Fakultet za poslovne studije i pravo-Beograd
Univerzite „Union-Nikola Tesla“ u Beogradu

TEORIJSKI I NORMATIVNI OKVIR ZAŠTITE KRITIČNE INFRASTRUKTURE U CRNOJ GORI

Doktorska disertacija

KANDIDAT

MA Marjan D. Marjanović

MENTOR

prof. dr Milan Milošević

Beograd, 2020.

REZIME

Svjesna činjenice da efikasan sistem zaštite kritičnih infrastruktura stvara preduslove za normalno i nesmetano funkcionisanje šireg društvenog sistema, Crna Gora poslednjih godina ulaže značajne napore, kako u pogledu normativnog definisanja tog sektora, tako i na planu iznalaženja optimalnih mehanizama zaštite nacionalne kritične infrastrukture. Ove napore ne treba shvatiti isključivo kao reagovanje na savremene trendove u ovoj oblasti, već i kao nužnost, odnosno obavezu usklađivanja nacionalnog zakonodavstva i prakse sa pravnim tekovinama Evropske unije (Acquis communautaire) u procesu priključivanja Crne Gore EU. Sve to predstavlja i diskontinuitet sa ranijim stanjem u kome je nacionalna kritična infrastruktura posmatrana isključivo iz ugla oružanih snaga i potreba sistema odbrane države. U aktuelnim okolnostima, posebno se osjetljivim smatra spektar vitalnih sektora koje obuhvata kritična infrastruktura i čiji djelimičan ili potpun prekid rada može narušiti normalno funkcionisanje određenog sistema i ugroziti nacionalnu bezbjednost. S druge strane, od kritične infrastrukture Crne Gore očekuje se da pruža osnovne usluge koje podržavaju razvoj crnogorskog društva i održavaju način na koji život u njemu funkcioniše. U vezi sa tim, kao jedan od prvih zadataka se nameće definisanje sektora infrastrukture koji su od vitalnog značaja i kao takvi predstavljaju kritičnu infrastrukturu.

Bezbjednost sistema kritične infrastrukture i njihovih funkcija nije značajna samo za državne institucije, budući da se bezbjednosne dileme u pogledu zaštite kritične infrastrukture mogu pojaviti u i privatnom sektoru koji se pojavljuje kao partner u izvršavanju misija i zadataka u toj oblasti. U vezi sa tim, ilustrativni su primjeri pojedinih država u kojima se resursi kritične infrastrukture, s obzirom na njihove specifičnosti i razmjere štetnih posledica potencijalnih napada i ugrožavanja, u današnjem vremenu štitite primjenom integrisanog modela korporativne bezbjednosti, pri čemu se neke funkcije povjeravaju specijalizovanim provajderima usluga privatnog obezbjeđenja. Ovako zamišljeni integrisani model zaštite u objektima i sistemima kritične infrastrukture bi, nakon izdvajanja funkcija koje obavljaju pripadnici privatnih kompanija za obezbjeđenje angažovani po principu outsourcing-a, mogao obuhvatiti veliki broj aktivnosti i djelatnosti u cilju adekvatne zaštite kritične infrastrukture. Predmetni model je važan za Crnu Goru, jer delegitimiše tradicionalno shvatanje prema kojem samo država ima monopol nad poslovima bezbjednosti, dok privatne bezbjednosne kompanije, zbog svoje profitno orijentisane prirode, nijesu pogodne za partnera javnom bezbjednosnom sektoru. U vezi sa tim, treba imati u vidu da u pojedinim visokorazvijenim državama privatni sektor ima potpuni partnerski odnos sa javnim sektorom, ne samo u zaštiti kritične infrastrukture, već i u prevenciji kriminala, borbe protiv terorizma i slično.

Ključne riječi: *Crna Gora, kritična infrastruktura, kritična informaciona infrastruktura, javno-privatno partnerstvo, privatni sektor bezbjednosti, javni sektor*

SUMMARY

Aware of the fact that an effective system of critical infrastructure protection creates preconditions for the normal and undisturbed functioning of the wider social system, Montenegro has made significant efforts in recent years, both in terms of normative definition of that sector and in finding optimal mechanisms for protection of national critical infrastructure. These efforts should not be understood solely as responding to current trends in the field, but also as a necessity, that is, an obligation to align national legislation and practice with the acquis communautaire in the process of accession to this EU country. All this also represents a discontinuity with an earlier state in which national critical infrastructure was viewed solely from the perspective of the armed forces and the needs of the state's defense system. In the current circumstances, the spectrum of vital sectors covered by critical infrastructure and whose partial or total disruption of operations may impair the normal functioning of a particular system and endanger national security is particularly sensitive. On the other hand, the critical infrastructure of Montenegro is expected to provide basic services that support the development of Montenegrin society and maintain the way life in it functions. In this regard, one of the first tasks is to identify the infrastructure sectors that are vital and as such constitute critical infrastructure.

The security of critical infrastructure systems and their functions is not only relevant to state institutions, since security dilemmas regarding critical infrastructure protection may also arise in the private sector, which appears to be a partner in carrying out missions and tasks in the field. In this regard, there are illustrative examples of individual countries where critical infrastructure resources, given their specificities and the extent of the detrimental effects of potential attacks and threats, are nowadays protected by an integrated corporate security model, with some functions being entrusted to specialized service providers private security. This conceived integrated model of protection in critical infrastructure facilities and systems, following the outsourcing of functions outsourced by private security companies, could encompass a large number of activities and activities to adequately protect critical infrastructure. The model in question is important for Montenegro, as it delegitimizes the traditional notion that only the state has a monopoly on security, while private security companies are not suitable for partnering the public security sector because of its profit-oriented nature. In this regard, it should be borne in mind that in some highly developed countries, the private sector has a full partnership with the public sector not only in the protection of critical infrastructure, but also in the prevention of crime, the fight against terrorism and the like.

Keywords: *Montenegro, critical infrastructure, critical information infrastructure, public-private partnership, private security sector, public sector*

SADRŽAJ:

SADRŽAJ TABELE:

SADRŽAJ ŠEME I GRAFIKONI:

UVOD

Funkcionisanje svakodnevnog života u savremenom društvu zasniva se, između ostalog, i na visokorazvijenoj infrastrukturi, naročito u oblastima upravljanja i kontrole snabdijevanja energijom, osiguranja izvora pitke vode, transporta, održavanja sistema informacionih tehnologija, telekomunikacija i drugog. Procesi globalizacije i tehnološke revolucije učinili su infrastrukturne sisteme veoma složenim i međuzavisnim, ali u isto vrijeme i izuzetno značajnijim za savremeno društvo. U tom smislu, infrastruktura koja osigurava osnovne funkcije države, ima podjednak značaj kao infrastrukturni sistemi koji omogućavaju obezbjeđivanje roba i usluga stanovništvu. Istorijski razvoj koncepta kričične infrastrukture je ujedno i pratilac razvoja države i društva. U ranim fazama tehnološkog i društvenog razvoja kritičnu infrastrukturu su činili putevi, akvadukti, luke i brodovi pomoću kojih je vršen transport važnih materijalnih dobara. U savremenom dobu, kao odraz razvoja i sve razuđenijih potreba ljudskog društva, kritična infrastruktura postaje znatno složenija, ali i izloženija različitim oblicima ugrožavanja.

Pouzdana infrastruktura je od ključne važnosti ne samo za ekonomski razvoj, jer doprinosi efikasnom poslovanju kompanija i pružanju usluga, već i za unapređenje povjerenja građana i društva u državu i njene institucije. Iz tih razloga savremene države prioritetno investiraju u kritičnu infrastrukturu i nastoje da dođu do najadekvatnijih rešenja na planu zaštite tih objekata i resursa. Iako je evidentno da postoje različiti pristupi toj problematici, svim državama je jedan od primarnih ciljeva uspostavljanje održive, moderne i efikasne infrastrukture koja će biti u funkciji razvoja nacionalne ekonomije i društvenog prosperiteta. S obzirom na značaj kritične infrastrukture za nacionalnu bezbjednost i percepcije različitih prijetnji toj infrastrukturi, savremene države preduzimaju različite normativne, organizacione i druge mjere i aktivnosti kako bi se potencijalna ugrožavanja preduprijedila, a eventualno nastale posledice što prije otklonile.

Jedan od sve zastupljenijih savremenih modela u oblasti zaštite kritične infrastrukture podrazumijeva saradnju i partnerstvo države sa privatnim akterima. Taj model odražava i aktuelne globalne trendove prema kojima javni sektor bezbjednosti sve više prepušta poslove lične i imovinske sigurnosti u nadležnost subjekata privatnog sektora bezbjednosti. Bezbjednost i zaštita kritične infrastrukture jedno je od najpogodnijih područja za javno-privatna partnerstva, s obzirom na javni karakter i značaj te infrastrukture. U prednosti modela javno-privatnog partnerstva spada i to što na taj način javni i privatni sektor umnožavaju i dijele svoje resusrse u cilju racionalnog i efikasnog angažovanja u zaštiti kritične infrastrukture. Pomenuti model je izvorno bio šire zamišljen kao jedno od rešenja problema sve izraženije neefikasnosti javnog sektora. U okviru toga je krajem XX vijeka privatni sektor bezbjednosti promovisan u značajnog aktera i u oblasti zaštite kritične infrastrukture, uz očekivanja da će imati važnu ulogu u smanjenju ugroženosti vitalnih sistema na nove bezbjednosne prijetnje. Ipak, dosadašnja praksa pokazuje da se u tom domenu izdvajaju države koje imaju razvijenu tradiciju javno-privatnog partnerstva, za razliku od većine drugih kod kojih je primjena koncepta tek na početku.

Varijacije javno-privatnog partnerstva postoje i u vezi pristupa različitim sektorima kritične infrastrukture, ali se nastoji da bude ostvarena koherentna politika zaštite infrastrukture. Međutim, koncept javno-privatnog partnerstva u zaštiti kritične infrastrukture ne treba posmatrati isključivo kao prenos državnih obaveza na privatne aktere. Riječ je o saradnji koja, između ostalog, obuhvata i

objedinjavanje resursa, međusobnu podršku i zajedničko odlučivanje. Razlozi za uspostavljanje javno-privatnog partnerstva su brojni i vezani su kako za sve izraženiji osećaj nesigurnosti u različitim djelovima društva, tako i za ograničene resurse policije i drugih organa javne bezbjednosti, ali i za unaprijeđeni kvalitet u radu i profesionalizam pripadnika privatnih bezbjednosnih službi. U vezi sa tim, kao posebne odlike i preimućstva privatnih aktera ističu se inovativnost i fleksibilnost privatnog sektora bezbjednosti.

Pogrešno bi bilo zaključiti da se uspostavljanjem javno-privatnog partnerstva u zaštiti kritične infrastrukture istovremeno smanjuje i uloga države. Nesumnjivo je da država i dalje ima veoma značajnu ulogu u svim fazama realizacije koncepta javno-privatnog partnerstva. U okviru toga, država je u obavezi da definiše potrebe za pružanjem pomoći privatnog sektora u zaštiti kritične infrastrukture i da opredijeli oblik i obim željene saradnje, zadržavajući pritom kontrolnu funkciju u periodu trajanja javno-privatnog partnerstva. Pored toga, na državi je da svoje ključne ciljeve i očekivanja precizno formuliše u sopstvenim strateškim dokumentima, na način da se jasno odredi uloga aktera privatnog sektora u zaštiti kritične infrastrukture i da im se istovremeno predoče prednosti i neophodnost njihovog angažovanja u tom domenu.

PRVI DIO

TEORIJSKO METODOLOŠKI OKVIR ISTRAŽIVANJA

1. TEORIJSKE OSNOVE DOKTORSKE DISERTACIJE

Termin kritična infrastruktura je relativno novijeg datuma, a u naučnoj i stručnoj literaturi se intenzivnije koristi nakon terorističkih napada u SAD u septembru 2001. godine. Karakteristično je da u teoriji i dalje ne postoji potpuna saglasnost o sadržini tog pojma i koncepta, dok se pitanjima definisanja kritične infrastrukture u većoj mjeri od teoretičara bave strateški dokumenti nadležnih institucija nacionalnih država, odnosno organa nadnacionalnih organizacija poput OUN, Evropske unije, NATO i OEBS-a. To se odnosi i na države sa prostora bivše SFRJ, uključujući i Crnu Goru, kod kojih je uočljivo nastojanje da što preciznije identifikuju i definišu sopstvenu kritičnu infrastrukturu.

U Crnoj Gori do sada praktično nije bilo naučnih radova na temu kritične infrastrukture i njene zaštite, izuzimajući par teorijskih članaka (Milan Bigović i Ana Rakočević u tematskom zborniku Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection iz 2014. godine), a u znatnoj mjeri je slična i situacija u Republici Srbiji i ostalim državama Zapadnog Balkana. Na primjer, u Srbiji se ne može govoriti o reprezentativnim naučnim radovima koji se isključivo bave temom kritične infrastrukture, već se uglavnom radi o stručnim člancima (Vladimir Jakovljević, Jasmina Gačić, Proda Šećerov, Želimir Kešetović, Mirko Škero, Vladimir Ateljević, Marija Mićović, Dragana Macura, Nebojša Bojović i drugi) ili o monografijama koje se primarno bave pitanjima upravljanja rizicima, vanrednih situacija, kriznog menadžmenta, privatne i korporativne bezbjednosti i slično, a čiji se autori (Vladimir Jakovljević, Ljubomir Stajić, Vladimir Cvetković, Zoran Keković, Želimir Kešetović, Dragan Mlađan, Dragan Trivan, Goran Mandić i drugi) u njima usput dotiču i problematike kritične infrastrukture. Ozbiljnija teorijska istraživanja o kritičnoj infrastrukturi su u proteklom periodu vršena u zemljama sa prostora bivše SFRJ koje su u međuvremenu postale članice Evropske unije i samim tim bile u obavezi da usvoje standarde EU u toj oblasti – Republici Hrvatskoj (monografije Davora Čemerina, Siniše Tatalovića, Damira Kulišića, Darija Matike) i Republici Sloveniji (naučni radovi Denisa Čalete, Mirana Vršeca, Milana Tarmana, Vita Murgela).

Različiti teorijski pristupi temi kritične infrastrukture su prisutni kod brojnih stranih autora, kao što su Charles Perrow, Urlich Beck, Brian P. Bennett, Robert Radvanovsky, Arnulf Grübler, Christer Pursainen, Elgin M. Brunner, Manuel Suter, Andreas Wenger, Victor Mauer, Isabelle Wigert, Myriam Dunn Cavelty, Hilde de Clerck, John Moteff, Paul Parfomak, Lewis Branscomb, Erwan Michel-Kerjan i niz drugih. Činjenica je, međutim, da do sada nije bilo domaćih i stranih naučnih radova koji se specifično bave pitanjima kritične infrastrukture u Crnoj Gori.

Kada je riječ o javno-privatnom partnerstvu, kao vidu saradnje između javnog i privatnog sektora koja ima za cilj obezbjeđenje finansiranja, izgradnje, obnavljanja i upravljanja infrastrukturnim objektima i sektorom usluga, odnosno finansiranje projekata i usluga koje tradicionalno obezbjeđuje javni sektor, u pitanju je model koji je u praksi prvi put primijenjen početkom 90-ih godina u Velikoj Britaniji. S obzirom da se Crna Gora još uvijek nalazi u

tranzicionom periodu u okviru koga se državne strukture usklađuju i prilagođavaju zahtjevima koji proizilaze iz članstva u NATO-u i potencijalnog članstva u Evropskoj uniji, u toku je proces reformi i transformacije cjelokupnog društva, koji podrazumijeva i usklađivanje kompletnog zakonodavstva sa pravom EU, a samim tim i zakonskih normi u oblasti javno-privatnog partnerstva. Inače, javno-privatno partnerstvo u Crnoj Gori je regulisano Zakonom o učešću privatnog sektora u vršenju javnih usluga, donijetim još 2002. godine, te Zakonom o koncesijama iz 2009. godine. Ovi zakonski akti ne predviđaju mogućnost uvođenja javno-privatnog partnerstva u područje kritične infrastrukture.

U Crnoj Gori je objavljeno svega nekoliko naučnih i stručnih radova koji se uopšteno bave tematikom javno-privatnog partnerstva ili nekim aspektima primjene tog modela, uključujući monografiju Jovane Marović Lokalne samouprave i javno-privatno partnerstvo iz 2014. godine, Javno-privatna partnerstva u Crnoj Gori grupe autora iz 2013. godine, zbornik Javno-privatna partnerstva u Crnoj Gori – transparentnost, efikasnost i odgovornost iz 2010. godine, te rad Ivana Boškovića Analiza Predloga Zakona o javno-privatnom partnerstvu iz 2018. godine. Slično je i stanje u Republici Srbiji, gdje se od značajnijih teorijsko-stručnih radova na ovu temu mogu pomenuti Javno-privatno partnerstvo – Priručnik za sprovođenje na lokalnom nivou autora Predraga Cvetkovića i Slađane Sredojević iz 2013. godine, te zbornici Partnerstvo javnog i privatnog sektora – dobra i loša iskustva u odabranim zemljama u tranziciji iz 2013. godine i Razvoj lokalne infrastrukture kroz javno-privatno partnerstvo – Priručnik za lokalne vlasti iz 2012. godine. Različitim aspektima ove problematike se bave i brojni strani autori, pretežno sa anglosaksonskog područja, kao što su Gordon Rausser, Leslie Kellerman, Matthias Beck, Susan Robertson, Karen Mundy, Jeffrey Delmon, Albert N. Link, Albert P. Chan, Piet de Vries, Darin Grimsey, Sidney M. Levy, Ronald D. Fischer, Oliver V. Porter, Gregory C. Shaffer i niz drugih.

