *Правна традиција и нови правни изазови* (стр. 13-14). Нови Сад: Правни факултет у Новом Саду.

Стајић, Љубомир, Радивојевић, Ненад, и Мирковић, Владан. (2017). Неки аспекти политике унутрашње безбедности као елемента Стратегије националне безбедности Републике Србије. *Зборник радова Правног факултета у Новом Саду* 51 (4), стр. 1325-1342.

Стајић, Љубомир. (2003). *Основи безбедности*. Београд: Полицијска академија.

Стајић, Љубомир. (2008). *Основи система безбедности – са основама истраживања безбедносних појава.* Нови Сад: Правни факултет у Новом Саду.

Стајић, Љубомир. (2008). Правни оквир приватне безбедности у светлу савременог схватања појма безбедности. *Зборник радова Правног факултета у Новом Саду* 42 (1–2), стр. 373-390.

Стајић, Љубомир. (2013). Контрола приватног сектора безбедности у Републици Србији. У Р. Кеча (Ур.). *Хармонизација српског и мађарског права са правом Европске уније: тематски зборник* (стр. 194-195). Нови Сад: Правни факултет у Новом Саду.

Стајић, Љубомир. (2015). *Основи система безбедности – са основама истраживања безбедносних појава.* Нови Сад: Правни факултет у Новом Саду.

Стајић, Љубомир. (2018). Заштита критичне инфраструктуре и приватно обезбеђење. У Љ. Стајић (Ур.). *Хармонизација српског и мађарског права са правом Европске уније: тематски зборник. Књ. 6* (стр. 119–135). Нови Сад: Правни факултет у Новом Саду.

Станаревић, Светлана. (2012). *Концепт безбедносне културе и претпоставке његовог развоја* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

Станаревић, Светлана. (2018). *Основи безбедности*. Београд: Универзитет у Београду, Факултет безбедности.

Statista Research Department. (2023, April 13). *Size of the security services market worldwide from 2011 to 2020, by region*. Statista. Доступно на: https://www.statista.com/statistics/323113/distribution-of-the-security-services-market-worldwide/.

Stein, J. George. (1990). Total defense: A Comparative Overview of the Security. Policies of Switzerland and Austria. *Defense Analysis* 6 (1), pp. 17-33.

Stenning, Philip. (2000). Powers and Accountability of Private Police. *European Journal on Criminal Policy and Research* 8 (3), pp. 325-352.

Stenning, Philip. (2009). Governance and accountability in a plural policing environment—The story so far. *Policing: A Journal of Policy and Practice* 3 (1), pp. 22-33.

Стевановић, Обрад, и Субошић, Дане. (2007). „Организациони системи с посебним освртом на системе безбедности“. У: З. Кековић (прир.). *Системи безбедности – хрестоматија* (стр. 13-28). Београд: Универзитет у Београду, Факултет безбедности.

Стојановић, Милан, и Павловић, Дејан. (2014). *Економска безбедност пословања*. београд: „Школа плус“ и Српска асоцијација менаџера корпоративне безбедности.

Стратегија националне безбедности Републике Србије. (2009). *Службени гласник РС*, бр. 88/2009.

Стратегија националне безбедности Републике Србије. (2019). *Службени гласник РС*, бр. 94/2019.

Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године. (2021). *Сл. гласник РС*, бр. 86/2021.

Стратегија развоја Министарства унутрашњих послова за период од 2018-2023. године. (2018). *Службени гласник РС*, бр. 78/2018.

Strom, Kevin, Berzofsky, Marcus, Shook-Sa, Bonnie, Barrick, Kelle, Daye, Cristal, Horstmann, Nicole, and Kinsey, Susan. (2010). *The private security industry: A review of the definitions, available data sources, and paths moving forward*. US Department of Justice and National Criminal Justice Reference Service, Final Report.

Swiss Re. (2016, Jul 25). *Analysis of Tianjin Port Explosion*. Swiss Re. Доступно на: https://www.swissre.com/en/china/news-insights/articles/analysis-of-tianjin-port-explosion-china.html.

Tagarev, D. Todor, and Pavlov, Nikolay. (2007). Planning Measures and Capabilities for Protection of Critical Infrastructures. *Information and Security: An International Journal* 22, pp. 38-48.

Талијан, Мирослав. (2016). Савремени тероризам и облици испољавања савременог урбаног тероризма. *Политика националне безбедности* VII (1), стр. 185-213.

Талијан, Момчило, и Талијан, Мирослав. (2010). „Основе за иновирање корпоративне безбедности“. У: *Дани безбједности на тему „Корпоративна безбједност - ризици, пријетње и мјере заштите* (стр. 11-34). Бања Лука.

