Јана МАРКОВИЋ
сарадник у настави, Факултет безбедности Универзитета у Београду

ДОИ: 10.5937/bezbednost2302197M
УДК: 005.934:351.82(497.11)
Прегледни научни рад
Примљен: 21. 3. 2023. године
Ревизија: 6. 4. 2023. године
Датум прихватања: 14. 7. 2023. године

Улога корпоративне безбедности у заштити критичне инфраструктуре Републике Србије

Апстракт: *Критична инфраструктура се може представити као елемент државе неопходан за њено функционисање и уједно услов обезбеђивања основних функција и пружања услуга државе према њеним грађанима. С друге стране, корпоративна безбедност се може представити као скуп функција које имају за циљ заштиту свих вредности ентитета у који је она (корпоративна безбедност) инкорпорирана, од свих претњи, без обзира на њихово порекло, врсту и интензитет, и то активностима проактивног и/или реактивног карактера. У раду се полази од идеје да, поред државе и њених органа, у заштити критичне инфраструктуре значај допринос даје корпоративна безбедност, као безбедност успостављена унутар свих ентитета који управљају системима, мрежама, објектима или њиховим деловима који су одређени као критична инфраструктура. Након анализе сектора критичне инфраструктуре у Републици Србији и земљама у окружењу, и стања њене заштите у нашој држави, као и кратког осврта на значај који корпоративна безбедност има за државу и њену националну безбедност, циљ рада је представити начин на који корпоративна безбедност кроз своје функције обезбеђује и доприноси свеукупној заштити критичне инфраструктуре.*

Кључне речи: *критична инфраструктура, заштита критичне инфраструктуре, корпоративна безбедност, функције корпоративне безбедности.*

Увод

Корпоративна безбедност јесте јединствен део општег безбедносног домена, систем и функција која је успела да обједини послове обезбеђења (*security*) и послове заштите (*safety*) који се већ дуго времена, а несрећно понекада и даље, идентификују као једно, а заправо пре представљају две стране једног сегмента безбедности. Иако је блиско повезана са корпоративним моделом којем обезбеђује део услова опстанка и функционисања, без обзира да ли је он приватног или јавног карактера, она (корпоративна безбедност) јесте феномен који делује како на националном, тако и на међународном нивоу. С једне стране, може се посматрати као део приватне безбедности која је успостављена на међународном нивоу, како су бројна правна лица која пружају услуге приватне безбедности међународног карактера. С друге стране, корпоративна безбедност припада систему приватне безбедности једне државе, чинећи на тај начин уједно и елемент националне безбедности државе. Уз то, ако сви системи безбедности националних држава припадају вишем, међународном систему, онда је и на тај начин корпоративна безбедност сваке организације[46] инкорпорирана у систем међународне безбедности.

Циљ рада јесте да укаже на улогу корпоративне безбедности у заштити критичне инфраструктуре којом уједно доприноси свеобухватном значају који има за систем безбедности и функционисање државе уопште.

Рад је садржински подељен на неколико целина, тако да се у оквиру сваке целине проблематизује питање релевантно за разумевање теме рада. Најпре је теоријски представљена критична инфраструктура са посебним акцентом на критичној инфраструктури у Републици Србији и начину њене уређености. Уз то, дат је и упоредни приказ идентификованих сектора критичне инфраструктуре у Републици Србији и државама у окружењу. Како је критична инфраструктура „критични" сегмент једне државе, тако се фокус помера на допринос или улогу коју корпоративна безбедност има

46 Термин „корпоративна безбедност" потиче од термина „корпорација". У домаћој правној терминологији, термин „правно лице" је потпуни еквивалент термину „корпорација". Појам организације јесте шири од појма правног лица и/или корпорације и широко је заступљен у литератури, па ће се из тог разлога овај појам наизменично користити са појмом правног лица.

управо у заштити критичне инфраструктуре. Иако је чине бројни елементи, који делујући заједно омогућавају постизање циљева због којих је успостављена, у складу са нивоом ризика и степеном последица које би могле да наступе услед испољавања тих ризика, издвојени су само неки од елемената корпоративне безбедности о којима ће бити речи у наставку рада.