Imajući u vidu iznijeto, nameće se opšti zaključak da teme kritične infrastrukture i javno-privatnog partnerstva u Crnoj Gori i drugim zemljama sa prostora Zapadnog Balkana do sada nisu sistematski naučno obrađivane. To se u još većoj mjeri odnosi na ulogu javno-privatnog partnerstva u zaštiti objekata i resursa kritične infrastrukture. S obzirom na načelna opredjeljenja Crne Gore za uvođenje tog modela, uz odsustvo adekvatne zakonske regulative, postoje jasni razlozi da se ova oblast podrobnije teorijski analizira i osvijetli.

2. PREDMET ISTRAŽIVANJA

Savremene društvene okolnosti i trendovi učinili su bezbjednosnu problematiku još složenijom, prvenstveno u pogledu raznovrsnosti i intenziteta pojava ugrožavanja bezbjednosti. Složenost oblika ugrožavanja bezbjednosti, u cilju adekvatnog odgovora, iziskuje i posebne bezbjednosne mjere. Svjedoci smo sve učestalijih prirodnih katastrofa i akcidenata uzrokovanih djelovanjem čovjeka, sa teškim posledicama za ljude, imovinu i životnu sredinu u cjelini. S druge strane, uočljiv je trend povećanja zavisnosti savremenog društva od raspoloživosti ključnih prirodnih i materijalnih dobara, te nesmetanog funkcionisanja energetskih, tehničkih i komunikacionih sistema, infrastrukturnih objekata, djelatnosti i službi, koje su od posebnog značaja za državu i čije bi uništenje ili prekid u radu ugrozili nacionalnu bezbjednost, nacionalnu ekonomiju, vitalne društvene funkcije, zdravlje stanovništva, javni poredak i zaštitu nacionalnih interesa. Imajući to u vidu, kao jedan od

primarnih i najvažnijih bezbjednosnih izazova savremenog doba nameće se potreba adekvatne i efikasne zaštite kritičnih infrastruktura.

Sintagma kritična infrastruktura preuzeta je iz vojne terminologije, a njome se označavalo sve što je neophodno za funkcionisanje vojnog sistema tokom vojnih sukoba kada su resursi usmjeravani na čuvanje objekata, sistema i mreža, kao i za onesposobljavanje istih na protivničkoj strani. Kada se radi o civilnom sistemu kritične infrastrukture, svaka država posebno definiše to područje, što upućuje na nepostojanje jedinstvenog određenja. Uobičajeno je da se na nacionalnom nivou određuju kritična područja, odnosno sektori po kojima je raspoređena kritična infrastruktura, pri čemu im se mijenja hijerarhijska pozicija prema nivou važnosti i značaju. Neposredno nakon terorističkog napada u SAD od 11. septembra 2001. godine, kritična infrastruktura postaje suštinski dio nacionalne bezbjednosti, a njena zaštita predstavlja jedan od prioriteta svake države. To je primoralo mnoge zemlje da osmisle različite sisteme odbrane od neželjenih događaja. Da bi jedan takav sistem funkcionisao i ostvario potrebnu efikasnost potrebno je prethodno definisati prioritete koje treba braniti, odnosno utvrditi šta je to bez čega društvo u cjelini ne može funkcionisati. S druge strane treba imati u vidu da države imaju različite resurse i sisteme koji utiču na njihovo funkcionisanje, te da svaka država nacionalnim propisima utvrđuje liste sopstvene kritične infrastrukture i modalitete njene zaštite.

Na nivou Evropske unije prisutno je nastojanje da se obezbijedi adekvatan i ujednačen nivo sigurnosti resursa odabrane kritične infrastrukture, što je u praksi sprovodljivo samo na osnovu zajedničkog evropskog normativnog okvira za njenu zaštitu. Fokusiranje institucija Unije na kritičnu infrastrukturu država članica je razumljivo zbog rizika da bi uništenje ili oštećenje određene kritične infrastrukture u jednoj zemlji članici moglo direktno ugroziti i druge države članice. Shodno standardima EU, u kritičnu infrastrukturu spadaju proizvodnja i prenos električne energije, hemijska industrija i nuklearna postrojenja, proizvodnja, transport i distribucija nafte i prirodnog gasa, telekomunikacioni sistemi, izvorišta pitke vode, proizvodnja životnih namirnica, sistemi grijanja, objekti i službe javnog zdravlja, sistemi javnog transporta, organi državne vlasti, finansijske i bezbjednosne ustanove. U tom kontekstu, a saglasno direktivi Evropske komisije – EU COM (2006) 786 final, Evropska unija je donijela Evropski program zaštite ključne infrastrukture, u kome je sadržana i Evropska lista ključne infrastrukture (ECI), sačinjena na osnovu prethodno dostavljenih predloga zemalja članica. U vezi sa tim, Unija definiše Evropsku kritičnu infrastrukturu koja se sastoji od resursa, službi, uređaja informacione tehnologije, sigurnosti mreža i infrastrukture, te bezbjednosne, ekonomske ili socijalne dobrobiti dvije ili više zemalja članica.

Crna Gora kao članica NATO-a i kandidat za članstvo u Evropskoj uniji neminovno mora pristupiti sprovođenju sistemskih mjera u cilju potpunog regulisanja zaštite kritične infrastrukture. Promjena društveno-političkih odnosa u pravcu uspostavljanja tržišne ekonomije, te sve prisutnije privatno vlasništvo u kompanijama koje upravljaju kritičnom infrastrukturom, samo su neki od faktora koji presudno utiču na percepciju promjena koje su nastupile i u ovoj oblasti. I pored toga, nema dileme da je država i dalje najvažniji subjekt u izgradnji i osiguranju efikasnog funkcionisanja sistema kritične infrastrukture. Država ima i najveći interes da kritična infrastruktura, bez obzira na vlasničku strukturu kompanija, neprekidno i nesmetano funkcioniše radi zadovoljavanja vitalnih potreba zajednice u svim okolnostima. Zbog toga država svojim regulatornim mjerama, te mjerama kontrole i stalnog nadzora, mora da ostvaruje svoj uticaj u cilju izgradnje adekvatnog sistema zaštite kritične infrastrukture i njegovog dovođenja do potrebnog nivoa funkcionisanja.

Sa aspekta zaštite kritične infrastrukture, za Crnu Goru je karakteristično da ta oblast još uvijek zakonski nije uređena. Iz toga proističe da je prvi neophodan korak donošenje Zakona o zaštiti kritične infrastrukture, kojim bi se uspostavio normativni okvir za definisanje i identifikaciju resursa u toj oblasti i definisale nadležnosti i odgovornost organa i organizacija, kao i nadzor u oblasti kritične infrastrukture. Nakon donošenja Zakona, naredni korak bi bio donošenje i usvajanje podzakonskih akata u cilju obezbjeđenja praktičnih rešenja i kriterijuma za identifikaciju kritične infrastrukture i sektora kritične infrastrukture. U procesu normativnog uređenja problematike kritične infrastrukture Crne Gore, potrebno je usklađivanje predmetnog zakona sa srodnim važećim zakonskim propisima. U vezi sa tim polaznu osnovu mogu predstavljati normativna rešenja iz oblasti sistema odbrane, budući da su njima obuhvaćeni određeni tehničko-tehnološki sistemi koji imaju poseban značaj za odbranu, kao i oni objekti u kojima se proizvodi, skladište ili čuvaju predmeti ili vrše usluge za potrebe odbrane. Pored navedenih tu su i oni objekti u kojima se nalaze državni organi i pravna lica od naročitog značaja za odbranu države, kao i određeni infrastrukturni objekti.

S druge strane, zalaganje za dogradnju koncepta javno-privatnog partnerstva kako bi se omogućila primjena tog modela u zaštiti kritične infrastrukture Crne Gore, zahtijeva i odgovarajuće usklađivanje zakona i propisa iz ove oblasti, prije svega donošenje Zakona o javno-privatnom partnerstvu. Naime, aktuelne zakonske odredbe iz ove oblasti, uz ostalo, ne prepoznaju mogućnost angažovanja privatnih bezbjednosnih kompanija u zaštiti kritične infrastrukture po modelu javno-privatnog partnerstva. Takođe, potrebno je precizirati i dopuniti zakonske odredbe o privatnoj bezbjednosti (Zakon o zaštiti lica i imovine), kako bi se eksplicitno omogućilo angažovanje privatnih bezbjednosnih kompanija na zadacima zaštite kritične infrastrukture. U vezi sa tim, od posebne je važnosti definisanje uslova koje moraju da ispune privatne bezbjednosne kompanije koje treba da budu angažovane na poslovima zaštite kritične infrastrukture. Usklađivanje zakonodavnog okvira podrazumijeva i druge zakone (Zakon o unutrašnjim poslovima, Zakon o zaštiti i spasavanju, Zakon o komunalnoj policiji, Zakon o oružju, Zakon o učešću privatnog sektora u vršenju javnih usluga i drugi), kao i strateška dokumenta (Strategija nacionalne bezbjednosti, Strategija sajber bezbjednosti, Strategija razvoja saobraćaja, Strategija razvoja energetike, Strategija upravljanja vodama i druge), u smislu da u njima na direktan ili indirektan način i u određenom obimu mora biti obuhvaćena problematika kritične infrastrukture.

Pored toga, u Crnoj Gori egzistira i čitav niz sektorskih zakona u oblasti odbrane, tajnosti podataka, bezbjednosti hrane, prostornog planiranja, zaštite od požara, zaštite životne sredine i drugih područja, koji ne pominju decidno termin kritične infrastrukture, ali tretiraju pojedine segmente kritične infrastrukture kao polaznu osnovu. To je od posebnog značaja za njihovo usklađivanje sa budućim Zakonom o zaštiti kritične infrastrukture, a u cilju potpunog normativnog uređenja ove oblasti. U procesu izgradnje adekvatnog sistema zaštite kritične infrastrukture Crne Gore izražena su zalaganja za primjenu koncepta javno-privatnog partnerstva, koji se implementira u pojedinim razvijenim državama. U vezi sa tim, procjenjuje se da primenljiv i efikasan model javno-privatnog partnerstva može predstavljati adekvatnu osnovu uspješnog funkcionisanja sistema zaštite kritične infrastrukture u Crnoj Gori. Sam koncept javno-privatnog partnerstva može se različito tumačiti, a u bezbjednosnom smislu predstavlja odraz prenosa državnih funkcija na privatni sektor u različitim poljima državne aktivnosti, uključujući i one u kojima je nacionalna država ranije držala monopol, što je slučaj upravo u zaštiti kritične infrastrukture. Uopšteno posmatrano, u teoriji se kao glavni

faktori privatizacije bezbjednosti obično navode smanjenje javne potrošnje i outsourcing usluga privatnom sektoru, tzv. marketizacija javne uprave, kao i drugi faktori koji su nastali kao posledica završetka Hladnog rata, uključujući smanjenje broja pripadnika u vojsci, policiji i službama bezbjednosti.

U većini razvijenih država svijeta kritična infrastruktura je pretežno u privatnom vlasništvu. U Crnoj Gori i državama u okruženju to za sada nije slučaj, ali se realno može očekivati veće učešće privatnog sektora u ovoj oblasti, s obzirom na globalne trendove liberalizacije tržišta. Javno-privatno partnerstvo se upravo i zasniva na primjeni koristi koje javni i privatni sektor mogu imati od udruživanja sredstava i znanja, a u cilju ispunjenja i (ili) poboljšanja sveukupne bezbjednosti države i ostvarenja potreba društva u cjelini. Zajedničko udruživanje znanja, sredstva i prednosti oba sektora, usklađivanje društvene i javne odgovornosti, efikasno upravljanje, te veće finansijske mogućnosti i „preduzetnički duh“ koji je svojstven privatnom sektoru, mogu doprinijeti ostvarivanju kvalitetnije i efikasnije zaštite kritične infrastrukture. U cilju zajedničkog djelovanja u različitim situacijama ugrožavanja kritične infrastrukture, nameće se i potreba uspostavljanja odgovarajućeg oblika obaveznih zajedničkih struktura (npr. Centar za koordinaciju i zaštitu kritične infrastrukture). U vezi sa tim, od posebnog je značaja da svaki partner u potpunosti ima jasno definisanu ulogu i odgovornost. To posebno dolazi do izražaja kada se uzme u obzir da partnerstvo između javnog i privatnog sektora na polju obezbjeđenja i zaštite kritične infrastrukture sada nije dovoljno razvijeno i ne koristi se kako bi se dostigao njegov maksimalni potencijal.

Angažovanje subjekata privatnog sektora bezbjednosti na poslovima zaštite kritične infrastrukture sprovodi se kroz postupak javnih nabavki, zbog čega je od posebnog značaja da subjekti privatnog obezbjeđenja i zaštite poseduju potrebni nivo kompetentnosti za ovu vrstu poslova. Iz tih razloga, pri opredjeljivanju za usluge privatnih bezbjednosnih kompanija osnovni kriterijum ne bi trebala da bude najniža ponuđena cijena, jer takav pristup u postupku javnih nabavki negativno utiče na kvalitet usluga angažovanih subjekata privatnog sektora bezbjednosti. To može imati ozbiljne posledice na stanje zaštite objekata i resursa kritične infrastrukture. Zato je posebno značajno da privatne bezbjednosne kompanije dostignu određene standarde u pogledu nivoa kvaliteta usluga, obučenosti kadra i opreme koju posjeduju kao osnovnog preduslova za angažovanje na zaštiti kritične infrastrukture. Na osnovu svega navedenog, možemo zaključiti da predmet ovog istraživanja predstavlja iznalaženje optimalnog modela javno-privatnog partnerstva u zaštiti kritične infrastrukture Crne Gore.

3. CILJEVI ISTRAŽIVANJA

Osnovni cilj ovog istraživanja odnosi se na istraživanje mogućnosti primjene koncepta javno-privatnog partnerstva u zaštiti kritične infrastrukture Crne Gore. Rezultati istraživanja treba jasno da ukažu na pravce kojima se treba rukovoditi pri uspostavljanju savremenog sistema zaštite kritične infrastrukture u Crnoj Gori.

3.1. Naučni ciljevi istraživanja

U najširem smislu naučni cilj istraživanja je sistematizacija naučnih saznanja iz oblasti bezbjednosnog menadžmenta u funkciji nacionalne bezbjednosti. U skladu sa definisanim predmetom istraživanja, osnovni naučni ciljevi koji istraživanjem treba ostvariti su naučna deskripcija, naučna klasifikacija i naučno objašnjenje sa elementima naučnog predviđanja.

Naučna deskripcija je prvenstveno vezana za razmatranja o javno-privatnom partnerstvu. U vezi sa tim u radu će biti razmatrana pitanja vezana za angažovanje privatnog sektora kroz koncept javno-privatnog partnerstva u zaštiti kritične infrastrukture Crne Gore. Pored toga, naučna deskripcija biće predstavljena i kroz istorijski prikaz razvoja javno-privatnog partnerstva kao i njegovog korišćenja u zaštiti kritične infrastrukture pojedinih država.

Naučna klasifikacija biće višestruko zastupljena u radu, pri čemu se njen najvažniji segment odnosi na klasifikaciju kritične infrastrukture Crne Gore, kroz razvrstavanje objekata i resursa prema značaju i sadržaju djelatnosti koje su od posebne važnosti za nesmetano funkcionisanje države i društva u cjelini. Pored toga, naučna klasifikacija će doći do izražaja i prilikom teorijskog razmatranja koncepta javno-privatnog partnerstva kroz njegove različite oblike koji se u svijetu primjenjuju u savremeno doba.

Naučno objašnjenje će se ostvariti kroz eksplikaciju uzročno-posledične veze između funkcionisanja kritične infrastrukture i zadovoljavanja potreba društva u cjelini, pri čemu će posebno biti analizirane i objašnjene međusobne veze između kritične infrastrukture i države, sa aspekta savremenih formi ugrožavanja bezbjednosti.