Talijan, Momčilo, i Ristović, Slavica. (2012). Neka shvatanja menadžmenta od značaja za inoviranje korporativne bezbednosti. *Revija za bezbednost* (6), str. 62-74.

Talijan, Momčilo. (2008). „Prve ustanove privatne bezbednosti (policije) u Srbiji“. U: *Privatna bezbednost: stanje i perspektive: zbornik radova: prvi međunarodni skup* (str. 40-62). Novi Sad: Fakultet za pravne i poslovne studije.

Taylor, Brendan. (2012). *The Evolution of National Security Studies*. National Security College occasional paper: 3. Acton: National Security College, Australian National University.

Technavio. (2024). *Private Security Services Market Analysis APAC, North America, Europe, South America, Middle East and Africa - US, China, India, Germany, UK - Size and Forecast 2024-2028*. Technavio. Доступно на: https://www.technavio.com/report/private-security-services-market-size-industry-analysis.

The Economist. (2024, March 24). *The impact of the Baltimore bridge disaster*. The Economist. Доступно на: https://www.economist.com/united-states/2024/03/26/the-impact-of-the-baltimore-bridge-disaster.

Thornton, H. Patricia, Ocasio, William, and Lounsbury, Michael. (2012). *The institutional logics perspective: A new approach to culture, structure and process*. OUP Oxford.

Timmerman, Peter. (1981). *Vulnerability, Resilience and the Collapse of Society: A Review of Models and Possible Climatic Applications*. Toronto: University of Toronto, Institute for Environmental Studies.

Tomić, Duško, i Milićević, Marlema. (2016). „Društveni značaj korporativne bezbednosti". U: *Zbornik Međunarodna naučna konferencija Mediji i ekonomija* (str. 187-200). Banja Luka.

Transparentnost Srbija i Centar za primenjene evropske studije. (2022). *GLAVNI PROBLEMI JAVNIH NABAVKI U SRBIJI: U kontekstu novih zakonskih rešenja i evropskih integracija*. Beograd: Transparentnost Srbija i Centar za primenjene evropske studije.

Трбојевић, Милован. (2018). Заштита критичних инфраструктура-искуства транзиционих земаља. *Политичка ревија* 56 (2), стр. 99-118.

Trifunović, Darko. (2019). National and International Security and corporate Governance. *Teme – Časopis za Društvene Nauke* 43 (4), str. 1233-1244.

Trivan, Dragan. (2012). *Korporativna bezbednost*. Beograd: Dosije studio.

Trivan, Dragan. (2013). Vpliv korporativne varnosti na nacionalno varnost. *Sodobni vojaški izzivi* 15 (3), pp. 69-98.

Ђурчић, Милица. (2023). *Национални интерес као аналитички оквир за истраживање политике националне безбедности Републике Србије* (Докторска дисертација). Београд: Универзитет у Београду, Факултет безбедности.

Unijat, Jelena, Petrović, Predrag, Milošević, Marko, i Stojanović, Sonja. (2008). U: *Privatne bezbednosne kompanije u Srbiji – prijatelj ili pretnja?* (str. 26-37). Beograd: Centar za civilno-vojne odnose.

United Nations Office for Disaster Risk Reduction. (2008). *UNISDR Terminology on Disaster Risk Reduction*. United Nations

United Nations Office on Drugs and Crime. (2014). *State Regulation concerning Civilian Private Security Services and their Contribution to Crime Prevention and Community Safety*. New York: United Nations.

United States Department of Homeland Security. (2003). *Homeland Security Presidential Directive 7 - HSPD-7*.

United States. President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection.* Commission.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).

Упутство о Методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања. (2019). *Сл. гласник РС*, бр. 80/2019.

Упутство за израду и објављивање информатора о раду органа јавне власти. (2022). *Сл. гласник РС*, бр. 10/2022.

Упутство за израду и усвајање пројеката информационих система органа управе. (1989). *Сл. гласник РС*, бр. 49/1989.

Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја. (2016). *Сл. гласник РС*, бр. 94/2016.

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја. (2016). *Сл. гласник РС*, бр. 94/2016.

Уредба о ближим критеријумима за одређивање обавезно обезбеђених објеката и начину вршења послова њихове заштите. (2016). *Сл. гласник РС*, бр. 98/2016.

Уредба о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА" и „СТРОГО ПОВЕРЉИВО". (2013). *Сл. гласник РС*, бр. 46/2013.

Уредба о криптобезбедности и заштити од компромитујућег електромагнетног зрачења. (2019). *Сл. гласник РС*, бр. 57/2019.

Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије. (2022). *Сл. гласник РС*, бр. 69/2022.

Уредба о критеријумима за утврђивање података значајних за одбрану земље који се морају чувати као државна или службена тајна и о утврђивању задатака и послова од посебног значаја за одбрану земље које треба штитити применом посебних мера безбедности. (1994). *Сл. лист СРЈ*, бр. 54/94.