Критична инфраструктура – основа функционисања државе

Критична инфраструктура се састоји од система (пре свега физичких, али и све заступљенијих виртуелних) који се сматрају основним за функционисање друштва и привреде, јер обезбеђују енергију, транспорт, телекомуникације и информационе услуге, снабдевање храном и водом и виталне здравствене услуге. Поремећај или уништење критичне инфраструктуре услед природних катастрофа, техничко-технолошких несрећа и криминалних активности имало би негативне, директне и посредне, последице по свакодневни живот, добробит грађана, и уједно безбедност државе. Данас се као значајне претње најчешће издвајају тероризам, организовани криминал и, самостално или у комбинацији са наведеним, сајбер претње. Нормално функционисање државе и њених грађана могло би бити у мањој или већој мери угрожено, а континуирано обезбеђивање и пружање услуга и задовољење потреба грађана нарушено. Уз то, како примећују Браун (Brown) и сарадници, сваки сектор критичне инфраструктуре представља огромну јавну инвестицију, па би „чак и мањи поремећај, насумично или намерно изазван, могао да деградира перформансе система и нанесе значајне економске губитке" (Brown et al., 2006: 530).

Значајно је указати на повезаност и међусобну зависност различитих критичних инфраструктура. Узмимо за пример електричну енергију, чије је континуирано снабдевање неопходно за све остале критичне инфраструктуре. С друге стране, електроенергетски системи не могу остварити своју улогу без подршке коју им обезбеђују критичне инфраструктуре из области телекомуникационих и информационих технологија.

Информациона и (теле)комуникациона технологија данас су присутне у готово свакој сфери друштвеног живота, па би „квар"

на њима могао проузроковати озбиљне последице, како по друге системе критичне инфраструктуре, тако и по сваки други сегмент функционисања државе. У *Стратегији развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године* наглашена је потреба за унапређењем критичне информационе инфраструктуре „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 за период од 2021. до 2026. године, 2021: 76).

Сасвим је сигурно да међузависност може побољшати оперативну ефикасност инфраструктуре, али иста та међузависност може допринети повећању рањивости система, па оштећење у једном сектору критичне инфраструктуре може произвести каскадне кварове, ширећи ефекте на регионални или национални ниво (Ouyang, 2014). С обзиром на велику међузависност (физичку, сајбер, географску и/или логичку (Мићовић, 2020: 38)) сложених система критичне инфраструктуре у оквиру једне државе, присутан је домино ефекат у виду „преливања" последица са једног система на други. Чињеница да су системи критичне инфраструктуре све повезанији, као и да су природни облици угрожавања све учесталији, а они изазвани људским чињењем (или комбиновани) све разноврснији и комплекснији, заштита критичне инфраструктуре се намеће као озбиљно питање и задатак.

Критична инфраструктура у Републици Србији

У Републици Србији се питања у вези са критичном инфраструктуром ближе уређују Законом о критичној инфраструктури (Сл. гласник РС, бр. 87/2018-41). Према овом закону, критичну инфраструктуру чине „системи, мреже, објекти или њихови делови, 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".

Иако не под термином *критична инфраструктура*, Закон о приватном обезбеђењу (Сл. гласник РС, бр. 104/2013-8, 42/2015-3, 87/2018-31) издваја обавезно обезбеђене објекте дефинишући их као објекте „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).

Узимајући у обзир ближе одређење објеката од посебног значаја у складу са Законом о одбрани (Сл. гласник РС, бр. 116/2007-3, 88/2009-3, 88/2009-31 – др. закон, 104/2009-13 – др. закон, 10/2015-3, 36/2018-11) и Одлуком о објектима од посебног значаја за одбрану (Сл. гласник РС, бр. 112/2008-22), одређени елементи критичне инфраструктуре из различитих сектора поклапају се са објектима који су одређени као посебно значајни.

Издваја се и Одлука о одређивању великих техничких система од значаја за одбрану (Сл. гласник РС, бр. 41/2014-3, 35/2015-22, 86/2016-6, 53/2017-51, 26/2019-11, 94/2019-83, 67/2021-36, 62/2022-4), којом су у ресурсе критичне инфраструктуре укључена четири велика техничка система из области телекомуникација, затим осам из области саобраћаја, седам из области енергетике, седам из области водоснабдевања и пет из других области (радио-дифузије, производња и промет гасова и пратеће опреме, газдовања шумама).