3.2. Društveni ciljevi istraživanja

U najširem značenju predmetno istraživanje je od posebnog značaja za institucije u okviru sistema nacionalne bezbjednosti Crne Gore koje su na direktan ili posredan način povezane sa funkcionisanjem kritične infrastrukture u zemlji. Naučna saznanja do kojih se bude došlo tokom istraživanja mogu biti značajna za donosioce političkih odluka i državne institucije koje se bave problemima zaštite kritične infrastrukture i implementacijom koncepta javno-privatnog partnerstva. Jedan od ciljeva istraživanja je i potpunije, realnije i objektivnije sagledanje postojećeg funkcionalnog i organizacionog aspekta zaštite kritične infrastrukture u Crnoj Gori. Pored toga, pomenuta saznanja treba da ukažu na pravce redefinisanja i osavremenjivanja načina zaštite kritične infrastrukture upotrebom koncepta javno-privatnog partnerstva. U vezi sa tim, društveni cilj ovog istraživanja jeste da se na osnovu teorijskih saznanja i empirijskih rezultata uspostavi adekvatan i efikasan model zaštite kritične infrastrukture Crne Gore. U radu će biti predložena i određena praktična rešenja u cilju dogradnje sistema zaštite i funkcionisanja kritične infrastrukture u Crnoj Gori uz uvažavanje realnih potreba i mogućnosti.

4. HIPOTETIČKI OKVIR ISTRAŽIVANJA

Generalna hipoteza
Uvođenje koncepta javno privatnog partnerstva u zaštiti kritične infrastrukture Crne Gore podrazumijeva prilagođavanje postojeće zakonske regulative.

Prva posebna hipoteza
U Crnoj Gori oblast kritične infrastrukture nije zakonom uređena.

Druga posebna hipoteza
Aktuelni zakonski okvir nije adekvatan modelu javno privatnog partnerstva u zaštiti kritične infrastrukture za kojim Crna Gora teži.

Treća posebna hipoteza
Model učešća javno privatnog partnerstva u zaštiti kritične infrastrukture podrazumijeva i implementaciju dobre prakse kakva postoji u pojedinim razvijem državama.

5. METODOLOGIJA ISTRAŽIVANJA

Na osnovu problema i predmeta, nedvosmisleno se nameće multimetodski pristup istraživanja koji zahtijeva komplementarnu analizu dostupnih izvora podataka. Predmetno istraživanje po svom karakteru predstavlja kombinaciju teorijsko- empirijskog postupka. U vezi sa tim, u istraživanju su primijenjene metode analiza sadržaja, istorijska metoda, komparativna metoda, statistička metoda, metoda modelovanja i metoda ispitivanja.

Metoda analize sadržaja primijenjena je prilikom proučavanja domaće i strane literature i istraživačkih iskustava: naučno-stručnih časopisa, stručnih knjiga, monografija, studija, kao i normativno-pravnih akata, dostupnih službenih dokumenata, izveštaja i analiza. U oviru metode analize sadržaja zastupljena je i pravno-dogmatska i normativna metoda u cilju naučne obrade normativnih sadržaja. Upotrebom ove metode analizirani se domaći i, uporedno, međunarodni pozitivnopravni propisi kojima se uređuju pitanja javno-privatnog partnerstva, kritične infrastrukture i druge srodne oblasti. U vezi sa tim, posebno su analizirana normativna akta koja se odnose kako na nacionalno, tako i na inostrana zakonodavstva u kojima je koncept javno-privatnog partnerstva razvijen, kao i relevantni propisi na nivou Evropske unije.

Istorijska metoda je neophodna kako bi se dobila „istorijska pozadina“ istraživanog problema i kako bi se na osnovu proučavanih iskustava u prošlosti pronašla perspektiva budućih rešenja. Ova metoda je posebno zastupljena u istraživanja istorijata javno privatnog partnerstva, kao i promjena u obimu i sadržaju kritične infrastrukture i slično.

Komparativna metoda i njena primjena omogućavaju uporednu analizu postojećeg stanja kritične infrastrukture kao i primjene koncepta javno privatnog partnerstva u njenoj zaštiti. Ova metoda je omogućila izvođenje poređenja postojećeg modela sa željenim rešenjima koja pozitivno utiču na cjelokupan aspekt zaštite kritične infrastrukture. Primjenom komparativne metode u ovoj

disertaciji identifikovane su razlike i sličnosti među određenjima najvažnijih pojmova, primjene modela javno- privatnog partnerstva, načinima zaštite kritične infrastrukture i slično.

Statistička metoda koristiti se u postupku prikupljanja, klasifikacije i statističke obrade dobijenih rezultata. Statistička metoda pomaže u definisanju trajanja i rasprostiranja konkretne pojave koje su predmet ovog istraživanja. Ova metoda je u stalnom prožimanju (sprezi) sa metodom modelovanja, koja zajedno sa statističkom metodom ima svoje mjesto u ovoj doktorskoj disertaciji. Statistička metoda primjenjuje se u obradi određenih činilaca kritične infrastrukture, kao što su ekonomski, demografski, energetski faktori i slično.

Metoda modelovanja omogućila je da napravimo jedan realan model koji predstavlja odraz ili projekciju određenog dijela društvene realnosti. Jedan razrađeni realan, statički model predstavlja stanje u samo jednom trenutku, koje se može razlikovati od stanja u svim drugim momentima, što u određenom smislu predstavlja ograničenje u donošenju nekog opšteg zaključka o predmetnoj pojavi. Ova metoda se posebno primjenjuje u posebnom dijelu rada u izradi predloga modela korišćenja javno privatnog partnerstva u zaštiti kritične infrastrukture Crne Gore.

Metoda ispitivanja koristi se za realizaciju empirijskog istraživanja, uz primjenu anketnog upitnika. Anketiranje je tehnika koja omogućava da se saznaju značajne činjenice koje se odnose na mogućnost angažovanja privatnog sektora u zaštiti kritične infrastrukture kao i na aktuelno stanje u ovoj oblasti. Anketiranje je sprovedeno u cilju prikupljanja podataka, a prema unaprijed pripremljenim pitanjima formulisana za ovo istraživanje. Predmetnim anketiranjem obuhvaćena su lica iz struke, odgovorna lica, rukovodioci i drugi koji su u neposrednom odnosu sa kritičnom infrastrukturom Crne Gore, i to iz: Sektora za vanredne situacije MUP CG, JP Elektroprivrede Crne Gore, JP Crnogorskog elektroprenosnog sistema, AD Pošte Crne Gore, Luke Bar i Kotor, HE Perućice, Pive, TE Pljevlje, privatnih bezbjednosnih kompanija u Crnoj Gori i drugih pravnih lica.

6. NAUČNI I DRUŠTVENI DOPRINOS DISERTACIJE

Naučna i društvena opravdanost ovog istraživanja priozilazi iz ciljeva koji se žele postići ovim istraživanjem, a koji se ogledaju u proširivanju saznanja o svim pitanjima vezanim za predmet istraživanja i implementiranju tih saznanja u teorijski fond nauka bezbjednosti.

6.1. Naučni doprinos

Naučna opravdanost istraživanja mogućnosti primjene koncepta javno-privatnog partnerstva u zaštiti objekata, institucija, sistema i mreža od značaja za ukupnu bezbjednost i zadovoljavanje vitalnih interesa društvene zajednice i naučni doprinos disertacije proizilaze iz definisanih ciljeva ovog rada koji se nastoje ostvariti implementacijom adekvatnog metodološkog okvira i opredijeljenog načina istraživanja, uz eksploataciju raspoloživih izvora podataka. Naučni doprinos disertacije se ogleda, prije svega, u činjenici da je u Crnoj Gori, Republici Srbiji i drugim zemljama zapadnog Balkana do sada bilo veoma malo naučnih radova koji se na sistematičniji način bave pitanjima bezbjednosti kritične infrastrukture, a da ni problematika javno-privatnog partnerstva i primjena tog koncepta i modela u zaštiti kritične infrastrukture nije u dovoljnoj mjeri istražena, niti teorijski produbljena.

O naučnoj opravdanosti istraživanja svjedoči i to što u teoriji i dalje nema potpuno usaglašene definicije pojma i koncepta kritične infrastrukture i njene zaštite, pri čemu se tim pitanjima u većoj mjeri od naučnih radova bave dokumenti različitih institucija na nacionalnom, regionalnom i međunarodnom nivou. Takođe, i istraživanja koja se tiču javno-privatnog partnerstva tek u novije vrijeme prelaze okvire zemalja u kojima je taj koncept nastao i gdje je razvijen, prije svega Velike Britanije i SAD. Sprovođenjem teorijskog i empirijskog istraživanja u okviru rada na doktorskoj disertaciji došlo bi se do pomaka u promišljanju i zasnivanju korpusa teorijskog saznanja o kritičnoj infrastrukturi i njenoj zaštiti kroz primjenu modela javno-privatnog partnerstva.

Opravdanost istraživanja i naučni doprinos disertacije su prije svega vezani za pojmovno određivanje, klasifikaciju i sistematizaciju postojećih naučnih saznanja koja se odnose na kritičnu infrastrukturu, njenu ulogu i značaj za ostvarivanje vitalnih društvenih potreba i funkcionisanje društva i države u cjelini, izvore i oblike ugrožavanja resursa te infrastrukture, pojmovno određenje koncepta i osnovnih principa javno-privatnog partnerstva, te na model javno-privatnog partnerstva u zaštiti kritične infrastrukture. Polazni naučni doprinos ovog istraživanja je naučna deskripcija navedenih fenomena.

Naučna klasifikacija ključnih pojmova iz pomenutih oblasti u okviru klasifikacionih klasa, postignuta je primjenom odgovarajuće metodologije u postupku istraživanja, takođe predstavlja naučni doprinos doktorske disertacije. Analizom i objašnjavanjem odnosa i veza između javnog i privatnog sektora kako u području bezbjednosti, tako i uopšte, gdje postoji sve veća povezanost i isprepletanost u modernom dobu, postignuto je naučno saznanje na nivou naučnog objašnjenja.

Kroz postupak verifikacije postavljenih hipoteza, odnosno njihovog odbacivanja na osnovu rezultata sprovedenog istraživanja, doktorska disertacija predstavlja naučni doprinos razjašnjavanju nepotpunih i nedovoljno dostupnih naučnih saznanja i proširenju fonda naučnog znanja u područjima vezanih za bezbjednosne nauke, međunarodno, krivično i kompanijsko pravo, državnu upravu, ekologiju, te nauku o međunarodnim odnosima. Dobijeni rezultati su ujedno podsticaj daljim, produbljenijim istraživanjima vezanim za javno-privatno partnerstvo i zaštitu kritične infrastrukture.

6.2. Društveni doprinos

Društveni doprinos istraživanja ogleda se u činjenici da Crna Gora u dosadašnjem periodu nije uspostavila adekvatan sistem zaštite kritične infrastrukture, koji bi bio na tragu rešenja zastupljenih u razvijenim zapadnim državama. Pri tome treba uzeti u obzir i političku orijentaciju zemlje za pristupanje u članstvo Evropske unije, samim tim i obavezu usklađivanja nacionalnog zakonodavstva u procesu pristupnih pregovora, što umnogome određuje i buduću normativu i praksu u oblasti kritične infrastrukture. Kao i druge države u okruženju i Crna Gora je suočena sa nizom najrazličitijih prijetnji koje mogu ugroziti funkcionisanje države i društva u cjelini. Iz navedenih i drugih razloga, uspostavljanje institucionalnog i normativnog okvira u oblasti zaštite kritičnih infrastruktura je od primarnog značaja za funkcionisanje lokalnih zajednica, države i društva. Pozitivna (kao i negativna) iskustva pojedinih zemalja, uz potrebno prilagođavanje uslovima i specifičnostima Crne Gore, značajno bi pomogli da se otklone uočeni nedostaci, što ujedno predstavlja više nego dovoljan razlog za društvenu opravdanost predmetnog istraživanja. Pored toga, realno je očekivati da će rezultati ovog istraživanja imati uticaj na proširenje istraživačke prakse radi

svestranijeg i sveobuhvatnijeg sagledavanja problema zaštite kritične infrastrukture u teoriji i praksi. Društveni doprinos istraživanja može se sagledati i u stvaranju objektivne slike stanja u ovoj oblasti, ali i kroz predlog modela zajedničke saradnje javnog i privatnog sektora u zaštiti kritične infrastrukture Crne Gore. Predmetni model je isključivo u funkciji stvaranja savremenog i održivog sistema funkcionisanja kritične infrastrukture, koji će u organizacionom i funkcionalnom smislu obezbijediti maksimalnu koordinisanost svih subjekata i poboljšati efikasnost u prevenciji različitih oblika ugrožavanja.

DRUGI DIO

KRITIČNA INFRASTRUKTURA

Koncept „kritične infrastrukture“ star je koliko i ljudska civilizacija. U starom Rimu, kritičnu infrastrukturu činili su uglavnom putevi i akvadukti. Putevi su bili vojni i omogućavali su veoma brz transport vojnika i vojne opreme u ugrožene provincije Rimskog carstva. Akvadukti su obezbjeđivali pitku vodu stanovništvu, što nije bilo samo veoma inovativno tehnološko rešenje, već i pitanje života, zdravlja i sanitarnih potreba. U staroj Kini, kritičnu infrastrukturu je predstavljao zid koji je pružao zaštitu od spoljnih neprijatelja i olakšavao ekonomski, vojni i kulturni razvoj. Kritičnu infrastrukturu u kolonijalnoj sili Španiji predstavljali su rudnici zlata u Južnoj Americi, kao i luke i flota koja je transportovala ovaj dragocjeni metal u zemlju. Danas je pojam kritične infrastrukture znatno širi, prvenstveno zbog tehnološkog napretka, ali je i pored toga značaj mnogih klasičnih kritičnih infrastrukturnih sistema i danas ostao nepromijenjen[1].

I u vreme hladnog rata države su planirale zaštitu svojih ključnih infrastrukturnih elemenata, kao što su elektrane, mostovi, luke i slično. U relativno mirnim osamdesetim godinama XX vijeka, napori za zaštitu ovih ključnih elemenata izgledali su manje važni. U isto vrijeme, rizici za društvo zbog nenamjernih i namjernih poremećaja kritične infrastrukture postepeno su se znatno povećali. U svakodnevnom životu savremenog društva, tehničke strukture, posebno u oblasti održavanja informacionih sistema, kontrole i upravljanja snabdijevanjem energijom, resursima pitke vode i saobraćajem, imaju prvorazredni značaj. Proces globalizacije i revolucije u oblasti informacione tehnologije pretvorile su kritičnu infrastrukturu u složene sisteme, međusobno zavisne i istovremeno veoma krhke i ranjive. Politički, ekonomski, društveni i ekološki događaji vezani za savremeno doba, a posebno teroristički napadi u raznim djelovima svijeta, globalna ekonomska recesija, razorni zemljotresi, nuklearne katastrofe (Fukušima, 11. mart 2011. godine), požari te posledice toplotnih talasa, naveli su čovječanstvo da uvidi kako je savremeni svijet u odnosu na ranije doba znatno ugroženiji od različitih katastrofa izazvanih djelovanjem čovjeka ili prirode. Ovi događaji su potencirali i međuzavisnost infrastrukture, društva i obavljanja vladinih funkcija. Sa aspekta opstanka, bezbjednosti i prosperiteta određene nacije ili države, od suštinskog je značaja da njegovi kritični sistemi budu na odgovarajući način organizovani i zaštićeni. Drugim riječima, komponente kritične infrastrukture moraju da izdrže bilo koju vrstu dejstva ili promjene, bilo političke, ekonomske, društvene ili ekološke, na način da budu obezbijeđeni osnovni uslovi za zadovoljavanje potreba društva i funkcionisanje nacionalnih ustanova[2].

Pojava i primjena koncepta kritične infrastrukture je, između ostalog, i posledica promjena u percepciji prijetnji i sve većom međusobnom zavisnošću raznih infrastrukturnih elemenata. To za posledicu ima povećanje ranjivosti društva od raznovrsnih oblika ugrožavanja, kao i pojava otkazivanja funkcija pojedinih kritičnih infrastrukturnih sistema. Savremeni društveni tokovi uticali su i na promjenu koncepta i stepena ranjivosti kritične infrastrukture. Ta ranjivost se do sada najčešće

[1] Grenda B., Ślachcińska E.: Terrorist Threats for the Critical Infrastructure of the State, *Advances in Economics,Business and Management Research*, volume 31, Atlantis Press, 2017,p. 165

[2] Nádai L., Padányi J.: *Critical Infrastructure Protection Research*, Springer International Publishing Switzerland 2016, p. 1

vezivala za probleme u funkcionisanju visokorizičnih tehnologija. Međutim, u aktuelnom trenutku s obzirom na obim, sadržaj i složenost kritične infrastrukture ranjivost je značajno veća, i na potencijalne prijetnje i ugrožavanja gleda se kao na pitanja od najvećeg značaja za nacionalnu bezbjednost. U tom kontekstu, pojam kritične infrastrukture obuhvata objekte kao što su zgrade, putevi i transportni sistemi, telekomunikacioni sistemi, vodovodni sistemi, energetski sistemi, hitne službe, bankarske i finansijske institucije i izvori snabdijevanja. Pored fizičkih struktura i sredstava, taj termin uključuje i virtuelne (sajber) sisteme i ljude. Uopšteno uzev, kritičnu infrastrukturu čine različiti sistemi koji su neophodni za nesmetano funkcionisanje vlasti na svim nivoima[3].