Уредба о начину и поступку означавања тајности података, односно докумената. (2011). *Сл. гласник РС*, бр. 8/2011.

Уредба о обавезама субјеката система смањења ризика од катастрофа и управљања ванредним ситуацијама у поступку израде Регистра ризика од катастрофа, начину израде Регистра ризика од катастрофа и уносу података. (2020). *Сл. гласник РС*, бр. 122/2020.

Уредба о обавезним средствима и опреми за личну, узајамну и колективну заштиту од елементарних непогода и других несрећа. (2011). *Сл. гласник РС*, бр. 3/2011, 37/2015.

Уредба о обезбеђивању и заштити информационих система државних органа. (1990). *Сл. гласник РС*, бр. 41/1990.

Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије. (1992). *Сл. гласник РС*, бр. 18/1992.

Уредба о обрасцима безбедносних упитника. (2010). *Сл. гласник РС*, бр. 30/2010.

Уредба о одређивању послова безбедносне заштите одређених лица и објеката. (2010). *Сл. гласник РС,* бр. 72/2010, 64/2013.

Уредба о подацима и пословима значајним за систем одбране који се морају чувати и штитити у складу са законом којим се уређује заштита тајности података и о критеријумима за попуну радних места на којима се ти задаци и послови обављају. (2020). *Сл. гласник РС,* бр. 8/2020.

Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа. (2013). *Сл. гласник РС*, бр. 63/2013.

Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима. (2011). *Сл. гласник РС*, бр. 53/2011.

Уредба о посебним мерама надзора над поступањем са тајним подацима. (2011). *Сл. гласник РС*, бр. 90/2011.

Уредба о посебним мерама физичко-техничке заштите тајних података. (2011). *Сл. гласник РС*, бр. 97/2011.

Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја. (2020). *Сл. гласник РС*, бр. 11/2020.

Уредба о разврставању објекта, делатности и земљишта у категорије угрожености од пожара. (2010). *Сл. гласник РС*, бр. 76/2010.

Уредба о садржају и начину израде плана смањења ризика од катастрофа. (2020). *Сл. гласник РС*, бр. 21/2020.

Уредба о садржају, начину израде и обавезама субјеката у вези са израдом процене ризика од катастрофа и планова заштите и спасавања. (2020). *Сл. гласник РС*, бр. 102/2020.

Уредба о садржини и начину вођења информационог система заштите животне средине, методологији, структури, заједничким основама, категоријама и нивоима сакупљања података, као и о садржини информација о којима се редовно и обавезно обавештава јавност. (2009). *Сл. гласник РС*, бр. 112/2009.

Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима. (2010). *Сл. гласник РС*, бр. 89/2010.

Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима. (2010). *Сл. гласник РС*, бр. 54/2010.

Уредба о условима испоруке и снабдевања електричном енергијом. (2023). *Сл. гласник РС,* бр. 84/2023.

Уредба о условима испоруке и снабдевања природним гасом. (2023). *Сл. гласник РС,* бр. 49/2022, 32/2023, 97/2023.

Уредба о утврђивању Листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја. (2019). *Сл. гласник РС*, бр. 94/2019.

Устав СФРЈ. (1974). *Сл. лист СФРЈ*, бр. 9/XXX.

van Bergen Thirion, C. J. (1998). *The Privatization of Security: A Blessing or a Menace?*. Pretoria: South African Defence College.

van Kreveld, Martin. (2012). *Uspon i propadanje države*. Beograd: Albatros plus; Fakultet bezbednosti.

van Steden, Ronald, and Sarre, Rick. (2007). The growth of private security: Trends in the European Union. *Security journal* 20, pp. 222-235.

van Steden, Ronald. (2007). *Privatizing policing: Describing and explaining the growth of private security* (PhD-Thesis). Amsterdam: Vrije Universiteit.

Vejnović, Duško, Trivunović, Janko, Matijević, Mile, Đokić, Petar, Vrtovec, Zmago, Lalić, Velibor, Šikman, Mile, Perko, Jože, i Đukić, Siniša. (2008). D*etektivska djelatnost: teorijski i praktični aspekti po standardima Evropske Unije*. Banja Luka: Defendologija centar za bezbjedonosna sociološka i kriminološka istraživanja; Ljubljana: Detektivska zbornica Republike Slovenije.

Veldman, Jeroen, and Willmott, Hugh. (2013). What is the corporation and why does it matter?. M@ n@ gement 5, pp. 605-620.

Venkatachary, Sampath Kumar, Prasad, Jagdish, and Samikannu, Ravi. (2017). Economic Impacts of Cyber Security in Energy Sector: A Review. *International Journal of Energy Economics and Policy* 7 (5), pp. 250-262.