Да би се могло говорити о заштити критичне инфраструктуре, предуслов је извршити њену идентификацију, и то секторски и према утврђеним критеријумима. Критеријуми за то прописани су посебним правним актом – Уредбом о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије (Сл. гласник РС, бр. 69/2022). Као критеријуми за идентификацију критичне инфраструктуре узимају се последице које могу наступити услед прекида рада система, мрежа, објеката или њихових делова, и то по секторима. Сектори у којима се врши идентификација и одређивање критичне инфраструктуре јесу: енергетика, саобраћај, снабдевање водом и

храном, здравство, финансије, телекомуникационе и информационе технологије, заштита животне средине и функционисање државних органа.

Национална процена ризика Републике Србије од катастрофа, израђена на основу Упутства о Методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања (Сл. гласник РС, бр. 80/2019-105), садржи 11 идентификованих сектора критичне инфраструктуре, односно, поред осам сектора наведених у предметном Закону и Уредби, раздваја снабдевање водом и снабдевање храном, унапређује функционисање државних органа у функционисање органа државне управе и хитних служби и додаје као посебан сектор науку и образовање (МУП РС, 2019).

Ако се узму у разматрање идентификације критичне инфраструктуре земаља у окружењу, на основу правног акта којим се регулише ова област у свакој земљи, ситуација је врло слична (Табела 1).

Табела 1: *Упоредни приказ идентификованих сектора критичне инфраструктуре, на основу правног акта којим се регулише ова област, у Републици Србији и државама суседима*[47]

Сектор	Србија	Црна Гора	Република Српска	Хрватска	Мађарска	Румунија	Бугарска	С. Македонија	Република Албанија
енергетика	+	+	индустрија, енергетика и рударство	+	+	+	+	/	/
саобраћај/ транспорт	+	+	+	+	+	+	+	/	/
снабдевање водом	+	+	+ комуналне делатности и водоснабдевање	+	+	+		/	/
снабдевање храном	+		+	+	пољопривреда	+ пољопривреда	+ пољопривреда	/	/
здравство	+	+	+	+	+	+	+	/	/
финансије/ банкарство	+	+	+	+	+	+	+	/	/

47 У табели је знаком „+" означено идентификовање сектора; код сектора са измењеним називом стављен је назив преузет из анализираног акта, а код сектора који су идентификовани уз „додатак" стављени су и знак „+" и тај „додатак".

Сектор	Србија	Црна Гора	Република Српска	Хрватска	Мађарска	Румунија	Бугарска	С. Македонија	Република Албанија
(теле) комуникационе и информационе технологије/ инфраструктуре	+	електронских комуникација и информационо-комуникационих технологија	+	+	+	+	+	/	/
заштита животне средине	+	+				+	+	/	/
функционисање државних органа	+	+						/	/
функционисање јавних (хитних) служби	+		+	+				/	/
наука и образовање	+		васпитање и образовање				+ технологија	/	/
производња, складиштење и превоз опасних материја			+	+				/	/
национални споменици и вредности			културна и природна добра	+	култура и наслеђе националне културе		културна баштина	/	/
социјално осигурање					+			/	/
(народна) одбрана					+	национална безбедност	+	/	/
заштита јавне безбедности					+		правда, јавни ред и безбедност	/	/
администрација						+		/	/
индустрија						+		/	/
простор и истраживање						+		/	/
поштанске и курирске услуге							+	/	/
економија							+	/	/
спортски објекти							+	/	/
природни ресурси							+	/	/
туризам							+	/	/
регионални развој и унапређење							+	/	/
државно и друштвено управљање							+	/	/
заштита од катастрофе							+	/	/

Извор: Аутор

Не задржавајући се на анализи података представљених у претходној табели, могуће је уочити да све државе за које су подаци доступни и анализирани препознају седам сектора критичне инфраструктуре (енергетика, саобраћај/транспорт, снабдевање водом, снабдевање храном, здравство, финансије/банкарство, (теле)комуникационе и информационе технологије/инфраструктуре) одређених у истом или сличном, проширеном контексту[48].