2.1. Pojam i klasifikacija kritične infrastrukture

Određenje pojma kritična infrastruktura je složen zadatak, prvenstveno zbog širokog obima koji on može da obuhvati, kao i velike raznolikosti sadržaja koji su po svojoj prirodi multidisciplinarni. Sam pojam „infrastruktura" može se definisati kao "osnovni okvir sistema ili organizacije" dok se za sintagmu "kritična infrastruktura" može upotrebiti mnoštvo definicija, jer je izraz „kritičan" promjenljiv i teško odredljiv. S druge strane, na složenost definisanja utiče i činjenica da se pojam kritična infrastruktura vremenom mijenjao pa je zbog toga ponekad ostajao nejasan ili nedovoljno određen. Prije terorističkih napada u SAD-u od 11. septembra 2001. godine, pojam infrastruktura odnosio se prvenstveno na javne radove i objekte koji su bili u javnom vlasništvu i kojima se upravlja, kao što su putevi, mostovi, vodovodi, aerodromi, morske luke, javne zgrade i slično. U savremenom dobu termin kritična infrastruktura predstavlja pojam koji sadrži, između ostalog, i vještačke mreže i sisteme koji pružaju potrebne usluge široj javnosti. Pored toga, predmetni pojam obuhvata i objekte i strukture, kako fizičke, tako i organizacione, koji pružaju osnovne usluge pripadnicima zajednice, što omogućava kontinuirano funkcionisanje društva na određenom prostoru. Pored toga, kritična infrastruktura je od vitalne važnosti za zajednicu ili naciju, jer u okolnostima njenog ometanja, oštećenja, uništenja ili nefunkcionisanja iz nekog drugog razloga, može imati negativan uticaj na bezbjednost, ekonomiju, nacionalno zdravlje i dobrobit građana i privrednog poslovanja. Pri tome se ne isključuje ni mogućnost značajnih gubitaka života u okolnostima kada nedostaje pružanje onih usluga koje omogućava kritična infrastruktura[4].

I pored složenosti definisanja, pojam kritične infrastrukture se obično određuje na jedan od dva načina. Prvi način se sastoji od nabrajanja svih vitalnih infrastruktura, kao što je bio slučaj u američkoj strategiji zaštite kritične infrastrukture iz 2003. godine, jednom od prvih dokumenata ove vrste[5]. Sa naučne strane posebno je značajan drugi pristup, koji definiše kritičnost kao rezultat specifičnih karakteristika. U ovom slučaju utvrđuju se određena (relaciona) svojstva sistema, jer je dati sistem kritičan u odnosu na druge sisteme ili entitete. Naime, sistem je kritičan za drugi sistem kada je prvi neophodan da bi se nastavilo sa radom drugog. Tako njemačka nacionalna strategija za zaštitu kritične infrastrukture definiše kritičnost kao relativnu mjeru za posledice poremećaja ili

[3] Kelley A., Pesch-Cronin N., Marion E.: *Critical infrastructure protection, risk management, and resilience: a policy perspective*, Taylor & Francis Group, 2016, p. 4
[4] Ibidem, pp. 4-5.
[5] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, United States Government, Washington, 2003

neuspjeha funkcije u vezi s isporukom dobara i usluga društvu[6]. U tom smislu, kritična infrastruktura je infrastruktura koja je potrebna da bi se nastavilo sa radom drugih većih tehničkih i/ili društvenih sistema ili koji su potrebni za obezbjeđivanje robe ili usluga koje se smatraju vitalnim za funkcionisanje modernog društva[7]. Iz navedenog možemo uočiti da je suštinski problem u definisanju pojma izraz kritičnost. U vezi sa tim, značajno je određenje po kome je „određen sistem kritičan ako obezbjeđuje rutinske funkcije, ako ne postoje praktične mogućnosti brze zamjene, iznenadna disfunkcija koja uzrokuje netrivijalne štete, i ako je ugrađen u integrisane sisteme ”[8]

Etimološki, korijen pojma kritičnost nalazi se u grčkom pojmu κρίσις (kriza) koji je u početku korišćen u medicinske svrhe da opiše određeni trenutak u toku bolesti u kome se određuje sudbina pacijenta (preživljavanje ili smrt). Termin i osnovni pojam kasnije su prevazišli polja teologije, prava i vojne strategije. Kada pokušamo da shvatimo potencijal termina kriza, jednako je važno ispitati i njegove metaforičke efekte. Upotreba svetske krize i uslovi povezani sa krizom evociraju slike radikalne promjene statusa kvo. Kao takav, izraz kriza postao je u modernoj istoriji sinonim za pojmove kao što su pobuna, konflikt ili revolucija[9]. Tokom ranog perioda hladnog rata, pojam kritičnosti je uključen u strategiju civilne odbrane Sjedinjenih Država. Naime, ovaj pojam je korišćen u kontekstu „mapiranja ranjivosti“, kao vrsta procjene vitalnih djelova države, odnosno važne tehničke infrastrukture[10]. Od tada se kritičnost sve više koristi u političkim i drugim debatama kao oznaka za identifikaciju organizacija i institucija koje su na bilo koji način važne, relevantne ili neophodne za nastavak snabdijevanja stanovništva i privrede dobrima i uslugama.

Većina naučnika u oblasti istraživanja infrastrukture koristi pojmove „kritičnost“ i „kritični“ u deskriptivnom značenju, slično njegovoj upotrebi u političkom diskursu. Pri tome pojedini autori kao polaznu osnovu uzimaju usluge stanovništvu (snabdijevanje vodom, energijom i slično) i ekonomiji koje se smatraju neophodnim, zbog čega se tehnički sistemi koji pružaju ove usluge označavaju kao kritična infrastruktura.[11] S druge strane, u naučnom pristupu zastupljena je istorijska ili razvojna perspektiva, pri čemu se polazi od skupa vitalnih dobara i usluga i prati kako su se u određenim društvima ili vremenskim periodima određene usluge smatrale sve važnijima zbog čega kritičnost predstavlja rezultat kolektivnih preferencija[12].

---

[6] *Bundesministerium des Innern Nationale Strategie zum Schutz Kritischer Infrastrukturen*, Bundesministerium des Innern. Berlin, 2009, p.7

[7] Lukitsch K., Müller M., Stahlhut C. Criticality in: Engels I., J. (ed.): *Key Concepts for Critical Infrastructure Research*, Springer, Wiesbaden, Germany, 2018, p. 12

[8] Egan M. J.: Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems, *Journal of Contingencies and Crisis Management*, 15, 2007, p. 5

[9] Koselleck et al.: Krise und Kritik. In: *Geschichtliche Grundbegriffe. Historisches Lexikon zur politisch-sozialen Sprache in Deutschland (Vol. 3)*, Klett-Cotta, Stuttgart, 1982, p. 619

[10] Collier S.J., Lakoff A.ndrew: Distributed Preparedness: The Spatial Logic of Domestic Security in the United States. In: *Environment and Planning D: Society and Space*, 26 (1), 2008, pp. 12–16

[11] Moteff J.,Copeland C.,Fischer J.: Critical Infrastructures: What Makes an Infrastructure Critical?,*The Library of Congress*, Washington, 2003, pp. 5-7, dostupno na: https://fas.org/irp/crs/RL31556.pdf

[12] Högselius P. et al. :The Making of Europe’s Critical Infrastructure: Common Connections and Shared Vulnerabilities. Houndmills, Basingstoke, Palgrave Macmillan, 2013, pp. 5-7, dostupno na: https://www.researchgate.net/publication/262684604_The_Making_of_Europe's_Critical_Infrastructure_Shared_Connections_and_Common_Vulnerabilities

2.2. Pristupi definisanju kritične infrastrukture na nivou država i međunarodnih organizacija

Termin infrastruktura korišćen je ranije u Francuskoj za označavanje posteljice – materijala koji se postavljao ispod pruge. Inače, sam pojam infrastruktura predstavlja kovanicu latinskog prefiksa infra, što znači dolje, ispod, a takođe i struktura. U kasnijoj upotrebi pojavljuje se u vojsci Sjedinjenih Američkih Država nakon formiranja NATO-a 1949. godine, a nakon toga i od strane urbanista nakon 1970. godine[13]. U Sjedinjenim Američkim Državama predmetni pojam se intenzivnije koristi od 1980. godine, nakon objavljene knjige *Amerika u ruševinama*[14], koja je pokrenula niz rasprava o problemima nacionalne infrastrukture, uzrokovane dugogodišnjim neadekvatnim ulaganjem i lošim održavanjem. To je između ostalog uticalo i na unapređenje upravljanja i održavanja infrastrukture u SAD-u.

U jednom od prvih određenja sintagme kritična infrastruktura pomenut je „veoma širok opseg javnih postrojenja i opreme koja je potrebna za pružanje društvenih usluga i podrške privrednim aktivnostima privatnog sektora“. Na ovakav način shvaćena, infrastruktura je obuhvatala širok spektar, uključujući puteve, mostove, vodene i kanalizacione sisteme, aerodrome, luke i javne objekte, uz mogućnost obuhvatanja i škola, zdravstvenih ustanova, zatvora, objekata za rekreaciju, proizvodnju električne energije, protivpožarne službe, deponije otpada i telekomunikacije[15]. Postoji i određenje da u kritičnu infrastrukturu spadaju„resursi i sistemi i mreže, fizički ili virtuelni, čije uništavanje ili onesposobljavanje može oslabiti nacionalnu bezbjednost, ekonomsku stabilnost i uticati na druge aspekte normalnog funkcionisanja društva“[16].

Pored navedenog, u upotrebi je i sličan pojam ključni resurs. Predmetni pojam označava sredstva koja su ili javno ili privatno kontrolisana, a neophodna su za minimalno poslovanje privrede i vlasti. Upotrebu predmetnog pojma možemo naći i u Nacionalnoj strategiji SAD iz 2003. godine, gdje isti obuhvata nacionalne spomenike, nuklearne elektrane, brane, vladine objekte, i najvažnija komercijalna sredstva. Do 2009. godine broj sektora ključnih resursa proširio se na 18, pri čemu su dobili nazive kritična infrastruktura i ključni resursi. Od tada, koncept kritične infrastrukture i ključnih resursa evoluirao je kako bi obuhvatio i druge sektore i resurse. U većini slučajeva u današnjoj nomenklaturi, ključni resursi nisu odvojeni od kritične infrastrukture, pa se često ovi pojmovi koriste kao sinonimi[17].

Za pojmovno određenje kritične infrastrukture, značajne su i definicije međunarodnih organizacija. Tako, na primer, NATO upotrebljava sintagmu „zaštita kritične infrastrukture“ koja sadrži „programe, djelatnosti i djelovanje vlada, vlasnika, operatora ili korisnika preduzete sa ciljem

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

[14] Choate P., Walter S.:*America in Ruins: The Decaying Infrastructure*, Duke Press PolicyStudies, New York, 1981

[15] Vaughan R., Pollard, R.: Rebuilding America VOL1, Planning and Managing Public Works in the 1980s., Council of State Planning Agencies, Washington D.C. 1984, pp. 1-2

[16] Rinaldi S.M.: Modeling and simulating critical infrastructures and their interdependencies, *37th Hawaii International Conference on System Sciences*, 2004. p.1, dostupno na: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.1206&rep=rep1&type=pdf

[17] Pesch-Cronin A. K., Marion E. N.: *Critical infrastructure protection, risk management, and resilience: a policy perspective*, Taylor & Francis Group, 2016, p. 5

zaštite vlastite kritične infrastrukture“.[18] U odnosu na navedenu definiciju, drugačije određenje imamo u slučaju Organizacije za ekonomsku saradnju i razvoj (*Organization for Economic Co-operation and Development*--OECD). Ova međunarodna organizacija pod kritičnom infrastrukturom podrazumijeva „skup infrastruktura i službi koje predstavljaju osnovu ekonomskog i socijalnog blagostanja, javne bezbjednosti i funkcionisanja vladinih organa“.[19] I u dokumentima UN-a susrećemo pojam kritične infrastrukture koja obuhvata „fizičke strukture, objekte, mreže i druga sredstva koja pružaju usluge od suštinskog značaja za društveno i ekonomsko funkcionisanje zajednice ili društva“.[20]

Pored navedenih određenja posebno su značajne definicije nacionalne kritične infrastrukture, koje države upotrebljavaju na osnovu svojih potreba za zaštitom s obzirom da ista predstavlja, između ostalog, osnov kvaliteta života i društvenog napretka. U vezi sa tim, nacionalne definicije se neznatno razlikuju u kriterijumima koji se koriste za definisanje kritičnosti infrastrukture. Većina država i nacionalnih institucija koristi kriterijume koji pokrivaju sve infrastrukture u svim sektorima. Sektorski kriterijumi se zatim koriste za unapređenje definisanja svakog specifičnog sektora. U nekim zemljama, ovi kriteriji apostrofiraju konačnost ili svrhu infrastrukture. Zato se naglašava da je infrastruktura kritična jer obavlja funkciju koja je od vitalnog značaja za društvo. U drugim slučajevima posebno se potencira ozbiljnost ili efekat poremećaja i uništenja date infrastrukture, koja je kritična zato što je njen gubitak izuzetno razoran za državu i društvo u cjelini[21].

Uz navedene različite pristupe, treba pomenuti i osnovne razlike na nivou nacionalnih država. Naime, geopolitički i geostrateški kao i geografski položaj države određuju sektore i podsektore kritične infrastrukture. S druge strane, države koje posjeduju nuklearni potencijal moraju ovom segmentu posvetiti posebnu pažnju, a pomorske države istu takvu pažnju nesmetanom transportu morskim putem, kao i lukama i lučkim postrojenjima. I pored toga, evidentan je opšti trend povećanja obima i sadržaja kritične infrastrukture, što utiče da definicije kritične infrastrukture imaju tendenciju znatnog proširenja. Liste kritične infrastrukture mnogih država obuhvataju ono što bi se moglo smatrati „tradicionalnim“ sektorima infrastrukture, kao što su transport i telekomunikacije, ali i sektore koji se obično ne bi smatrali sektorima infrastrukture kao što su hrana, zdravstvo, vlada i finansije. Sve to u krajnjoj liniji utiče i na programe koje države usvajaju u cilju upravljanja rizikom u zaštiti kritične infrastrukture. Upravljanje rizikom pomaže vladama da identifikuju ključne bezbjednosne rizike, procijene rizike i uspostave strategije i prioritete u zaštiti nacionalne kritične infrastrukture.

Pored navedenog, u ovom dijelu rada daćemo i nacionalna određenja kritične infrastrukture pojedinih država. Za Austriju, kritična infrastruktura je „ona infrastruktura ili njeni djelovi koji su od ključne važnosti za osiguranje važnih društvenih funkcija“, pri čemu „njihovo nefunkcionisanje ili uništenje ima ozbiljne posledice na zdravlje, sigurnost ili ekonomsko i socijalno blagostanje

[18] Jakovljević V.: Resursi kritične infrastrukture i njihov značaj za upravljanje vanrednim situacijama, *Zbornik radova FCO*, Beograd, 2010. str. 65-69
[19] Gordon K., Dion M.: Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security, *OECD*, France, 2008, p. 3
[20] United Nations International Strategy for Disaster Reduction (UNISDR), *Terminology on Disaster Risk Reduction*, dostupno na https://www.unisdr.org/we/inform/terminology#letter-c
[21] Lazari A.: *European Critical Infrastructure Protection*, Springer, 2014, p. 3

stanovništva ili funkcionisanje vladinih institucija“.[22] U Italiji se pod kritičnom infrastrukturom podrazumijeva „sistem, resurs, proces, struktura, čak i virtualna, čije uništavanje, prekid ili čak djelimična ili privremena nedostupnost ima za posledicu značajno slabljenje efikasnosti i normalnog funkcionisanja zemlje, kao i bezbjednosti i ekonomske, finansijske i socijalne sisteme, uključujući centralne i lokalne organe javne uprave“.[23]

S druge strane u Francuskoj se ne upotrebljava pojam „kritičnost“ već pojam „vitalnost“ sa značenjem osnovne usluge ili infrastrukture. Zbog toga se u toj zemlji vitalna infrastruktura definiše kao „svaka ustanova, postojenje ili struktura, čija nedostupnost ili uništenje kao rezultat zlonamernog djelovanja, sabotaže ili terorističke akcije može direktno ili indirektno da izuzove štetu, posebno ako je njena djelatnost teško zamenjiva, ozbiljno ugrožava ratni ili ekonomski potencijal, nacionalnu bezbjednost, opstanak nacije, ili da ozbiljno utiču na zdravlje ili život stanovništva“.[24] Pored navedenog, francuska strategija je specifična jer uvodi pojam „vitalne zone“, kao oblast koja obuhvata nekoliko „vitalnih tačaka“, koje pripadaju različitim „vitalnim operatorima“. To je posebno značajno sa bezbjednosnog aspekta budući da postoji međuzavisnost između „vitalnih tačaka“, jer bi ostvarivanje prijetnje jednom od njih imalo posledice po integritet i djelatnosti ostalih. S druge strane, preduzimanje mjera bezbjednosti na jednoj „vitalnoj tački“ ili na zajedničkom dijelu utiče na bezbjednost jedne ili više drugih „vitalnih tačaka“[25].