Vidriková, Dagmar, Boc, Kamil, Dvořák, Zdenek, Řehák, David. (2017). *Critical Infrastructure and Integrated Protection*. Ostrava: The Association of Fire and Safety Engineering.

von Bertalanffy, Ludwig. (1950). An outline of general systems theory. *Br J Philos Sci* 1 (2), pp. 134-165.

von Bertalanffy, Ludwig. (1968). *General Systems Theory: Foundations, Developments, Applications*. New York: George Braziller.

von Bertalanffy, Ludwig. (1972). The History and Stauts of General System Theory. *The Academy of Management Journal* 15 (4), pp. 407-426.

von Bertalanffy, Ludwig. (1973). „The meaning of general system theory". *General system theory: Foundations, development, applications* (pp. 30-53). New York: George Braziller.

Vršec, Miran. (2011). „The Role and Risks of Outsourcing in the Processes of Providing Corporate Security in Critical Infrastructure". In: D. Čaleta and P. Shemella (Eds.). *Counter terrorism challenges regarding the process of critical infrastructure protection* (pp. 47-66). Institute for Corporative Security Studies - ICS; Center for Civil-Military Relations.

Vuković, Milovan, and Štrbac, N. (2019). *Metodologija naučnih istraživanja*. Bor: Tercija.

Walby, Kevin and Lippert, Randy. (2014). „Introduction: Governing Every Person, Place, and Thing — Critical Studies of Corporate Security". In: K. Walby and R. Lippert (Eds.). *Corporate Security in the 21st Century* (pp. 1-13). Hampshire: Palgrave Macmillan.

Walby, Kevin, and Lippert, Randy. (2015a). *Municipal Corporate Security in International Context* (1st ed.). Routledge.

Walby, Kevin, and Lippert, Randy. (2015б). The difference homeland security makes: Comparing municipal corporate security in Canada and the United States. *Security Dialogue* 46 (3), pp. 238–255.

Walby, Kevin, Lippert, K. Randy, and Gacek, James. (2016). „Securitising 'National Interests': Canadian Federal Government Departments, Corporate Security Creep, and Security Regimes. In: Lippert, R., Walby, K., Warren, I., Palmer, D. (Eds.). *National Security, Surveillance and Terror. Crime Prevention and Security Management* (pp. 155-176). Palgrave Macmillan, Cham.

Walby, Kevin, Luscombe, Alex and Lippert, Randy. (2014). „Corporate Security and Enterprise Risk Management". In: K. Walby and R. Lippert (Eds.). *Corporate Security in the 21st Century* (pp. 116-133). Hampshire: Palgrave Macmillan.

Walker, Jeremy, and Cooper, Melinda. (2011). Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation. *Security Dialogue* 42, pp. 143-160.

Weber, Maks. (1999). *Vlast i politika*, preveli Vjeran Katunarić, Senka Burić i Ivan Burić. Zagreb: Naklada Jesenski i Turk.

Weber, Valentin, Pericàs Riera, Maria, and Laumann, Emma. (2023). *Mapping the World's Critical Infrastructure Sectors, DGAP Policy Brief 35*. German Council on Foreign Relations.

Weiss, P. Robert. (1986). „Private Detective Agencies and Labour Discipline in the United States, 1855-1946", *The Historical Journal*, 29 (1), pp. 87-107.

Weiss, P. Robert. (2014). „Corporate Security at Ford Motor Company: From the Great War to the Cold War". In: K. Walby and R. Lippert (Eds.), *Corporate Security in the 21st Century* (pp. 17-38). Hampshire: Palgrave Macmillan.

Welker, A. Marina. (2009). Corporate security begins in the community': mining, the corporate social responsibility industry, and environmental advocacy in Indonesia. *Cultural anthropology* 24 (1), pp. 142-179.

White House. (2003). *The Physical Protection of Critical Infrastructures and Key Assets*.

White, Adam. (2012). The new political economy of private security. *Theoretical Criminology* 16, pp. 85-101.

Williams, W. James. (2005). „Reflections on the Private versus Public Policing of Economic Crime", *British Journal of Criminology* 45 (3), pp. 316-339.

Wolfers, Arnold. (1952). "National Security" as an Ambiguous Symbol. *Political Science Quarterly* 67 (4), pp. 481-502.

Wolfers, Arnold. (1962). *Discord and Collaboration – Essays on International Politics*. Baltimore: THE JOHNS HOPKINS PRESS.

Wright, D. James. (2015). *International Encyclopedia of the Social and Behavioral Sciences* (2nd edition). Oxford: Elsevier.

Yalichev, Serge. (1997). *Mercenaries of the Ancient World*. Edinburgh: Constable.

Yusta, M. Jose, Correa J. Gabriel, and Lacal-Arántegui, Roberto. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy policy* 39 (10), pp. 6100-6119.