Уколико се осврнемо на више правне акте у Републици Србији, уређеност области критичне инфраструктуре је следећа. Упркос томе што Стратегија националне безбедности садржи неколико одредаба[49] које се односе на критичну инфраструктуру, обим у којем се овај стратешки документ бави критичном инфраструктуром и њеном заштитом никако није адекватан уколико се узме у обзир правна снага коју има у правном систему наше земље. У Стратегији одбране приступ је другачији и комплетнији. Осигурање безбедности објеката критичне инфраструктуре издвојено је као један од циљева заштите безбедности Републике Србије и њених грађана, акценат је стављен на потпуно спровођење нормативно-правних решења, као и непрекидно предузимање свих превентивних мера, и успостављање интегрисаног информационог система за безбедносни надзор објеката критичне инфраструктуре (Стратегија одбране РС, 2019).

Оно што може бити интересантно када је реч о надлежностима у вези са критичном инфраструктуром, јесте то да је Министарство унутрашњих послова одређено да „уређује, планира, координира, контролише активности, комуницира и даје информације у вези са критичном инфраструктуром" (Закон о критичној инфраструктури, 2018: члан 4), док покровитељство над објектима од посебног значаја за одбрану има Министарство одбране. Уз то, кри-

48 У законској регулативи Црне Горе, сектор снабдевања храном није изричито препознат, али садржи одредбу „као и у другим областима од јавног интереса" (Zakon, 2019: члан 6), под којом се и овај сектор може подвести. С друге стране, када је реч о секторима у Бугарској, сектор снабдевања водом препознат је као подсектор сектора (заштите) животне средине (Наредба, 2012: члан 2).

49 Потреба за појачаном заштитом критичне енергетске инфраструктуре услед повећаног броја сукоба изазваних надметањем за обезбеђење енергената и других природних сировина; препознавање напада на критичну инфраструктуру као фактора угрожавања безбедности, условљено глобалним развојем информационих технологије; идентификовање и заштита објеката критичне инфраструктуре (Стратегија националне безбедности РС, 2019).

тичној инфраструктури је у Стратегији одбране посвећено знатно више пажње него у вишој стратегији – Стратегији националне безбедности. Наравно, како не постоји стратегија која би уређивала област унутрашњих послова на одговарајућем нивоу општости, она се не може ни разматрати. Како критична инфраструктура заузима простор одређених сектора, поред Министарства унутрашњих послова, активности од значаја за заштиту критичне инфраструктуре спроводе министарства задужена за секторе критичне инфраструктуре и оператори критичне инфраструктуре[50]. 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), у складу са Законом о смањењу ризика од катастрофа и управљању ванредним ситуацијама (Сл. гласник РС, бр. 87/2018-3).

Улога корпоративне безбедности и њених функција у заштити критичне инфраструктуре

Да би се говорило о самој улози коју корпоративна безбедност има у заштити критичне инфраструктуре, неопходно је сагледати елементе који је чине и преко којих она ову своју улогу и остварује. Најједноставније одређење било би да функције корпоративне безбедности чине физичка и техничка заштита свих материјалних (физичких и финансијских) и нематеријалних (људских и других нематеријалних) ресурса организације подржане стратешким документима, политикама и процедурама рада, као административни део или безбедносни менаџмент. Ипак, овакво тумачење није само најједноставније, већ је и непотпуно, а самим тим и неисправно, будући да не обухвата неке од суштинских елемената који због свог значаја треба да буду препознати као засебни.

Аутори (Kovacich, Halibozek, 2003: 161; Cabric, 2015: 23; Цигурски, 2015: 257; Brooks, 2013; Мандић и Станојевић, 2020: 27) који су

50 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).

се бавили елементима корпоративне безбедности, препознали су мање-више исте елементе. Следећи њихова теоријска одређења, под корпоративну безбедност би се могли подвести следећи елементи:

- физичка, техничка и физичко-техничка заштита лица, имовине и пословања;
- безбедност података и информација уз заштиту (телекомуникационих) и информационих система;
- противпожарна заштита, безбедност и здравље на раду и заштита животне средине;
- управљање ризицима уз надзор и контролу и истраге;
- управљање кризама (кризни менаџмент) уз управљање континуитетом пословања.