Znatno kraće ali i sadržajnije je određenje kritične infrastrukture u Poljskoj, gdje se pod ovim pojmom „podrazumijevaju sistemi i međusobno povezani funkcionalni objekti koji se u njima nalaze, uključujući objekte, postrojenja, instalacije i usluge od ključnog značaja za bezbjednost države i njenih građana, kao i za obezbjeđivanje efikasnog funkcionisanja organa javne uprave, institucija i preduzeća“.[26] S druge strane, u Španiji se pojam strateška infrastruktura izjednačava sa pojmom kritična infrastruktura. Tako je kritična infrastruktura ujedno strateška infrastruktura koja pruža osnovne usluge, čije je funkcionisanje neophodno i koja ne dozvoljava alternativna rešenja, dok bi njihov prekid ili uništenje imalo ozbiljan uticaj na osnovne usluge“.[27] Na Novom Zelandu pojam kritična nacionalna infrastruktura obuhvata „fizičku i digitalnu imovinu, usluge i lance snabdijevanja, čiji bi poremećaj (gubitak) ozbiljno uticao na održavanje nacionalne i javne bezbjednosti, osnovnih prava i dobrobiti svih novozelandskih stanovnika“.[28]

---

[22] Austrian Cyber Security Strategy, Vienna, 2013, p. 20, dostupno na: https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf

[23] Presidency of the Council of Ministers,*Civil Protection Agency*, dostupno na:http://www.protezionecivile.gov.it/tools/footer/glossary?p_p_id=DpcGlossario_WAR_DpcGlossario100SNAPSHOT&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_DpcGlossario_WAR_DpcGlossario100SNAPSHOT_letter=C&_DpcGlossario_WAR_DpcGlossario100SNAPSHOT_action=listByLetter

[24] Premier Ministre Secretariat general de la Defense et de la Securite Nationale, *Instruction Generale Interministerielle relative a la Securite des Activites d'importance vitale* N°6600/SGDSN/PSE/PSN du 7 janvier 2014, p. 3, dostupno na: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf

[25] Ibidem, p. 7

[26] *Rządowego Centrum Bezpieczeństwa*, Warszawa, dostupno na: https://rcb.gov.pl/en/critical-infrastructure/

[27] Spanish Ministry of the Interior, *The National Center for Infrastructure Protection and Cybersecurity (CNPIC)*, dostupno na: http://www.cnpic.es/en/Preguntas_Frecuentes/Que_es_una_Infraestructura_Critica/index.html

[28] New Zealand's Cyber Security Strategy, Department of the Prime Minister and Cabinet, 2019, p. 16, dostupno na: https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

DRŽAVA	DEFINICIJA KRITIČNE INFRASTRUKTURE
SAD	Sistemi i sredstva, fizički ili virtuelni, koji su od vitalnog značaja za SAD i njihova nesposobnost ili uništenje može imati uticaj na bezbjednost, ekonomsku sigurnost, javno zdravlje ili bilo koju kombinaciju ovih stvari.
Velika Britanija	Nacionalna kritična infrastruktura sastoji se od sredstava, usluga i sistema koji podržavaju ekonomski, politički i društveni život u Velikoj Britaniji čiji značaj je takav da gubitak može da: izazove velike gubitke života, da ima ozbiljan uticaj na nacionalnu ekonomiju i imaju i druge teške socijalne posledice za zajednicu.
Njemačka	Kritična infrastruktura obuhvata organizacije i ustanove od velikog značaja za zajednicu, čiji neuspjeh ili oštećenje može izazvati trajan nedostatak zaliha, velike poremećaje u javnom redu i druge dramatične posledice.
Letonija[29]	Kritična infrastruktura su objekti, sistemi ili njihovi djelovi u Letoniji, koji su važni za obavljanje funkcija od suštinskog značaja za društvo, kao i za obezbjeđivanje zaštite zdravlja ljudi, bezbjednosti, ekonomskog ili socijalnog staranja, čije uništavanje ili neispravnost mogu značajno da utiču na vršenje državnih funkcija.
EU[30]	Kritična infrastruktura podrazumijeva postrojenja, sistema ili određene komponente tih sistema, koji se nalaze u državama članicama i koji su esencijalni za obavljanje osnovnih funkcija država i Unije, koji su neophodni za funkcionisanje zdravstva, za bezbjednost članica i za ekonomsko i socijalno blagostanje građana, a čije bi otkazivanje ili ometanje funkcionisanja imalo znatan negativan uticaj na države članice, a indirektno i na čitavu Evropsku uniju.

Tabela br.1.: Definicije kritične infrastrukture u pojedinim državama[31]

U hrvatskom zakonodavstvu definisano je da su „nacionalne kritične infrastrukture sistemi, mreže i objekti od nacionalne važnosti, čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posledice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okolinu, bezbjednost i ekonomsku stabilnost i neprekidno funkcionisanje vlasti“.[32] U odnosu na navedenu definiciju je znatno uže određenje u švajcarskim dokumentima, gdje taj pojam obuhvata „procese, sisteme i objekte koji su neophodni za funkcionisanje ekonomije i blagostanje stanovništva[33]. I bez dodatnih analiza evidentno je da kritična infrastruktura obuhvata širok spektar vitalnih sektora (Tabela br.1).

Kritična infrastruktura najčešće uključuje saobraćaj, transport, proizvodnju i distribuciju energije, informacione i komunikacione sisteme, zdravstvene službe, sisteme za snabdijevanje vodom i hranom, finansijske službe, državnu infrastrukturu i slično. U okolnostima eventualnog djelimičnog ili potpunog otkazivanja ovih infrastruktura dolazi do ugrožavanja društva, nacionalne bezbjednosti i do najrazličitijih drugih problema. Zato mnoge države nastoje da identifikuju i analiziraju kritične sektore kao i podsektore, procese i objekte uz korišćenje različitih metodoloških i političkih pristupa.

[29] Cyber Security Strategy of Latvia, p. 20

[30] Council Directive 2008/114/EC, On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, *Official Journal of the European Union, L 345/75-L 345/82, 2008.*

[31] Gordon K., Dion M.: Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security, OECD, France, 2008, p. 4

[32] Zakon o kritičnim infrastrukturama, „*Narodne novine*“ br. 56/13, čl. 3

[33] *National strategy for the protection of Switzerland against cyber risks 2018-2022*, p. 30

Međutim, sama složenost infrastrukturnih sistema je najveći zajednički problem svih država koje su pristupile identifikovanju i izgradnji politike zaštite kritične infrastrukture[34]

Evidentno je da ne postoji opšteprihvaćena definicija kritične infrastrukture jer je to pitanje koje se tiče svake države posebno. Pored toga, postoje različiti kriterijumi izbora infrastrukture za kritičnu infrastrukturu što zavisi od države porijekla i praktičnog tumačenja liste kritične infrastrukture i što je u krajnjoj liniji uslovljeno metodološkim pristupom. Pored toga, u današnje vrijeme, svaka država ili organizacija je prinuđena da definiše i klasifikuje svoju infrastrukturu, a naročito onu za koju smatra da je kritična. Prema dokumentima Evropske unije, kritične infrastrukture moraju biti definisane i navedene u svim državama članicama, kao i u zemljama koje pretenduju da postanu punopravne članice EU. Istovremena različite konceptualizacije i određenja kritične infrastrukture u državama posledica su i različite percepcije prijetnji i bezbjednosnih rizika, kao i razlika u geografskom položaju, istorijskom nasleđu i sociopolitičkim faktorima. U skladu sa postavljenim kriterijuma, a radi potpunijeg i sveobuhvatnijeg definisanja, potrebno je i adekvatnije sagledavanje različitih tipova kritične infrastrukture. U načelu, kritična infrastruktura može biti od posebnog značaja za države, regione ili svijet, pa se može govoriti o nacionalnoj, regionalnoj (na primjer evropskoj, evroazijskoj) i globalnoj kritičnoj infrastrukturi. Sa aspekta države kritičnu infrastrukturu možemo posmatrati sa lokalnog, regionalnog (ekonomskog ili kulturnog regiona u državi), nacionalnog i međunarodnog nivoa. Infrastuktura u najopštijem smislu može se podijeliti na tvrdu i na meku infrastrukturu. Pojam tvrda infrastruktura obuhvata fizičke sisteme potrebne za funkcionisanje savremenog industrijskog društva. S druge strane, termin meka infrastruktura obuhvata one institucije koje su prijeko potrebne za očuvanje ekonomskih, zdravstvenih, kulturnih i društvenih standarda[35].

Posebno je interesantna podjela kritične infrastrukture Njemačke (Tabela br. 2) koja je na osnovu tehničke, strukturalne i funkcionalne specifičnosti klasifikovala vitalnu (apsolutno neophodnu) osnovnu tehničku infrastrukturu, s jedne strane, i vitalnu (apsolutno suštinsku) infrastrukturu društveno-ekonomskih usluga, s druge strane.

OSNOVNA TEHNIČKA INFRASTRUKTURA	INFRASTRUKTURA SOCIJALNO-EKONOMSKIH USLUGA
Snabdijevanje energijom	Zdravstvo; hrana
Informaciono- komunikaciona tehnologija	Hitne i spasilačke službe; kontrola i upravljanje katastrofama
Transport	Parlament; vlada; javna uprava; agencije za sprovođenje zakona
Snabdijevanje pijaćom vodom i i odlaganje voda	Finansije; posao osiguranja
	Mediji; i kulturni objekti (kulturno nasleđe)

Tabela br. 2.: Podjela nacionalne kritične infrastrukture u Njemačkoj[36]

[34] Lewis T.: *Infrastructure Protection in Homeland Security, Defending a Networked Nation,* Wiley Interscience, 2006.
[35] Niskanen A. W.: The soft infrastructure of a Market, CATO Journal, In: Gotbaum R: The Difference Between Soft And Hard Infrastructure, And Why It Matters, *State Impact Magazine*, New Hampshire, 2011, pp. 233-238,
[36]*National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Berlin, 2009, r. 7

Postoje značajne međuzavisnosti između ova dva infrastrukturna sektora, jer se gotovo sve infrastrukture društveno-ekonomskih usluga u velikoj mjeri oslanjaju na neograničenu dostupnost osnovne tehničke infrastrukture. Međutim, tehnička osnovna infrastruktura u značajnoj mjeri zavisi od socijalno-ekonomske uslužne infrastrukture, poput stabilne pravne službe ili funkcionisanja prve reakcije, hitne medicinske i spasilačke službe u slučaju krize.

Iz navedenog se može zaključiti da su u upotrebi i različite metodologije, koje možemo grupisati u tri najvažnije vrste. Prva vrsta zasniva se na uslugama (primjer Švajcarske), kada vlada identifikuje kritičnu infrstrukturu (imovinu) na osnovu kriterijuma specifičnih za sektor koji određuju prag nivoa usluge. Druga vrsta zasnovana je na operatoru (primjer Francuske) gde je najvažniji zadatak utvrditi koja su sredstva ili usluge kritične za pojedine operatore kritične infrastrukture. Treća vrsta bazira se na pristupu koji koristi elemente servisno orijentisanog pristupa, što je slučaj u Velikoj Britaniji. Naime, Velika Britanija prepoznaje devet kritičnih sektora i dvadeset podređenih kritičnih službi. Ove usluge su sastavljene od sredstava koja je potrebno identifikovati. Ministarstvo nadležno za taj sektor vrši početni izbor imovine i operatora koji se biraju na osnovu njihovog relativnog tržišnog udijela.[37]

Kada se u Sjedinjenim Američkim Državama raspravlja o klasifikaciji kritične infrastrukture, najčešće se pominje definicija iz Izvršne naredbe 13010, koja predstavlja osnovu za dalje određenje šta infrastrukturu čini kritičnom: „Određene nacionalne infrastrukture koje su toliko vitalne da bi ometanje njihovog rada ili uništenje imalo efekat slabljenja odbrambene ili ekonomske sigurnosti SAD“[38]. Daljom operacionalizacijom navedene naredbe dolazi se do podjele kritične infrastrukture na: „telekomunikacije, sisteme električne energije, skladištenje i transport nafte i gasa, bankarstvo i finansije, transport, sisteme za snabdijevanje vodom, hitne službe (medicinske, policijske, zaštite i za spasavanja) i kontinuitet vlasti“.[39]

Kritičnu infrastrukturu možemo uslovno podijeliti i na fizičke i sajber (*cyber*) sisteme koji su od vitalnog značaja za nesmetano funkcionisanje privrede i vlade. Navedna podjela je posebno značajna sa aspekta bezbjednosti, jer fizička bezbjednost obično znači zaštitu fizičkih sredstava (uključujući kompjutersku opremu) od oštećenja fizičkom silom kao što su eksplozije, vjetar, vatra i slično. S druge strane, sajber bezbjednost označava zaštitu i fizičkih i sajber sredstava od operativnog pada ili od neovlašćenog kompjuterskog pristupa operativnom softveru ili podacima. Pružanje fizičke i sajber bezbjednosti kritičnim infrastrukturama podrazumijeva širok obim aktivnosti koji mogu da variraju. Jedna od podjela kritične infrastrukture može se zasnivati i na osnovu geografskog rasporeda. Naime, objekti kritične infrastrukture su neravnomjerno raspoređeni u prostoru. Oni su najčešće smješteni u urbanim sredinama, pri čemu se procjenjuje da se 80 % resursa kritične infrastrukture nalazi na 20% teritorije određene države[40]. Razlog navedenom treba tražiti između ostalog i u koncentraciji stanovništva u urbanim sredinama u mnogim djelovima svijeta, što ujedno otvara mnoga pitanja vezana za održivi razvoj. Zahtjevi za pouzdanost urbane infrastrukture su među

[37] *Good practices manual for CIP policies, For policy makers in Europe*, European Commission-Directorate-General Home Affairs, 2011, p. 23

[38] Executive Order 13010 - Critical Infrastructure Protection, *Federal Register, Vol. 61, No. 138*. pp. 37347-37350, dostupno na: https://www.hsdl.org/?abstract&did=1613

[39] Ibidem, p. 37347.

[40] Lewis T.: *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Wiley Interscience,New Jersey, 2014, p. 18

najvažnijim izazovima, jer postaju sve kritičniji za visoko koncentrisane gradske sredine. Zbog toga i zaštita kritične infrastrukture u gradovima zaslužuje posebnu pažnju u okviru nacionalnih okvira zaštite.

Pored navedenog, često se upotrebljavaju i izrazi kritična infrastruktura i kritična informaciona infrastruktura, što su različiti, ali povezani pojmovi. Međutim, veza između njih se uglavnom zanemaruje, iako je neophodno napraviti i razliku. Kritične infrastrukture uključuju i kritičnu informacionu infrastrukturu, ali nisu ograničene samo na informacionu infrastrukturu, koja je samo njihov dio. Nefunkcionisanje informacione infrastrukture može dovesti do nefunkcionisanja ukupne kritične infrastrukture, ali kritična infrastruktura može biti ugrožena i zbog mnogih drugih razloga koji ni na koji način nisu povezani sa informacionom infrastrukturom[41]. Najznačije nacionalne podjele kritične infrastrukture za pojedine države prikazane su u Tabeli br. 3

Velika Britanija	Njemačka	Švedska	Norveška	Holandija	Švajcarska
Energija	Energija	Energija	Energija i objekti	Energija i objekti	Objekti i službe
Telekomunikacije	Telekom. i informac. infrastr.	Telekomunikacije	Telekomunikacije	Telekomunikacije	Telekomunikacije
Zdravstvene službe	Zdravstvo	Zdravstvo	Zdravstvo	Zdravstvo	Zdravstvo
Finansije	Bankarstvo i finansije	Bankarstvo i finansije	Bankarstvo i finansije	Bankarstvo i finansije	Finansije
Transport	Transportni sistemi	Transport	Transport	Transport	Transport
Hitne službe	Hitne i spasilačke službe	Hrana	Spasilačke službe	Hrana	Hrana
Centralna vlast	Vlast i javne službe	Elektronske informacione službe	Snabdijevanje naftom i gasom	Javni red i bezbjednost	Distribucija informacija
Voda	/	Voda	Policija	Upravljanje vodama	Vodosnabdijevanje
/	/	Društvene vrijednosti	Društvena bezbjednost	Vlast	Administracija
/	/	/	Odbrana	Odbrana	Vojna odbrana
/	/	/	/	Pravosuđe	Civilna odbrana
/	/	/	/	Pijaća voda	Socijalna sigurnost

Tabela br. 3.: Lista kritične infrastrukture pojedinih evropskih država[42]

[41] Zaballos G.,A., Jeun I.: *Best Practices for Critical Information Infrastructure Protection (CIIP), Experiences from Latin America and the Caribbean and Selected Countries*, Inter-American Development Bank, Washington, 2016, p. 3-4

[42] Mićović M.: Bezbednosni aspekti funkcionisanja kritične infrastrukture u vanrednim situacijama, *doktorska disertacija*, Fakultet bezbednosti, Beograd, 2016, str. 42

2.3. Značaj kritične infrastrukture

Državne politike, strategije, doktrine i pojedine direktive pristupaju problematici kritične infrastrukture na različite načine, ali najčešće u cilju uspostavljanja moderne i efikasne infrastrukture koja je od vitalnog značaja za razvoj moderne ekonomije i nacionalni progres. Dobro osmišljena infrastruktura je osnovni pokretač nacionalnog prosperiteta i predstavlja preduslov za ekonomsku ekspanziju i budući rast. Infrastruktura omogućava nacionalnu produktivnost, kvalitet života i ekonomsku progresiju kroz pokretanje rasta, stvaranje radnih mjesta i poboljšanje produktivnosti, kvaliteta života i efikasnosti. Ona podstiče rast tako što obezbjeđuje široku mrežu podrške na koju se svi oslanjaju. Umrežena infrastruktura, za šta su primjer transport i komunikacije, podstiče dugoročni ekonomski učinak, jer pruža korist drugim sektorima, ali i doprinosi poboljšanju učinkovitosti poslovanja i stvaranju efikasnih mehanizama za koordinaciju i upravljanje lancima snabdijevanja i isporuku proizvoda. Otporne i pouzdane mreže obezbjeđuju poslovno samopouzdanje što dovodi do povećanja poslovnih investicija i rasta i stvaranja novih ekonomskih mogućnosti. Ulaganje u infrastrukturu i način upravljanja ovim investicijama takođe može imati značajan uticaj na ekonomske ciljeve vlade. Zato su investicije u infrastrukturu neophodne za funkcionisanje ekonomije i doprinose efikasnosti poslovanja, povezanosti i poslovnom rastu, što između ostalog može dovesti do povećanja povjerenja u postojeću i buduću infrastrukturu[43].