Żaboklicka, Ewa. (2020). Critical infrastructure in the shaping of national security. *Security and Defence Quarterly* 28 (1), pp. 70-81.

Закон о ваздушном саобраћају. (2010). *Сл. гласник РС*, бр. 73/2010, 57/2011, 93/2012, 45/2015, 66/2015, 83/2018, 9/2020, 62/2023.

Закон о безбедности и здрављу на раду. (2023). *Сл. гласник РС*, бр. 35/2023.

Закон о централном регистру обавезног социјалног осигурања. (2018). *Сл. гласник РС*, бр. 95/2018, 91/2019.

Закон о доприносима за обавезно социјално осигурање. (2004). *Сл. гласник РС*, бр. 84/2004, 61/2005, 62/2006, 5/2009, 52/2011, 101/2011, 47/2013, 108/2013, 57/2014, 68/2014, 112/2015, 113/2017, 95/2018, 86/2019, 153/2020, 44/2021, 118/2021, 138/2022, 92/2023.

Закон о државним и другим празницима у Републици Србији. (2001). *Сл. гласник РС*, бр. 43/2001, 101/2007, 92/2011.

Закон о евиденцијама у области рада. (1996). *Сл. гласник РС*, бр. 46/1996, РС 101/2005, РС 36/2009.

Закон о информационој безбедности. (2016). *Сл. гласник РС*, бр. 6/2016, 94/2017, 77/2019.

Закон о интегрисаном спречавању и контроли загађивања животне средине. (2004). *Сл. гласник РС*, бр. 135/2004, 25/2015, 109/2021.

Закон о јавним набавкама. (2019). *Сл. гласник РС*, бр. 91/2019, 92/2023.

Закон о јавним предузећима и обављању делатности од општег интереса. (2000). *Сл. гласник РС,* бр. 25/2000.

Закон о јавним предузећима. (2016). *Сл. гласник РС,* бр. 15/2016, 88/2019.

Закон о критичној инфраструктури. (2018). *Сл. гласник РС*, бр. 87/2018.

Закон о мирном решавању радних спорова. (2004). *Сл. гласник РС*, бр. 125/2004, 104/2009, 50/2018.

Закон о облигационим односима. (1978). *Сл. гласник*, бр. 29/1978, 39/1985, 45/1989, 57/1989, 31/1993, РС 18/2020.

Закон о одговорности правних лица за кривична дела. (2008). *Службени гласник РС,* бр. 97/2008.

Закон о планирању и изградњи. (2009). *Сл. гласник РС*, бр. 72/2009, 81/2009, 64/2010, 24/2011, 121/2012, 42/2013, 50/2013, 98/2013, 132/2014, 145/2014, 83/2018, 31/2019, 37/2019, 9/2020, 52/2021, 62/2023.

Закон о порезима на употребу, држање и ношење добара. (2001). *Сл. гласник РС*, бр. 26/2001, 80/2002, 43/2004, 31/2009, 101/2010, 24/2011, 68/2014, 112/2015, 86/2019, 118/2021, 92/2023.

Закон о приватном обезбеђењу. (2013). *Сл. гласник РС*, бр. 104/2013, 42/2015, 87/2018.

Закон о привредним друштвима. (2011). *Службени гласник РС,* бр. 36/2011, 99/2011, 83/2014 - др. закон, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021, 19/2025.

Закон о процени утицаја на животну средину. (2004). *Сл. гласник РС*, бр. 135/2004, 36/2009.

Закон о професионалној рехабилитацији и запошљавању особа са инвалидитетом. (2009). *Сл. гласник РС*, бр. 36/2009, 32/2013.

Закон о раду. (2005). *Сл. гласник РС*, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017, 113/2017, 95/2018.

Закон о родној равноправности. (2021). *Сл. гласник РС*, бр. 52/2021.

Закон о слободном приступу информацијама од јавног значаја. (2004). *Сл. гласник РС*, бр. 120/2004, 54/2007, 104/2009, 36/2010,105/2021.

Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама. (2018). *Сл. гласник РС*, бр. 87/2018.

Закон о спречавању дискриминације особа са инвалидитетом. (2006). *Сл. гласник РС,* бр. 33/2006, 13/2016.

Закон о спречавању злостављања на раду. (2010). *Сл. гласник РС*, бр. 36/2010.

Закон о штрајку. (1996). *Сл. лист СРЈ*, бр. 29/96 и *Сл. гласник РС*, бр. 101/2005, 103/2012.

Закон о тајности података. (2009). *Сл. гласник РС*, бр. 104/2009.

Закон о условима за упућивање запослених на привремени рад у иностранство и њиховој заштити. (2015). *Сл. гласник РС*, 91/2015, 50/2018.