Данас је тешко, па и немогуће, замислити системе или објекте критичне инфраструктуре који немају ангажовану или сопствену службу обезбеђења и имплементиране системе и елементе техничке заштите. Говоримо о службеницима обезбеђења који кроз своје делатности, примењујући овлашћења која имају у складу са позитивним правним прописима и интерним актима, доприносе безбедности локација на којима обављају своје послове и извршавају додељене задатке. Вршењем својих делатности, попут прегледа простора и патролирања, службеници обезбеђења прате реално стање у штићеном простору. Том приликом они могу да уоче било какво понашање које се санкционише, али и било какве неправилности или нерегуларности које не представљају нормално (уобичајено) стање ствари. Када је реч о постројењима која представљају критичну инфраструктуру, правовремено уочавање оштећења или уништења чак и најситнијих елемената, подрхтавања које није уобичајено, цурења материја[51] или сличних појава може допринети спречавању инцидената, односно, умањењу њихових последица, и управо у овим ситуацијама службеници обезбеђења могу имати значајну улогу. Због специфичности сектора и постројења где врше послове, поред основне обуке за добијање лиценце, службеници обезбеђења морају проћи и посебну обуку, прилагођену карактеристикама штићеног простора и задацима који су постављени пред њих. Том обуком они би се припремили за извршавање задатака

51 Један од начина детекције цурења јесу визуелна детекција, камере или детектори са делимичном покривеношћу (American Petroleum Institute, 2016: 512). Овај начин би службеници обезбеђења могли да примењују у оквиру својих активности.

специфичних за локацију коју обезбеђују, који би се могли сврстати у послове посебне намене. Уз то, говоримо о постављању елемената механичког карактера и имплементацији елемената и система електронске заштите, попут система видео-обезбеђења, алармних система или система којима се обезбеђује контрола приступа[52]. Успостављању физичке и техничке заштите мора претходити задовољење одређених обавеза, као што је израда посебних докумената у области приватног обезбеђења, попут акта о процени ризика у заштити лица имовине и пословања, и на основу њега, плана обезбеђења. У Републици Србији, област физичке, техничке и физичко-техничке заштите регулисана је у првом реду Законом о приватном обезбеђењу и прописима донетим на основу овог закона.

Сваки сектор критичне инфраструктуре користи податке и информације, и све је присутније њихово ослањање на информационо-комуникациону технологију (ИКТ). За ову област од значаја су Закон о тајности података и Закон о заштити пословне тајне са свим подзаконским актима, односно, Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године и Закон о информационој безбедности. Иако последњи наведени Закон препознаје ИКТ системе од посебног значаја, односно, критичну информациону инфраструктуру као посебну и значајну, то не ограничава ову функцију корпоративне безбедности само на овај сегмент националне критичне инфраструктуре.

Функције попут противпожарне заштите, безбедности и здравља на раду и заштите животне средине успостављене су и спроводе се, као и претходно наведене, на основу законских и подзаконских аката. Пракса, међутим, показује да су ове функције далеко више утемељене и самим тим регулисане и примењене од првог елемента – физичке, техничке и физичко-техничке заштите.

Све до сада наведене функције делују проактивно, а када дође до остварења неког од ризика и наступања кризе, њихова улога постаје реактивна. Можемо рећи да су до сада наведене функције подршка преосталим функцијама корпоративне безбедности – управљање ризицима и кризама. Без обзира на извор и врсту ризика, организација и њен менаџмент морају се континуирано бавити проценом

52 Више о наведеном у: Мандић, Ј. Г., Станојевић, П. (2020). Корпоративна безбедност. Факултет безбедности Универзитета у Београду, Београд.