Rasprostranjena i efikasna infrastruktura predstavlja i ključ za osiguranje efikasnog funkcionisanja privrede, jer je ista važan faktor u određivanju lokacije investicijskih ulaganja i određivanju vrsta ekonomskih aktivnosti, kao i sektora koji se mogu razvijati u određenoj državi. S druge strane, dobro razvijena infrastruktura smanjuje i efekat udaljenosti između regiona, integrišući nacionalno tržište i povezujući ga sa drugim tržištima, uz istovremeno smanjenje troškova, što je od posebnog značaja u svaremenim ekonomskim odnosima.

Po definiciji, infrastruktura se vezuje za strukture koje formiraju osnovnu bazu, neophodnu za odvijanje određenih aktivnosti. Infrastrukture održavaju vitalne funkcije društva i čine svakodnevni život predvidljivim, sigurnim i zdravim, ali i obezbjeđuju resurse za stvaranje i obnavljanje svakodnevnih aktivnosti. U oblikovanju dinamike svakodnevnog životnog toka, one utiču na ono što se smatra normalnim i dovoljnim[44]. Preplitanje infrastrukture i društvenog života rezultira činjenicom da su pogodnosti, sigurnost i zdravo svakodnevno življenje povezani, pri čemu se svakodnevni društveni procesi oslanjaju na pristup infrastrukturi i njihovu pretpostavljenu besprekornost.

Kritična infrastruktura je okosnica modernog društva i od suštinskog je značaja za nacionalni prosperitet. Otporna i sigurna infrastruktura je od vitalnog značaja za ekonomski prosperitet, jer ne samo da podupire efikasno poslovanje kompanija i pružanje usluga, već podupire dugoročno povjerenje i planiranje na nacionalnom i regionalnom nivou, a time i osiguranje stalnog i stabilnog nivoa ulaganja. Obezbjeđivanje ove otpornosti i bezbjednosti može stoga djelovati i kao direktna injekcija u regionalnu ili sektorsku ekonomiju, a takođe i kao katalizator za dalji ekonomski rast i investicije. Međutim, kada dođe do prekida u pružanju usluga kritične infrastrukture, posebno u

---

[43] *Role of Critical Infrastructure in National Prosperity*, Shared Narrative, Government of Canada, 2015, pp. 2,3, dostupno na: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-rl-crtclnfrstrctr-ntnlprsprty/index-en.aspx

[44] Hand M., Shove E., Southerton D: Explaining Showering: A Discussion of the Material, Conventional, and Temporal Dimensions of Practice, *Sociological Research Online No* 1, British Sociological Association, London 2005, p. 10

područjima kao što su energetska, transportna i komunikaciona mreža, to potencijalno može imati direktne negativne ekonomske uticaje, prije svega vezano za troškove popravke štete na fizičkoj strukturi, kao i indirektne ekonomske uticaje na društvo, uključujući prekid poslovanja u globalnom lancu snabdijevanja i povećanje kratkoročne i dugoročne nezaposlenosti.

Poremećaji u funkcionisanju kritične infrastrukture mogu uticati i na pravovremenu isporuku roba i usluga koje su od posebnog značaja za nacionalne ekonomije, što može u krajnjoj liniji uticati i na gubitak poslovanja i prihoda od poreza na pogođenim područjima, ali i širih regionalnih posledica. U okolnostima katastrofa, evidentni su direktni i indirektni ekonomski uticaji i poremećaji koji se manifestuju u sektorima radne snage, trgovine, proizvodnje, transporta, lanaca snabdijevanja, a pogađaju i društvo u cjelini. Tako je, na primjer, uragan Sindi u Sjedinjenim Američkim Državama 2013. godine prouzrokovao ekonomski gubitak od 65 milijardi američkih dolara[45]. Učestale ili teško nadoknadive štete sa produženim periodom oporavka za poslovne subjekte i privredu u cjelini doprinose proširenju i povećanju gubitaka na nacionalnom nivou, što ukazuje na povećanu važnost jačanja otpornosti kritične infrastrukture unutar države.

Savremena društva su sve više zavisna od kritičnih infrastrukturnih sistema koji pružaju osnovne usluge i podržavaju ekonomski prosperitet društva i države u cjelini. S obzirom da su ovi sistemi sve više međusobno zavisni, postoji rizik da po principu kaskade i manji propusti eskaliraju u događaje katastrofalnih razmjera. Kada se kritična infrastruktura ugrozi ili poremeti, sami građani osećaju ekonomski uticaj tih prijetnji i posledica ugrožavanja. Zbog toga ulaganja u otpornost infrastrukture i izgradnja robusnih sistema na nacionalnom nivou mogu smanjiti dužinu i obim poremećaja u funkcionisanju kritične infrastrukture[46].

Da kritična infrastruktura ne mora biti vezana samo za resurse koji su od značaja za ekonomski razvoj i stabilnost zemlje, pokazuje i primjer Sjedinjenih Američkih Država, koje su 2010. godine donijele aneks Plana zaštite nacionalne kritične infrastrukture, uključujući u tu zaštitu i spomenike, objekte i ostalu kulturnu baštinu od nacionalnog i istorijskog značaja. Vlada SAD-a je pomenutim sektorskim planom željela da ukaže na značaj zaštite tih kulturnih i istorijskih dobara od potencijalnih izvora ugrožavanja imajući u vidu njihovu vrijednost kao nacionalnih simbola i uticaj koji bi njihovo uništenje ili oštećenje imalo na moral građana.[47]

U razvijenom svijetu društvene funkcije u velikoj mjeri zavise od umreženih sistema. Čak i najosnovnije svakodnevne funkcije uključuju interakciju sa različitim kritičnim infrastrukturnim sistemima. Na primjer, milioni ljudi širom svijeta koriste transportnu infrastrukturu da bi došli do posla, škole ili lokalnog tržnog centra.Telekomunikacijska infrastruktura se koristi za održavanje kontakata sa porodicom i prijateljima, kupovinu ili obavljanje finansijskih transakcija. Energetska infrastruktura se koristi za zagrijevanje domova, napajanje lokalnih industrija i isporuku goriva za prevozna sredstva. Iako su ove osnovne aktivnosti relativno lako shvatljive, širina upotrebe te infrastrukture je manje očigledna.

---

[45] Hurricane Sandy Rebuilding Task Force, "*Hurricane Sandy Rebuilding Strategy," Stronger Communities*, A Resilient Region August, 2013, p. 20, dostupno na: https://www.hud.gov/sites/documents/HSREBUILDINGSTRATEGY.PDF

[46] Lazari A.: *European Critical Infrastructure Protection*, Springer, 2014, r.7

[47] *National Monuments and Icons Sector – Specific Plan: An Annex to the National Infrstructure Protection Plan*, U.S. Department of Homeland Security, 2010, dostupno na: https://www.hsdl.org/?abstract&did=691293

Kritična infrastruktura se može posmatrati i kao struktura čije nefunkcionisanje pojačava poremećaje i podstiče društveno nepovjerenje, pa je stoga primamljiva meta sa stanovišta terorista[48]. Iskorišćavanje kritične infrastrukture za terorističke napade manifestuje i simbolizuje ranjivost društvenog poretka. To se posebno odnosi na strukture koje obezbjeđuju svakodnevne pogodnosti stanovništva, jer teroristi njihovim ugrožavanjem nastoje da pošalju psihološki važnu poruku da niko nije siguran. Vjerovatnoća da kritična infrastruktura bude meta takvih napada povećava se prisutnom tendencijom terorističkih grupa da se usmjeravaju na takozvane meke ciljeve, da izvode sve kompleksnije napade i da žele maksimiziranje broja žrtava[49]. Kod terorističkih akata na kritičnu infrastrukturu osnovni ciljevi su izazivanje poremećaja u pružanju javnih usluga na koje se stanovništvo snažno oslanja i podrivanje povjerenje građana u sposobnost nacionalnih vlasti da zaštite građane. To se u Evropi prvi put u punoj mjeri manifestovalo tokom terorističkih napada u Madridu 2004. godine i godinu dana kasnije u Londonu[50].

Analizirajući značaj kritične infrastrukture, potrebno je pomenuti i efekte razvoja telekomunikacionih tehnologija koji su najočigledniji u urbanim sredinama. Naime, svakodnevno se koriste usluge niza različitih informaciono-tehnoloških sistema i mreža. Industrijski sistemi koji se kontrolišu preko Interneta takođe su uključeni u upravljanje kritičnom infrastrukturom. U najkraćem, veoma veliki broj ljudi, uređaja i objekata danas su međusobno povezani. Između ostalog, strukturna funkcionalnost modernih gradova je definisana i osnovnim algoritmima, softverom i njihovom sigurnošću[51].

Kada se razmatra socio-tehnička priroda kritičnih infrastruktura, treba napomenuti da ozbiljni poremećaji u sistemu mogu ići izvan geografskih, organizacionih i administrativnih granica država, čime se aktivira višestruki skup aktera, čija je sposobnost da sarađuju neophodna da bi se situacija vratila u normalno stanje. Pored navedenog, postoji i zavisnost sistema koja se često naziva međuzavisnost, jer se u funkcionisanju infrastrukturnih sistema problem može pojaviti između različitih tipova sistema, različitih faza razvoja sistema i različitih faza rada i održavanja sistema. Međuzavisnost ima značajan uticaj na dinamiku poremećaja kritične infrastrukture. Zbog međuzavisnosti, abnormalni događaj u jednom sistemu može izazvati negativan uticaj negdje drugdje, što opet može izazvati dodatne efekte kako na originalni sistem tako i na druge sisteme koji su povezani sa njim. Zbog međusobne povezanosti i socio-tehničke prirode kritične infrastrukture, poremećaji mogu biti i veoma nelinearni i nepredvidivi. Uz to, međuzavisnost može da djeluje na način da intenzivira strukturu jer prenosi efekte sa različitih nivoa i mjesta na druge sisteme[52].

---

[48] Glass T.A., Schoch-Spana, M.: Bioterrorism and the People: How to Vaccinate a City against Panic, *Clinical Infectious Diseases*, Volume 34, Issue 2. Oxford academic, 2002, pp. 217–223

[49] Boin A.; Smith D.: Terrorism and Critical Infrastructures: Implications for Public–Private Crisis Management, *Public Money & Management*Volume 26, Issue 5, Taylor & Francis, 2006, pp. 295–304

[50] Maiolo M., Pantusa D.: Infrastructure Vulnerability Index of drinking water systems to terrorist attacks,*Cogent Engineering*, Volume 5, Issue 1 2018, pp. 2–3, dostupno na: https://www.cogentoa.com/article/10.1080/23311916.2018.1456710.pdf

[51] Brenner J.F.: Eyes wide shut: The growing threat of cyber attacks on industrial control systems. Bulletin of the Atomic Scientists., 69 (3), 2013, pp. 15–20, dostupno na: https://journals.sagepub.com/doi/pdf/10.1177/0096340213501372

[52] Pescaroli G., Alexander D.: A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor,*GRF Davos Planet@Risk*, Volume 3, Number 1, Special Issue on the 5th IDRC Davos 2015, pp. 58–67, dostupno na: https://www.researchgate.net/publication/277220856_A_definition_of_cascading_disasters_and_cascading_effects_Going_beyond_the_toppling_dominos_metaphor

Poseban značaj kritične infrastrukture može se sagledati i iz ugla kriza koje po svojoj prirodi imaju različite veličine i karaktere. U tom smislu, kriza podrazumijeva prijetnju osnovnim vrijednostima sistema ili funkcionisanja sistema održavanja života, kojima se mora hitno pristupiti u uslovima velike nesigurnosti. Kvarovi na kritičnoj infrastrukturi koji odstupaju od uobičajenih i „ponašaju se" naizgled nepredviđeno, prelazeći iz jednog sistema u drugi, teže da stvore osjećaj krize. Primjer za to je i raspad elektroenergetske mreže u sjeveroistočnom dijelu SAD-a 2003.godine, koji je bio više od vanredne situacije. Taj događaj je predstavljao pravu krizu koja je emitovana uživo na glavnim televizijskim mrežama i ujedno predstavljala operativni i strateški izazov državnim i privatnim akterima. Inače, sa aspekta kritične infrastrukture treba praviti i jasnu razliku između pojma krize i katastrofe. Označavanje situacije kao katastrofe znači da je došlo do gubitaka života i teške, dugoročne štete na imovini i infrastrukturi. Drugim riječima, katastrofa je „kriza sa lošim završetkom"[53]. Kvarovi kritične infrastrukture sami po sebi lako stvaraju osećaj krize, ali objektivno rijetko dovode do katastrofe (na primjer, kriza zagađenja vode u Sidneju, 1998. godine)[54].

Značaj kritične infrastrukture se povećava ukoliko je država industrijski razvijenija. Sa ekonomskim razvojem se povećava i zavisnost od nesmetanog funkcionisanja kritične infrastrukture, i to ne samo na sopstvenoj teritoriji, već i na područjima susjednih država. Na osnovu analize savremenih trendova u kritičnoj infrastrukturi, nedvosmisleno se može uočiti trend povećanja njenog značaja ne samo za državu i društvo, već i za svakodnevni život pojedinca. Takav trend možemo očekivati i u budućnosti s obzirom da je moderan način života postao neodvojiv od sadržaja kritične infrastrukture. Razlog tome treba tražiti u činjenici da će savremeni svijet i u budućnosti zavisiti više-manje od pojedinih sektora infrastrukture, a posebno energetskog sektora, komunikacija, transportnih sistema, finansija, interneta i javnih službi. Zbog toga će i svaki poremećaj u njihovom radu dovoditi do ozbiljnih stanja i poteškoća za pojedince, društvo i poslovne entitete, kao i za funkcionisanje države u cjelini. I u kriznim i vanrednim situacijama pojedini sektori kritične infrastrukture imaće poseban značaj. To su prvenstveno javne usluge koje se odnose na rad bolnica, policijskih i vatrogasnih stanica, centra za snabdijevanje hranom i drugo, a takođe i izvori voda i kanalizacionih mreža, saobraćajni sektor (putevi, pruge, aerodromi i luke), telekomunikacije i izvori energije (struja, gas, benzin i drugo).

2.4. Prijetnje i rizici u kritičnoj infrastrukturi

S obzirom na činjenicu da ne postoji opšteprihvaćeno određenje pojma kritične infrastrukture, kao i na razlike u pogledu obima i sadržaja infrastrukture koja se smatra kritičnom, umnogome je otežan proces identifikacije oblika ugrožavanja kritične infrastrukture. To je uticalo i na to da se oblici ugrožavanja kritične infrastrukture mogu klasifikovati na različite načine. Evidentno je da se mnogi od njih međusobno prepliću, ili su kauzalno uslovljeni, što za posledicu ima da neke rizike nije moguće svrstati u samo jednu kategoriju. S druge strane, pojedini rizici se često ne mogu uklopiti u

[53] Boin R.A.: From Crisis to Disaster: Toward an Integrative Perspective, in: Perry R., Quarantelli E.L.(eds): *What is a Disaster? New Answers to Old Questions*, Xlibris Press, Philadelphia 2005, p. 163

[54] McConnell A.: Post-Crisis Reform and Learning in the Aftermath of the 1998 Sydney Water Crisis, Report Number: GOV2005-4, School of Economics and Political Science, Sydney University, 2005, dostupno na: http://www.econ.usyd.edu.au/13602.html.

ponuđene klasifikacione klase. Zbog nedostataka univerzalno važećih i nepromjenljivih kriterijuma klasifikacije, neophodno je stvaranje fleksibilnih kriterijuma, čija je promenljivost u direktnoj zavisnosti od konkretnih varijeteta i specifičnih prostornih i vremenskih činilaca, kao i faktora sredine[55]. I pored navedenog, kritična infrastruktura može biti izložena različitim prijetnjama koje moraju biti uključene kako u analizu rizika i prijetnji, tako i u izbor opcija za djelovanje (obuhvatanje svih opasnosti). Jedna od relevantnih i često upotrebljavanih podjela zasniva se na porijeklu oblika ugrožavanja kritične infrastrukture. Podjela na osnovu ovog kriterijuma obuhvata tri osnovne kategorije (Tabela br. 4).