Закон о волонтирању. (2010). *Сл. гласник РС*, бр. 36/2010.

Закон о забрани дискриминације. (2009). *Сл. гласник РС*, бр. 22/2009, 52/2021.

Закон о запаљивим и горивим течностима и запаљивим гасовима. (2015). *Сл. гласник РС*, бр. 54/2015.

Закон о запошљавању и осигурању за случај незапослености. (2009). *Сл. гласник РС,* бр. 36/2009, 30/2010, 88/2010, 38/2015, 113/2017, 113/2017, 49/2021.

Закон о запошљавању странаца. (2014). *Сл. гласник РС,* бр. 128/2014, 113/2017, 50/2018, 31/2019, 62/2023.

Закон о заштити од буке у животној средини, *Сл. гласник РС*, бр. 96/2021.

Закон о заштити од пожара, *Сл. гласник РС*, бр. 111/2009, 20/2015, 87/2018, 87/2018, 87/2018.

Закон о заштити података о личности. (2018). *Сл. гласник РС*, бр. 87/2018.

Закон о заштити пословне тајне. (2021). *Сл. гласник РС*, бр. 53/2021.

Закон о заштити природе. (2009). *Сл. гласник РС*, бр. 36/2009, 88/2010, 91/2010, 14/2016, 95/2018, 71/2021.

Закон о заштити становништва од изложености дуванском диму. (2010). *Сл. гласник РС*, бр. 30/2010.

Закон о заштити узбуњивача. (2014). *Сл. гласник РС*, бр. 128/2014.

Закон о заштити животне средине. (2004). *Сл. гласник РС*, бр. 135/2004, 36/2009, 36/2009, 72/2009, 43/2011, 14/2016, 76/2018, 95/2018.

Закон о здравственом осигурању. (2019). *Сл. гласник РС*, бр. 25/2019, 92/2023.

Закон о агенцијском запошљавању. (2019). *Сл. гласник РС*, бр. 86/2019.

Закон о одбрани. (1994). *Сл. лист СРЈ,* бр. 43/94, 11/95, 28/96, 44/99, 3/2002.

Закон о одбрани. (2007). *Сл. гласник РС*, бр. 116/2007, 88/2009, 88/2009, 104/2009, 10/2015, 36/2018.

Закон о заштити ваздуха. (2009). *Сл. гласник РС*, бр. 36/2009, 10/2013, 26/2021.

Закон о оружју и муницији. (2015). *Сл. гласник РС*, бр. 20/2015, 10/2019, 20/2020, 14/2022.

Закон о јавном окупљању. (2016). *Службени гласник РС*, бр. 6/2016.

Закон о полицији. (2016). *Службени гласник РС*, бр. 6/2016, 24/2018, 87/2018.

Zarate, Juan Carlos. (1998). The emergence of a new dog of war: Private international security companies, international law, and the new world disorder. *Stan. J. Int'l L.* 34, pp. 75-162.

Zedner, Lucia. (2006). Liquid security: Managing the market for crime control. *Criminology and Criminal Justice* 6 (3), pp. 267-288.

Zedner, Lucia. (2006). Policing Before and After the Police. *British Journal of Criminology* 46, pp. 78-96.

Zimmerman, Rae, Restrepo, E. Carlos, Dooskin, J. Nicole, Hartwell, V. Ray, Miller, I. Justin, Remington, E. Wendy, Simonoff, S. Jeffrey, Lave, B. Lester, and Schuler, E. Richard. (2005). *Electricity case: main report-risk, consequences, and economic accounting*. Los Angeles: CREATE.

Zimmerman, Rae. (2004). Decision-making and the vulnerability of interdependent critical infrastructure. In: *2004 IEEE International Conference on Systems, Man and Cybernetics* (IEEE Cat. No. 04CH37583) (pp. 4059-4063). IEEE.

Живановић, М. Вукојица, и Радојевић, М. Слободан. (2024). Политика одбране заснована на концепту тоталне одбране. *Политика националне безбедности*, 26 (1), стр. 165-188.

8. ПРИЛОЗИ

8.1. Прилог 1: Правна лица (велики технички системи од значаја за одбрану (критична инфраструктура)) која су обухваћена истраживањем

1. Предузеће за телекомуникације „Телеком Србија" акционарско друштво, Београд;
2. BELGRADE AIRPORT d.o.o. Beograd;
3. Контрола летења Србије и Црне Горе SMATSA д.о.о., Београд;
4. Акционарско друштво „Електропривреда Србије", Београд са зависним привредним друштвима;
5. Акционарско друштво 'Електромрежа Србије', Београд;
6. „НИС" а.д., Нови Сад и његова зависна привредна друштва;
7. ХИП-ПЕТРОХЕМИЈА д.о.о. Панчево;
8. ТРАНСНАФТА АД Панчево;
9. Јавно комунално предузеће „Београдски водовод и канализација", Београд;
10. Јавно предузеће за водоснабдевање „Рзав", Ариље;
11. Јавно предузеће за газдовање шумама „Србијашуме" са потпуном одговорношћу, Београд.