и управљањем ризика у циљу њихове митигације, односно, избора најадекватније стратегије за поступање са ризиком (контрола, смањење, задржавање, пребацивање или трансфер). У већини ситуација, када су ризици идентификовани, могуће је пронаћи начине за њихово смањење. Ипак, проналажење ефикасних начина за деловање или поступање према њима често се не остварује услед пропуста у разумевању или управљању ризиком. На овој основи, развијени су бројни стандарди који дају смернице за менаџмент ризиком, међу којима је и технологија инспекције засноване на ризику (*Risk-Based Inspection Technology*), која је усмерена ка интегрисаном програму управљања ризицима и представља водећи стандард у петрохемијској индустрији[53]. Овај сегмент је у Републици Србији делом регулисан законском регулативом, која одређује операторе критичне инфраструктуре и обавезује их на израду безбедносног плана управљања ризиком. Тај план садржи анализу ризика на основу које се дефинишу безбедносни циљеви и мере (Закон о критичној инфраструктури, 2018: члан 2). Да би овакав план био израђен, неопходан је мултисекторски рад запослених код оператора критичне инфраструктуре, што се уједно може посматрати као остваривање надлежне функције корпоративне безбедности. Треба указати на то да је од значаја препознавање ризика како из спољашњег окружења, тако из унутрашњег окружења, односно, ризика које генеришу запослени, било у виду чињења санкционисаних дела или асоцијалног понашања које може да ескалира и нанесе штетне последице. Уколико се у обзир узме значај критичне инфраструктуре, као и чињеница да запослени у различитим секторима критичне инфраструктуре располажу значајним сазнањима о функционисању ових система и њихових делова, они (запослени) могу се препознати као озбиљна потенцијална претња. Одатле, као значајна функција корпоративне безбедности издвајају се надзор и контрола, као и спровођење истрага, које би за циљ имале благовремено уочавање потенцијалног или стварног угрожавања од стране запослених и правовремено предузимање потребних мера које би укључиле обавештавање и сарадњу са надлежним државним органима.

Подједнако важно као и управљање ризицима јесте управљање кризама. Кризни менаџмент, како се најчешће назива, треба да

53 Видети више у: American Petroleum Institute. (2016). *API RECOMMENDED PRACTICE 581 – Risk-Based Inspection Technology*.

идентификује могуће кризне ситуације, да се припреми за њихово наступање, односно, да припреми одговор на њих уколико се оне догоде, а све у циљу спречавања, односно, минимизирања негативних последица и повратка у стање нормалног функционисања. Као део кризног менаџмента, а све чешће као посебна функција, издваја се управљање континуитетом пословања. Ова функција „обезбеђује наставак пословања услед ометања или прекида изазваних кризом или неком другом непредвиђеном ситуацијом" (Марковић, 2021). Иако се може сматрати чисто реактивним приступом (Мандић и Станојевић, 2022: 445), да би се ефикасно управљало континуитетом пословања, потребно је предузети проактивне и припремне мере (развити стратегију, извршити анализу утицаја на пословање, дефинисати план). Ако сагледамо улогу и значај ове функције, јасно је да је потребно уложити све могуће напоре за њено успостављање и функционисање. На тај начин, обезбеђују се услови за континуирано функционисање сектора критичне инфраструктуре и њихових делова и самим тим континуирано пружање услуга држави и њеним грађанима. Уз то, ова функција свакако доприноси континуираном планирању заштите критичне инфраструктуре као једном од начела деловања (Закон о критичној инфраструктури, 2018: члан 3) у области критичне инфраструктуре у Републици Србији[54].

Закључак

Последице угрожавања критичне инфраструктуре могле би се сагледати са аспекта губитка људских живота, оштећења и/или уништења имовине, ометања и/или прекида пословних функција, економских, социјалних, еколошких и здравствених последица. Различити облици угрожавања, различитих степена вероватноће, интензитета и потенцијалних последица, комбиновани са све више повезаним, међузависним и уједно рањивијим системима критичне инфраструктуре, захтевају од свих заинтересованих актера на

54 На нивоу Европске уније препознато је значајно учешће приватног сектора у надгледању и управљању ризицима, планирању континуитета пословања и опоравку након катастрофе, па се државе чланице позивају на подстицање пуног учешћа приватног сектора у овим активностима (Directive 2008/114/EC, 2008). Република Србија прилагођава своје законодавне акте прописима Европске уније, па је оправдано очекивати да ће и сама тежити укључивању приватног сектора у ове активности.