PRIRODNE NEPOGODE	TEHNIČKI KVAR / LJUDSKA GREŠKA	TERORIZAM, KRIMINAL, RAT
ekstremni vremenski događaji, oluje, obilne padavine,pad temperature, poplave,toplotni talasi, suše	kvar sistema, nedovoljna ili pretjerana složenost, greške u planiranju, hardverske i (ili) softverske greške	terorizam
šumski požari	nepažnja	sabotaža
seizmički događaji	nesreće i vanredna stanja	ostali oblici kriminala
epidemije i pandemije ljudi, biljaka i životinja	greške u organizaciji, upravljanju krizama, neadekvatna koordinacija i saradnja	građanski ratovi i ratovi
kosmički događaji, energetske oluje, meteoriti i komete		

Tabela br. 4.: Oblici ugrožavanja kritične infrastrukture[56]

Proces klimatskih promjena u svijetu je ubrzan u poslednjih nekoliko decenija, u što su uključeni i globalni porast nivoa mora, te smanjenje polarnih ledenih površina. Globalne klimatske promjene su značajno povećale vjerovatnoću različitih ekstremnih vremenskih i klimatskih događaja. Tako su prosječne temperature vazduha na evropskom kontinentu u periodu od 2006. do 2015. godine bile za oko 1,5°C više u odnosu na predindustrijski period (druga polovina XIX vijeka), sa projekcijom rasta većeg od globalnog prosječnog povećanja temperature. Pored toga , Evropa je doživjela nekoliko ekstremnih ljetnih toplotnih talasa nakon 2003. godine, što je dovelo do povećanja stope smrtnosti i izazvalo negativne ekonomske efekte. U većem dijelu sjeverne Evrope zabilježeno je povećanje padavina, posebno tokom zime, uz smanjenje padavina tokom ljetnjeg perioda u južnoj Evropi. Takođe, kapacitet sniježnog pokrivača na sjevernoj hemisferi je značajno opao od 20-ih godina XX vijeka, sa drastičnim smanjenjem od 1980. godine. Toplotni talasi sličnog ili većeg intenziteta se očekuju u učestalim dvogodišnjim intervalima u drugoj polovini XXI vijeka, u uslovima scenarija pojačane emisije sunčevog zračenja.[57] U periodu od 1998. do 2009. godine, Evropa je pretrpjela neke od najvećih prirodnih katastrofa na globalnom nivou, uključujući zemljotrese u Izmiru (Turska), oluje Lotar i Kiril (zapadni i centralni i djelovi istočne Evrope) i široko rasprostranjene

[55] Keković Z., Savić S., Komazec N., Milošević M., Jovanović D.: *Procena rizika u zaštitilica, imovine i poslovanja*, Centar za analizu rizika i upravljanje krizama, Beograd, 2011, str. 107
[56] *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Ministry of the Interior, Federal Republic of Germany, 2009, p. 9
[57] Climate change, impacts and vulnerability in Europe 2016, An indicator-based report, p. 17

poplave u centralnim područjima kontinenta i Ujedinjenom Kraljevstvu. Pored navedenih katastrofa, značajne su bile i posledice poplava i klizišta 2005. godine u alpskom regionu, šumskih požara u Grčkoj i drugim djelovima jugoistočne Evrope u 2007. i 2009. godini, kao i suša na Pirinejskom poluostrvu 2005., 2006. i 2008. godine. Ukoliko se ove prirodne katastrofe posmatraju na nacionalnom nivou, uočljivo je da je njihova distribucija neujednačena, pošto su najčešće bile pogođene Turska (64 zabilježena događaja), Rumunija (58) i Francuska (56 događaja). Inače, većina prirodnih katastrofa u Evropi bila je uzrokovana poplavama i olujama[58].

Jedna od najvažnijih posledica klimatskih promjena je povećanje frekvencije i magnitude ekstremnih događaja kao što su poplave, suše, vjetrovi i toplotni talasi. Klimatske promjene takođe mogu izazivati i druge opasnosti kod kojih klima ili vremenski uslovi imaju suštinsku ulogu, kao što su sniježne lavine, klizišta i šumski požari. Kada je riječ o prirodnim katastrofama u Evropi nakon 1980. godine, 90% događaja i 80% ekonomskih gubitaka uzrokovano je hidrometeorološkim ili klimatološkim opasnostima. Ovaj zaključak se djelimično može povezati sa stanjem odsustva velikih geofizičkih opasnosti, kao što su katastrofalni zemljotresi ili vulkanske erupcije u Evropi, sa izuzecima na sjeveru (Island), jugu (Italija, Grčka) i istoku (Turska). U poređenju sa drugim kontinentima, veći dio Evrope ima relativno stabilnu geologiju, što ove pojave čini manje vjerovatnim. Iz svega navedenog evidentno je postojanje prirodnih nepogoda koje mogu ugroziti nesmetano funkcionisanje države i društva, kao i kritične infrastrukture. Međutim, u analizi i identifikaciji prirodnih oblika ugrožavanja ne treba isključiti ni mogućnost ugrožavanja prostora više država. (Tabela br.5).

država	**vrsta hazarda**							
	zemljotresi	poplave	klizišta	suše	ekstremne temperature	olujni vjetrovi	požari	epidemije
Albanija	+	+	+	+	+	+		+
BiH		+	+	+		+	+	+
Bugarska	+	+		+	+	+	+	
Mađarska[59]		+		+	+	+		+
Hrvatska	+	+		+	+	+	+	
Sjeverna Makedonija		+		+	+	+	+	+
Srbija	+	+			+	+	+	+
Crna Gora	+	+			+		+	+

Tabela br. 5.: Matrica prirodnih hazarda pojedinih država regiona[60]

Iako se prijetnje relevantne za operatore kritične infrastrukture mogu klasifikovati na više načina, terorizam se izdvaja kao očigledno namjerna prijetnja. Pritom teroristički napad nije uvijek

[58] *Mapping the impacts of natural hazards and technological accidents in Europe, An overview of the last decade*, European Environment Agency, Copenhagen, 2010, p. 25

[59] *Climate Change and Hungary: Mitigating the hazard and preparing for the impacts* (The "Vahava" report), Budapest, 2010

[60] *South Eastern Europe Disaster Risk Mitigation and Adaptation Initiative*, Risk Assessment for South Eastern Europe Desk Study Review, United Nations, Geneva, 2008, p. 42

osmišljen da uništi sam objekat, odnosno resurs kritične infrastrukture. On može biti planiran i tako da se posledice napada na kritičnu infrastrukturu koriste za ostvarivanje nekog šireg i dugoročnijeg cilja terorista. Uz to, jedna od najvažnijih karakteristika modernog terorizma je nepredvidivost mjesta i oblika napada, upotrebljenih sredstava i efekata koje on može izazvati. U tom smislu, teroristi mogu vršiti ubistva, otmice ljudi, vozila, i aviona. Pored toga, teroristi mogu izazivati strah slanjem eksplozivnih materija ili otrovnih hemikalija i bioloških sastojaka putem pošte. Imajući to u vidu, svaki od sistema klasifikovanih kao kritična infrastruktura može biti potencijalna meta terorističkog napada, premda ciljevi tih napada mogu biti različiti[61].

Jedan od primjera terorističkih prijetnji mogao bi biti napad na nuklearne elektrane, što bi rezultiralo ispuštanjem radijacije i drastičnim ugrožavanjem ljudi i životne sredine. Iako veća umreženost i integracija modernih upravljačkih sistema olakšava rad infrastrukture, time se takođe povećavaju rizici od neovlašćenih upada i ciljanih sajber napada. U takvim okolnostima prijetnje povezane sa sajber prostorom zahtijevaju posebnu pažnju operatora kritične energetske infrastrukture, naročito ako se imaju u vidu kaskadni efekti, dobro koordiniran sajber napad može izazvati daleko veću štetu od fizičkog napada. Pomenuta ranjivost čini kritičnu infrastrukturu potencijalno atraktivnom metom terorističkih napada, budući da teroristi imaju za cilj da naprave što veću štetu i privuku što veću pažnju javnosti, za razliku od kriminalaca čiji je fokus na profitu. Na primjer, zbog povezanosti sistema i domino efekata, sajber napadi na nuklearnu kritičnu energetsku infrastrukturu imaju veliki potencijal da izazovu dugotrajne prekide u proizvodnji i snabdijevanju strujom.[62]

Nacionalna kritična infrastruktura može biti neposredno ugrožena i iz sajber prostora. Sajber napadi bi mogli biti indirektni, na primjer uticajem na dostupnost informacionih servisa kroz blokiranje pristupa uslugama, ili direktni - napadom na nacionalnu elektroenergetsku mrežu. U slučaju takvih napada, štete i gubici nisu vezani samo za cjelovitost ili dostupnost izvora informacija, već i za pristup samim kritičnim uslugama. U ovom slučaju nisu u opasnosti isključivo informacije, niti njihovi pojedinačni korisnici, već interesi društva u cjelini. Dobar primjer takvih napada su sajber napadi u Estoniji 2007. godine[63].

Mreže sistema i infrastrukturnih elemenata su u ranijem periodu bile fizički i logički nezavisne i razdvojene, te su kao takve imale malu interakciju ili povezanost sa ostalim infrastrukturnim sektorima. Sa razvojem tehnologije, sistemi unutar svakog sektora postali su automatizovani i povezani međusobno putem računarskih i komunikacionih sredstava. Iako ovakva povezanost i automatizacija sistema i elemenata povećavaju efikasnost, oni ih takođe čine podložnijim prekidima i napadima. Dostignuti nivo međusobne povezanosti infrastrukture čini je ranjivijom na poremećaje. Incident koji bi u prošlosti bio izolovan, danas može prouzrokovati velike poremećaje zbog kaskadnih efekata.

---

[61] Bennett T. B.: *Understanding, Assessing, and Responding to Terrorism, Protecting Critical Infrastructure and Personnel*, John Wiley & Sons, Inc, 2018, p. 46

[62] *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, Organization for Security and Co-operation in Europe (OSCE), 2013, p. 28

[63] Solms von R., Niekerk van J.: From information security to cyber security, *Computers & Security,Vol 38*, International Federation for Information Processing, 2013, p. 100

Ozbiljnu prijetnju kritičnoj infrastrukturi predstavlja i organizovani kriminal, naročito za sektore finansija i komunikacija. Organizovane kriminalne grupe koje raspolažu specijalizovanim vještinama i djelovanjem, bilo da su povezane sa krađom, hakovanjem ili uskraćivanjem usluga vitalnim sistemima, postaju sasvim realna prijetnja društvu[64]. U okviru toga, meta ugrožavanja organizovanog sajber kriminala su sve češće bankovni računi građana i poslovnih subjekata, pri čemu se koristi paleta sve inovativnijih zlonamjernih kompjuterskih programa (virusa). Veoma razvijena industrija visokotehnološkog kriminala i crno tržište ključna su podrška kriminalnim organizacijama u ovoj oblasti. Međutim sve dok se rizikom može upravljati i dok su gubici uglavnom pokriveni sektorskim garancijama, povjerenje u informaciono- komunikacione tehnologije, a samim tim i u kritičnu informacionu infrastrukturu neće biti trajnije poljuljano. Osim direktnog finansiranja, organizovani kriminal u ovoj oblasti je danas u mogućnosti i da nudi iznajmljivanje „botneta" – zlonamjernog softvera koji se koristi za izvođenje kompjuterskih napada. Ostale kriminalne organizacije i grupe nedržavnog tipa (mogu biti povezane i sa državnim akterima) i individualni hakeri mogu unajmljivati takve mreže za izvođenje DDoS (Distributed Denial of Service Attack) napada na informacionu infrastrukturu, što uključuje kompjuterske viruse, krađu identiteta, slanje neželjenih poruka i drugo[65].

Pored navedenih rizika i prijetnji, postoji i posebna vrsta prijetnji kritičnoj infrastrukturi tehničke prirode. U tom smislu, efekti koje proizvode ove prijetnje na kritični infrastrukturni sistem ili njegove podsisteme mogu prouzrokovati neželjene događaje, što može dovesti do poremećaja, a u ekstremnim slučajevima i ozbiljnijih kvarova različitih podsistema. To se posebno odnosi na poremećaje funkcionalnih parametara koji uzrokuju pad performansi određenih elemenata. U takvim situacijama je pad performansi direktno proporcionalan intenzitetu vanredne situacije i stepenu otpornosti odgovarajućeg kritičnog infrastrukturnog elementa. Kvarovi na infrastrukturnom sistemu sami po sebi posledično proizvode negativne uticaje. Ovi uticaji se mogu širiti ne samo unutar kritičnog infrastrukturnog sistema (između zavisnih podsistema), već i izvan njega, nanoseći štetu društvu i nacionalnim interesima kao što su nacionalna bezbjednost, ekonomija i osnovne ljudske potrebe[66].

Na intenzitet i širenje uticaja kvarova na kritične infrastrukturne sisteme utiču različiti spoljni i unutrašnji faktori određenog sistema. Dok spoljni faktori uključuju naročito pripremljenost i otpornost okruženja, kao i opseg i trajanje vanredne situacije, glavni unutrašnji faktori uključuju vrstu i obim kvara unutar sistema. U tom kontekstu, tehnička i bezbjednosna pitanja stoje u osnovi svih aspekata međuzavisnosti i infrastrukturnog okruženja. Tehnologija je omogućila savremenu infrastrukturu i primarni je izvor međuzavisnosti. Napredak tehnologije, poput kompjuterizacije i automatizacije, povećao je efikasnost, pouzdanost i ponudu infrastrukture. Na vlasnicima i operatorima infrastrukture je da donose adekvatne poslovne odluke o nabavci i ugradnji nove tehnologije radi povećanja funkcionalnosti infrastrukture, proširivanja njenih mogućnosti i kapaciteta

[64] Marjanović M., Nađ I.: Assessment of threats to critical infrastructure facilities from serious and organized crime, In: Keković Z., Čaleta D., Kešetović Ž., Jeftić Z.*: National critical infrastructure protection regional perspective*, Faculty of Security Studies, Belgrade, 2013, p. 88

[65] Lopez J., Setola R., Wolthusen D. S.: *Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense*, Springer-Verlag Berlin Heidelberg 2012, p. 60

[66] Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, European Union,Council Directive 2008/114/EC of 8 December 2008

ili povećanja efikasnosti. Tehnologija je u najvećoj mjeri odgovorna za čvrsto povezanu, međuzavisnu infrastrukturu u kojoj danas uživamo, pri čemu je daleko odmakla automatizacija dramatično povećala sajber međuzavisnost u svim infrastrukturama i istovremeno je učinila znatno složenijom. Međutim, umreženost, složenost i velika međuzavisnost dovode i do povećanih rizika i povećanih zahtjeva za bezbjednost prilikom povezivanja podsistema i osiguranje njihove otpornosti[67].

Prirodu uticaja na kritičnu infrastrukturu karakteriše obim, struktura, intenzitet, trajanje i efekat vanrednih situacija. U svim takvim slučajevima se uticaji sa strukturalnog aspekta mogu klasifikovati kao direktni ili indirektni. Neposredni uticaj poremećenog podsistema na drugi podsistem ili direktno na društvo smatra se direktnim ili primarnim dejstvom. Suprotno tome, indirektni efekti uticaja dešavaju se kroz bilo koji kritični infrastrukturni podsistem, bez obzira da li utiču kao rezultat na neki drugi podsistem ili društvo. Indirektni efekti uticaji mogu biti sekundarni (kroz jedan podsistem) ili multi-strukturni (kroz nekoliko podsistema). Ostale važne karakteristike uticaja su njegov intenzitet i trajanje. Intenzitet uticaja zavisi od obima propusta u sektoru (tj. kako utiče na ostale sektore i nivoe sektorskih međuzavisnosti. Kada su međusobne veze slabe, intenzitet uticaja je nizak i uticaj na ostale sektore je samo djelimičan. Međutim, kada su te veze jake, intenzitet udara je visok i uticaj na ostale sektore može biti poražavajući (ili apsolutni). To ukazuje da intenzitet predstavlja važnu varijablu, čije trajanje može biti kratkoročno, srednjoročno ili dugoročno[68].