8.2. Прилог 2: Иницијална питања за експертски интервју са руководиоцима на пословима безбедности у великим техничким системима од значаја за одбрану (критична инфраструктура)

УПИТНИК ЗА ЕКСПЕРТСКИ ИНТЕРВЈУ

Поштовани/а,

за потребе писања докторске дисертације под називом „Корпоративна безбедност као елемент система националне безбедности у заштити критичне инфраструктуре Републике Србије" пријављеној на Факултету безбедности Универзитета у Београду, планирано је спровођење интервјуа са експертима из области корпоративне безбедности, који су запослени у правним лицима која представљају критичну инфраструктуру Републике Србије.

Сврха интервјуа јесте прикупљање података у циљу утврђивања да ли и на који начин корпоративна безбедност кроз заштиту критичне инфрастуктуре доприноси функционисању система националне безбедности Републике Србије и тиме остварењу њене националне безбедности као стања. Прикупљени подаци користиће се искључиво у научне сврхе односно за потребе израде докторске дисертације.

Планирано је бележење аудио снимка тока разговора (уз сагласност) на месту и времену према договору. Интервју садржи 29 питања распоређених у две групе.

Хвала Вам на издвојеном времену и сарадњи!

Прва група питања

1. Како бисте описали улогу корпоративне безбедности у систему националне безбедности наше земље?

2. Да ли сматрате да корпоративна безбедност (успостављена у организацији) може допринети националној безбедности? Објасните свој став.
3. Да ли сматрате да корпоративна безбедност (успостављена у организацији) може бити партнер Министарству унутрашњих послова (полицији) у остваривању јавне безбедности? Објасните свој став.
4. Уколико је одговор на претходно питање ДА, које су то области или послови где се сарадња/партнерство може остварити?
5. Каква је по Вашем мишљењу нормативна уређеност корпоративне безбедности у односу на заштиту критичне инфраструктуре од?
6. Како оцењујете допринос закона и пратећих подзаконских аката из области корпоративне безбедности на њен рад и функционалнст и које бисте кључне проблеме идентификовали, уколико сматрате да постоје?
7. На који начин по Вашем мишљењу треба унапредити правни оквир како би се омогућило ефикасно функционисање корпоративне безбедности у функцији заштите критичне инфраструктуре?
8. Како бисте унапредили безбедност критичне инфраструктуре у нашој земљи?
9. Како би требало да се организује праћење заштите критичне инфраструктуре у систему националне безбедности?
10. Да ли сте били (или сте и даље) члан професионалног или стручног удружења или сте присуствовали састанцима/скуповима који су били посвећени унапређењу безбедности критичне инфраструктуре на нивоу локалне заједнице или државе?
11. Уколико је одговор на претходно питање ДА, да ли сматрате да се на тим састанцима/скуповима води довољна расправа о унапређењу безбедности критичне инфраструктуре?

Друга група питања

1. Која је Ваша област стручног ангажовања и на којим пословима радите у организацији? (Ваша радна позиција)
2. На основу чега су успостављене организација и функције корпоративне безбедности у Вашој организацији?
3. Како су организовани послови корпоративне безбедности у Вашој организацији?
4. Уколико је корпоративна безбедност посебна организациона целина, можете ли ми рећи назив организационе целине и њену организациону структуру?
5. Уколико је корпоративна безбедност посебна организациона целина, можете ли ми рећи у каквом је односу са другим организационим целинама, а посебно са топ менаџментом, главним/извршним директором?
6. На који начин менаџмент организације подржава мисију корпоративне безбедности?
7. На који начин се унапређује корпоративна безбедност у Вашој организацији?
8. Који се послови/функције корпоративне безбедности реализују у Вашој организацији?
9. Који су штетни догађаји са којима се суочила Ваша организација?
10. Која су три најважнија потенцијална ризика по Вашу организацију?

11. Како оцењујете досадашњу сарадњу са Министарством унутрашњих послова на пољу остваривања безбедности? Наведите случајеве сарадње.
12. Шта по Вашем мишљењу може да се унапреди по питању те сарадње?
13. Да ли Ваша организација користи услуге правних лица и предузетника за приватно обезбеђење или за детективску делатност?
14. Уколико је одговор на претходно питање ДА, за које услуге/послове исте ангажујете?
15. Да ли и колико сте задовољни радом правних лица и предузетника за приватно обезбеђење или за детективску делатност? Објасните свој став.
16. Које бисте кључне проблеме издвојили у вези са ангажовањем и радом правних лица и предузетника за приватно обезбеђење или за детективску делатност, уколико сматрате да постоје?
17. Који су по Вашем мишљењу разлози изнајмљивања ових услуга?
18. Ваш став о нечему што сматрате значајним, а што није обухваћено интервјуом.