националном и међународном нивоу, а у првом реду од држава, улагање напора у заштиту критичне инфраструктуре као један од основних предуслова изградње, одржања и унапређења отпорности државе и друштва. Због већ наведених карактеристика ових система, односно, њихове повезаности и међузависности која превазилази границе националне државе, све је важније радити на успостављању и јачању међудржавне сарадње и изградње стратешких партнерстава свих актера чија је делатност од круцијалног значаја за заштиту критичне инфраструктуре. У том контексту, актери који обезбеђују остваривање функције(а) корпоративне безбедности, заузимају значајно место и улогу.

Корпоративна безбедност као унутрашња безбедност организације успостављена је у циљу заштите, у овом случају свих система, мрежа, објеката или њихових делова који су одређени као критична инфраструктура. Правовремено уочавање раних сигнала који упозоравају на угрожавање, као и предузимање благовремених активности на спречавању и сузбијању последица угрожавања када до њих дође, кључна је намена корпоративне безбедности. Да би ово остварила, она мора објединити све функције, које, испуњавајући задатке за које су успостављене, доприносе остваривању те намене. Задатак је менаџмента и свих одговорних лица да обезбеде услове за усклађено и ефикасно остваривање свих функција корпоративне безбедности, јер, колико год се о њима може говорити као засебним елементима, оне се међусобно подржавају допуњујући једна другу.

Узимајући у обзир значај који национална критична инфраструктура има за Републику Србију и њене грађане, пажња која јој се посвећена у нормативним актима је врло оскудна. Предметни закон је усвојен тек 2018. године и од тада није редигован иако су наредне године усвојене стратегије у области одбране, војске и унутрашњих послова. Поред наведеног, на основу предметног закона донет је само један подзаконски акт иако се у стратегијама (заправо у Стратегији одбране) напомиње да ће посебна пажња бити посвећена потпуном спровођењу нормативно-правних решења (вероватно се алудира на решења која се односе на поједине сегменте критичне инфраструктуре), да ће се предузимати све превентивне, односно, проактивне мере (иако није јасно које су то „све" мере) и успоставити интегрисани информациони систем за безбедносни надзор објеката критичне инфраструктуре (за који нема увида).

На основу свега изнетог, издваја се потреба за свеобухватнијим сагледавањем улоге корпоративне безбедности у заштити критичне инфраструктуре и подстицањем дијалога о њеном доприносу, као и потреба да се овој проблематици посвети више пажње, како у нормативној сфери тако и на практичном нивоу. Уз то, у заштити критичне инфраструктуре од посебног је значаја успостављање и ефикасно спровођење претходно добро дефинисаног, вођеног и надгледаног јавно-приватног партнерства, па и оно мора бити саставни део ових дијалога и деловања.

Литература

1. *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről* (Закон о идентификацији, одређивању и заштити виталних система и објеката). Magyar Közlöny 2012. évi 154. sz. 26099. https://net.jogtar.hu/jogszabaly?docid=a1200166.tv., доступан 24. 2. 2023.
2. American Petroleum Institute. (2016). *API Recommended Practice 581 – Risk-Based Inspection Technology.*
3. Brooks, J. D. (2013). Corporate Security: Using Knowledge Construction to Define a Practising Body of Knowledge. Asian *Journal of Criminology,* 8(2): 89–101.
4. Brown, G., Carlyle, M., Salmerón, J., Wood, K. (2006). Defending critical infrastructure. *Interfaces*, 36(6): 530-544.
5. *Закон о безбједности критичних инфраструктура у Републици Српској*, Службени гласник Републике Србије, бр. 58/19.
6. *Zakon o kritičnim infrastrukturama*, Službeni list RH, NN 56/13, 114/22.
7. *Закон о критичној инфраструктури*, Службени гласник Републике Србије, бр. 87/2018-41.
8. *Zakon o određivanju i zaštiti kritične infrastrukture*, Službeni list CG, br. 72/2019.
9. *Закон о одбрани,* Службени гласник Републике Србије, бр. 116/2007-3, 88/2009-3, 88/2009-31 (др. закон), 104/2009-13 (др. закон), 10/2015-3, 36/2018-11.
10. *Закон о приватном обезбеђењу*, Службени гласник Републике Србије, бр. 104/2013-8, 42/2015-3, 87/2018-31.

11. Kovacich, L. G., Halibozek, P. E. (2003). *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth–Heinemann is an imprint of Elsevier Science, Burlington.
12. *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Official Journal of the European Union, L 345/2008, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114, доступан 24. 2. 2023.
13. LEGE nr. 225, MONITORUL OFICIAL nr. 677/18, https://legislatie.just.ro/Public/DetaliiDocument/203523, доступно 24. 2. 2023.
14. Мандић, Ј. Г. (2020). *Корпоративна безбедност – пословна функција организације*. У Зборник радова „Науке безбедности – врсте и облици", Факултет безбедности Универзитета у Београду, Београд, стр. 167-182.
15. Мандић, Ј. Г., и Станојевић, П. (2020). *Корпоративна безбедност*. Факултет безбедности Универзитета у Београду, Београд.
16. Марковић, Ј. (2021). *Континуитет пословања као функција корпоративне безбедности* (Мастер рад). Универзитет у Београду, Факултет безбедности.
17. Мићновић, Д. М. (2020). *Специфичности критичне инфраструктуре у Републици Србији*. Криминалистичко-полицијски Универзитет, Београд.
18. МУП РС. (2019). *Процена ризика од катастрофа у Републици Србији*. Министарство унутрашњих послова Републике Србије.
19. *Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях* (Уредба о реду, начину и надлежним органима за успостављање критичних инфраструктура и њихових објеката и процени ризика за њих). Приета с ПМС № 256 от 17.10.2012 г., Обн., ДВ, бр. 81/12, изм. и доп. ДВ. бр. 19/2013, изм. ДВ. бр. 27/16, https://www.lex.bg/index.php/mobile/ldoc/2135816878, доступан 24. 2. 2023.
20. *Одлука о објектима од посебног значаја за одбрану*, Службени гласник Републике Србије, бр. 112/2008-22.
21. *Одлука о одређивању великих техничких система од значаја за одбрану*, Службени гласник Републике Србије, бр. 41/2014-

3, 35/2015-22, 86/2016-6, 53/2017-51, 26/2019-11, 94/2019-83, 67/2021-36, 62/2022-4.

22. Ouyang, M. (2014). *Review on modeling and simulation of interdependent critical infrastructure systems*. Reliability engineering & System safety, 121: 43-60.
23. Rinaldi, S. M., Peerenboom, J. P., Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, 21(6): 11-25.
24. *Стратегија националне безбедности Републике Србије,* Службени гласник Републике Србије, бр. 94/2019.
25. *Стратегија одбране Републике Србије*, Службени гласник Републике Србије, бр. 94/2019-4.
26. *Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године*, Службени гласник Републике Србије, бр. 86/2021-5.
27. *Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије*, Службени гласник Републике Србије, бр. 69/2022.
28. Čabric, M. (2015). *Corporate security management: Challenges, risks, and strategies*. Butterworth-Heinemann is an imprint of Elsevier, Oxford.
29. Цигурски, О. (2018). *Системско-структурни приступ у анализи и решавању безбедносних проблема корпорација – системски концепт*. У Зборник радова „Корпоративна безбедност – хрестоматија", Факултет безбедности Универзитета у Београду, Београд, стр. 253-276.

The Role of Corporate Security in the Protection of the Critical Infrastructure of the Republic of Serbia

Abstract: *Critical infrastructure can be presented as an element of the state necessary for its functioning and at the same time a condition for performing basic functions and providing state services to its citizens. On the other hand, corporate security can be presented as a set of functions aimed at protecting all the values of the entity in which it (corporate security) is incorporated, from all threats, regardless of their origin, type and intensity, through proactive and/or reactive activities. The work is based on the idea that, in addition to the state and its authorities, corporate security significantly contributes to the protection of critical infrastructure, as a form of security established within all entities that manage systems, networks, facilities or their parts that are designated as critical infrastructure. After the analysis of the critical infrastructure sector in the Republic of Serbia and neighboring countries and the situation related to its protection in our country, as well as a brief review of the importance of corporate security for the state and its national security, the aim of the paper is to present the way in which corporate security, through its functions, ensures and contributes to the overall protection of critical infrastructure.*

Keywords: *critical infrastructure, critical infrastructure protection, corporate security, corporate security functions*