9. БИОГРАФИЈА КАНДИДАТКИЊЕ

Јана М. Марковић рођена је 17. јуна 1996. године у Крагујевцу, где је завршила основну и средњу школу – гимназију. Факултет безбедности уписала је 2015. године и слушала је предмете са изборне групе *студије безбедности*. У фебруару 2020. године одбранила је дипломски рад на тему „Угорженост и заштита експоната у музејима“ и закључно њиме остварила просечну оцену 9,51. Мастер студије на Факултету безбедности уписала је исте године определивши се за изборну групу *корпоративна безбедност* на смеру *студије наука безбедности*. У септембру 2021. године одбранила је мастер рад на тему „Континитет пословања као функција корпоративне безбедности“ са оценом 10, и закључно њиме остварила просечну оцену 9,88. Докторске студије на Факултету безбедности уписала је 2021. године. Говори енглески језик.

Исте године, постала је демонстратор на Факултету безбедности, на катедри *студије безбедности.* Била је стипендиста Министарства просвете, науке и технолошког развоја од 2022. до јануара 2023. када је засновала радни однос на Факултету безбедности у својству сарадника у настави на предмету Корпоративна безбедност.

Јана М. Марковић је објавила више од десет академских радова из области студија безбедности и посебно, приватне и корпоративне безбедности, као и неколико приказа публикација. Била је технички уредник Зборника радова *Друга меморијална научна конференција „Предраг Марић“* (2023) и уредник Зборник сажетака *Трећа научна конференција – Урбана безбедност и урбани развој* (2024). Од 2023. до 2025. године обављала је дужност секретара научног часописа *Савремене студије безбедности* у издању Факултета безбедности.

Учествовала је на неколико националних и међународних научних конференција. Била је у организационом техничком одбору две националне конференције: Друга научна конференција Урбана безбедност и урбани развој (2022) и Трећа научна конференција Урбана безбедност и урбани развој (2024). Била је у организационом одбору две међународне конференције: *Innovation, Research, and Knowledge in the (Re)configuration of Human Security* (Београд, новембар 2022) и *Geography, Identity, and Politics: Concepts, Theories, and Cases in Geopolitical Analysis* (Будимпешта, октобар 2024).

Била је ангажована као волонтер на пројекту *Управљање новим безбедносним ризицима – истраживање и развој симулација*, NEWSIMR&D, #7749151, који финансира Фонд за науку Републике Србије у оквиру Програма „ИДЕЈЕ“.

Изјава о ауторству

Име и презиме аутора **Јана М. Марковић**

Број индекса **д2/21**

Изјављујем

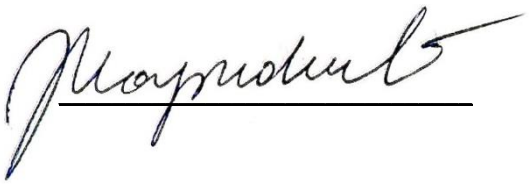
да је докторска дисертација под насловом

Корпоративна безбедност као елемент система националне безбедности у заштити критичне инфраструктуре Републике Србије

- 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/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, **18. 03. 2025.**



Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора **Јана М. Марковић**

Број индекса **д2/21**

Студијски програм **Студије наука безбедности**

Наслов рада **Корпоративна безбедност као елемент система националне безбедности у заштити критичне инфраструктуре Републике Србије**

Ментор **др Горан Ј. Мандић, ванредни професор**

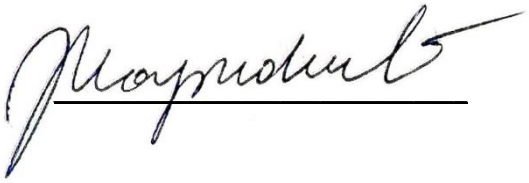
Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањивања у **Дигиталном репозиторијуму Универзитета у Београду.**

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, **18. 03. 2025.**



Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Корпоративна безбедност као елемент система националне безбедности у заштити критичне инфраструктуре Републике Србије

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

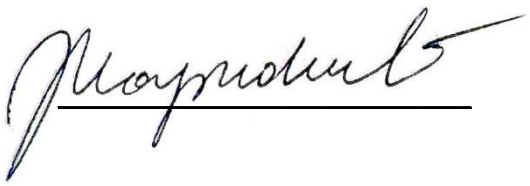
Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

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)

(Молимо да заокружите само једну од шест понуђених лиценци.
Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, **18. 03. 2025.**



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 дозвољавакомерцијалну 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.