2.5. Zaštita kritične infrastrukture na nivou Evropske Unije

Kada je u pitanju zaštita kritične infrastrukture Evropska unija se može posmatrati kao jedan od značajnih faktora na međunarodnom planu. Naime, EU je pokretač mnogih inicijativa i programa u cilju adekvatne zaštite „evropske kritične infrastrukture“. Istorija evropskog razvoja u ovoj oblasti ima donekle sličnosti sa SAD-om jer su i u ovom slučaju teroristički napadi u Madridu 2004. i Londonu 2005. godine podstakli potrebu za evropskim pristupom na planu zaštite kritične infrastrukture. Pored toga, pretpostavlja se da je pitanje bezbjednosti kritične infrastrukture povezano i sa pojavom straha da bi se negativni efekti, uzrokovani prekidom ili nefunkcionisanjem kritične infrastrukture koja se nalazi u određenoj državi članici EU, mogli proširiti na druge susjedne zemlje. Kao primjer navedenom mogu poslužiti kompleksne infrastrukture poput energetskih mreža ili gasovoda, jer se nalaze na cijeloj teritoriji EU i imaju vitalne čvorove i kritična sredstva u različitim državama članicama. Istovremeno, druge infrastrukture koje spadaju u sektor transporta mogu se smatrati vitalnim za dvije ili više država članica, kao što su na primjer transnacionalni putevi i tuneli postavljeni na državnim granicama i slično[69].

Teroristički napadi na evropskom prostoru uticali su, između ostalog, da se terorizam posmatra kao prvi izvor prijetnji o kome se raspravljalo na nivou EU. Tako je u junu 2004. godine Evropski savjet zatražio od Evropske komisije da pripremi strategiju za zaštitu kritične infrastrukture.

---

[67] Rinaldi S.M., Peerenboom J.P., Kelly T.K.: Identifying, understanding and analyzing critical infrastructure interdependencies,*IEEE Control Systems Magazine*, 21(6), 2001, pp. 16-20, dostupno na: https://pdfs.semanticscholar.org/b1b7/d1e0bb39badc3592373427840a4039d9717d.pdf

[68] Rehak D., Markuci J., Hromada M., Barcova K.: Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system, *International Journal of Critical Infrastructure Protection*, 14, 2016 pp. 7-12

[69] Lazari A.: *European Critical Infrastructure Protection*, Springer, 2014, p. 45

Prva inicijativa koju je predložila Komisija pod nazivom "Zaštita kritične infrastrukture u borbi protiv terorizma"[70], ponudila je predloge i sugestije za jačanje sistema zaštite kritične infrastrukture u Evropi. Zaključci Evropskog vijeća o „Prevenciji, pripravnosti i odgovoru na teroristički napad", kao i „Program solidarnosti EU na posledice terorističkih prijetnji i napada"[71], koje je Vijeće usvojilo u decembru 2004. godine, još više su naglasili namjere Komisije da uspostavi „Evropski program za zaštitu kritične infrastrukture".

Kao rezultat napora u ovoj oblasti, Evropska komisija je predložila osnivanje Evropskog programa za zaštitu kritične infrastrukture (*European Programme on Critical Infrastructure Protection-EPCIP*). Program se sastoji od tri cjeline - Direktive za identifikaciju i imenovanje (ECI), Finansijskog programa i Informacione Mreže kritične infrastrukture (*Critical Infrastructure Warning Information Network -CIWIN*)[72]. Nakon izvještaja Komisije EU donijet je i Zeleni dokument o evropskom programu zaštite kritične infrastrukture (*Green Paper on a European Program for Critical Infrastructure Protection - Green Paper on EPCIP*). U ovom dokumentu data je i definicija zaštite kritične informacione infrastrukture, gdje se navodi da „svi programi i aktivnosti vlasnika, operatora, proizvođača i korisnika infrastrukture kao i regulatornih organa, koji za cilj imaju obezbjeđivanje kvalitetnog funkcionisanja, smanjenje štete i brz oporavak kritične informacione infrastrukture u slučaju kvarova ili napada na kritičnu informacionu infrastrukturu, predstavljaju zajedno program zaštite kritične informacione infrastrukture"[73]. Zaštita kritične informacione infrastrukture bi trebalo da se posmatra u kontekstu međusektorske povezanosti, s obzirom na to da prožima skoro sve ostale kritične sektore i trebalo bi da se koordiniše sa zaštitom svih ostalih kritičnih infrastrukturnih sektora.

Glavni zadatak predmetnog dokumenta je uključivanje što većeg broja zainteresovanih strana u izradu studije za uspostavljanje Evropskog programa za zaštitu kritične infrastrukture. Zato su u ovom dokumentu predstavljene mnoge mogućnosti u cilju dobijanja povratnih informacija o tome koja bi opcija bila poželjnija, a iz koje bi proistekla zajednička odluka. Misija, koja je postavljena još od početnih faza evropskog pristupa kritičnoj infrastrukturi, bila je da svim elementima kritične infrastrukture pruži adekvatan nivo zaštite, a posebno onima čiji neuspjeh može rezultirati najvećim uticajem na društveni život i bezbjednost država članica. U vezi sa tim, od posebnog značaja je da je predmetni dokument ustanovio principe koji treba da stoje u osnovi napora EU. Predlaže se da se jačanje kritične infrastrukture u EU postigne uspostavljanjem zajedničkog okvira koji sadrži zajedničke ciljeve, zajedničke metodologije (npr. najbolje prakse) i usklađene mehanizme praćenja. Neki od elemenata, koji bi bili dio zajedničkog okvira, uključuju između ostalog i:

- zajedničke principe zaštite kritične infrastrukture,
- zajedničke dogovorene (uspostavljene) standarde

---

[70] The Communication from the Commission to the Council and the European Parliament on "Critical Infrastructure Protection in the fight against terrorismdostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702

[71] *EU Solidarity Programme on the consequences of terrorism* dostupno na: http://www.consilium.europa.eu/uedocs/cmsUpload/15480EU_Solidarity_Programme.pdf

[72] Koubatis A., Schönberger J.Y.: Risk management of complex critical systems', *Journal of Critical Infrastructures*, Vol. 1, Nos. 2/3, 2001, pp. 195–215

[73] Commission of the European Communities, *Green Paper on a European Programme forCritical Infrastructure Protection* (Brussels, 17.11.2005.), COM(2005) 576 final, p. 19, dostupno na: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf

- zajedničke definicije na osnovu kojih se mogu dogovoriti specifične definicije sektora,
- zajedničku listu sektora kritične infrastrukture,
- prioritetne oblasti zaštite kritične infrastrukture,
- definisanje odgovornosti ključnih aktera,
- metodologiju za poređenje i određivanje prioriteta infrastrukture u različitim sektorima i drugo[74].

Predmetni dokument je posebno značajan jer u Aneksu II, definiše 11 kritičnih infrastrukturnih sektora, među kojima su i istraživanje svemira i civilna administracija (Tabela br. 6). Ovdje je važno napomenuti da se uprkos naporima u sprovođenju tako široke analize oblasti zaštite kritične infrastrukture, kasnije usvojena Direktiva Evropske komisije, fokusira isključivo na dva sektora, i to energiju i transport[75].

SEKTOR	PODSEKTORI
Energetika	proizvodnja nafte i gasa, rafinisanje, prerada i skladištenje uključujući i gasovode i naftovode; proizvodnja struje; transmisija struje, gasa i nafte; distribucija struje nafte i gasa
Informacione i komunikacione tehnologije	informacioni sistemi i mrežna zaštita; internet; pružanje usluga u oblasti fiksne telefonije; pružanje usluga u oblasti mobilne telefonije; radio komunikacija i navigacija; satelitska komunikacija
Voda	obezbjeđivanje i distribucija pijaće vode; kontrola kvaliteta vode; kontrola dostupnosti pijaće vode
Hrana	snabdijevanje hranom i očuvanje bezbjednosti i kvaliteta hrane
Zdravstvo	medicinska i bolnička njega; ljekovi, serumi, vakcine; bio-laboratorije; bio-agensi
Finansijski sistemi	službe isplate; vladine finansijske službe
Organi javnog reda i mira, javne bezbjednosti i sudstvo	očuvanje javnog reda, mira, bezbjednosti; sudska administracija
Civilna administracija	vladini organi; oružane snage; službe civilne administracije; službe za reagovanje u vanrednim situacijama; poštanske i kurirske službe
Saobraćaj i transport	drumski saobraćaj; željeznički saobraćaj; vazdušni saobraćaj; rečni saobraćaj; pomorski i okeanski saobraćaj i transport
Hemijska i nuklearna industrija	proizvodnja, skladištenje i prerada hemijskih i nuklearnih supstanci; cjevovodi za transport opasnih materija)
Istraživanje svemira	svemir, istraživanje

Tabela br.6.: Lista kritičnih sektora i podsektora EU[76]

[74] Lazari A.: *European Critical Infrastructure Protection*, Springer, 2014, p. 46

[75] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114

[76] Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM (2005) 576 final, p. 24, dostupno na:

Posebna specifičnost Unije je da veliki dio kritične infrastrukture posjeduje i njome upravlja privatni sektor. To je ujedno i razlog što je u svom izvještaju 574/2001 od 10. oktobra 2001. godine Komisija EU posebno naglasila da „jačanje i uvođenje određenih bezbjednosnih mjera radi prevencije napada usmjerenih na društvo u cjelosti mora biti sprovođeno od strane javnih organa država članica EU. Stoga je značaj javnog sektora u procesu zaštite kritične infrastrukture u okviru EU ogroman“.[77] Međutim, i pored toga problem zaštite kritične infrastrukture na nivou EU upotpunjuje problem pomoći među državama s obzirom da je ova oblast neposredno povezana sa nacionalnom bezbjednošću zbog čega državama nedostaje podjela informacija u ovoj sferi.

Za prostor EU posebno je značajna Direktiva iz 2008. godine[78], u kojoj su definisane procedure u cilju uspješnog identifikovanja i zaštitite kritične infrastrukture, a koje su obavezujuće za sve države članice. Obaveze država su da u skladu sa definisanim kriterijumima u sektoru energetike i saobraćaja identifikuju potencijalnu kritičnu infrastrukturu. To je ujedno i potreban uslov za utvrđivanje kritične infrastrukture na nivou EU, jer je na osnovu identifikovanja kritičnih sektora na nivou svake države članice, taj zadatak moguće izvršiti. Predmetna Direktiva navodi da „evropska kritična infrastruktura obuhvata objekte, sisteme ili djelove koji se nalaze u državama članicama EU, a koji su važni za održavanje vitalnih životnih funkcija, zdravstva, bezbjednosti, zaštite i ekonomskog ili socijalnog blagostanja ljudi, a čije narušavanje može imati katastrofalan uticaj na sve države članice“.[79] Pored navedenog, posebno je značajna odredba po kojoj je „kritična infrastruktura ona koja se nalazi u bilo kojoj državi članici EU, a čije bi narušavanje ugrozilo najmanje dvije države članice EU“, i „značaj ovakve kritične infrastrukture se procjenjuje na osnovu proučavanja efekata koji nastaju kao rezultat međusektorske zavisnosti od drugih infrastrukturnih sektora“[80]. Navedena odredba nedvosmisleno ukazuje da u okolnostima kada do narušavanja infrastrukture dođe u nacionalnom okviru, tada se ista ne smatra kritičnom za prostor EU.

2.5.1. Zaštita kritične informacione infrastrukture EU

Suočen sa sve većim brojem sajber napada na pojedince, kompanije i kritičnu infrastrukturu, diskurs EU je polako počeo da odražava ideju da društveno oslanjanje na tehnologiju predstavlja brzo rastući bezbjednosni rizik koji mora biti adekvatno riješen. Iako je Evropska unija odavno razvila aktivnosti u vezi sa računarskom bezbjednošću i elektronskim komunikacijama, tek je u poslednjoj deceniji donijela jasnu odluku da razvije potpuno nov pristup sajber bezbjednosti. Takav potez obilježen je donošenjem odgovarajućih zakonskih i organizacionih mjera, kao što su Okvirna odluka Savjeta iz 2005. godine o napadima na informacione sisteme, te stvaranje novih organizacionih infrastruktura, uključujući uspostavljanje Evropske agencije za bezbjednost mreža i informacija 2004.

---

https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf

[77] Critical Infrastructure Protection in the Fight againstTerrorism, Commission of the European Communities (Brussels, 20 October 2004), COM (2004) 702 final, p.4

[78] The identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Council Directive 2008/114/EC of 8 December 2008

[79] COUNCIL DIRECTIVE 2008/114/EC , article 2(a)

[80] COUNCIL DIRECTIVE 2008/114/EC , article 2(v)

godine i Evropskog centra za sajber kriminal pri Europolu 2013. godine. U središtu ovog novog područja politike Evropske unije nalazi se težnja ka institucionalnoj i koherentnoj politici, što se smatra ključnim za efikasan odgovor na sajber izazove sa kojima se Evropa trenutno suočava. Koherentnost je postala naročito važna u politici sajber bezbjednosti u EU, jer je dugo vremena njeno upravljanje bilo veoma raštrkano, pri čemu su relevantni akteri u ovoj oblasti radili nezavisno jedan od drugog[81] (Tabela br. 7).

Godina	NAZIV	KRATAK OPIS
2004	Evropski program zaštite kritične infrastrukture (EPCIP) (EC, 2004).	uspostavljanje osnovnih principa zaštite kritične infrastrukture EU.
2006	Saopštenje Komisije o EPCIP,COM (2006) 786 final (EC, 2006)	olakšavanje prenosa EPCIP na nacionalnom nivou.
2008	Direktiva 2008/114 za identifikovanje i označavanje evropske kritične infrastrukture i procjeni potrebe za njihovom zaštitom	omogućuje principe i postupke za razgraničenje kritične infrastrukture na nivou EU ili nacionalne kritične infrastrukture koja je prepoznata kao kritična infrastruktura na nivou EU.
2010	Štokholmski program - otvorena i sigurna Evropa služenje i zaštita građana, C 115/01	definisanje mape puta EU za pravdu, slobodu i bezbjednost.
2010	Saopštenje Komisije, Parlamenta i Savjeta EU o strategiji za unutrašnju bezbjednost: Pet koraka ka sigurnijoj Evropi, COM (2010) 673 final (EC, 2010)	identifikovanje i rešavanje zajedničke bezbjednosne prijetnje EU, kao što su nacionalne katastrofe, kriminalne mreže i radikalizam
PODRŽAVAJUĆA DOKUMENTA		
2012	Radni dokument Komisije o preispitivanju EPCIP SWD (2012) 190 final	sublimira rezultate EPCIP-a
2013	Radni dokument o novom pristupu EPCIP, 28.8.2013. SWD (2013) 318 final (EC, 2013)	institut novog pristupa za EPCIP organizovan oko tri stuba: prevencija, spremnost i reagovanje.

Tabela br. 7.: Ključne politike i pravni dokumenti koji čine okvir zaštite informacione infrastrukture EU[82]

Koncept zaštite kritične informacione infrastrukture prvi put je uveden u sistem strateške bezbjednosne politike EU 2003. godine. Motiv je bio priznanje da je sve prisutnija integracija

[81] Carrapico H., Barrinha A.: The EU as coherent (cyber) security actor? *Journal of Common Market Studies*, 55(6), 2017, p. 1259–1261,dostupno na:https://onlinelibrary.wiley.com/doi/epdf/10.1111/jcms.12575

[82] García Z. A., Jeun I.: *Best practices for Critical Information Infrastructure Protection (CIIP): experiences from Latin America and the Caribbean and selected countries*, Inter-American Development Bank, Washington, D.C., 2016, p. 9

tehnologije, između ostalih sektora, povećala evropsku zavisnost, a samim tim i ugroženost međusobno povezane infrastrukture u transportu, energetici i informacijama. Promjena bezbjednosne politike podrazumijevala je da države članice EU takođe moraju da u svojim nacionalnim politikama vode računa o ciljevima zaštite kritične informacione infrastrukture

Evropska komisija je 2008. godine ustanovila politiku u oblasti kritične komunikacije i zaštite kritične informacione infrastrukture. Osnovni zadatak ove politike je da obezbijedi odgovarajući nivo zaštite kritične informacione infrastrukture u Evropskoj uniji. To je samo dio znatno šireg evropskog programa u ovoj oblasti (*European Programme for Critical Infrastructure Protection - EPCIP*)[83], i nedvosmisleno upućuje na aktuelnost zaštite kritične infrastrukture kako u Evropi tako i u čitavom svijetu.

Razlog i potreba za izdvajanjem informacione infrastrukture leži u činjenici da je za adekvatno funkcionisanje skoro svih kritičnih infrastruktura neophodna bezbjednost odgovarajućih informacionih sistema. Realizaciju strategije koja se odnosi na ovaj sektor odobrio je Savjet EU, koji je i promovisao unapređenje pouzdanosti i otpornosti komunikacionih mreža informacionih sistema. Pored navedenog, Evropska Komisija je usvojila i saopštenje koje je posebno značajno s obzirom da sadrži osnovna načela u ovoj oblasti i akcioni plan u zaštiti kritične informacione infrastrukture. Ovim dokumentom je ukazano na potrebu razvoja, pripremljenosti i prevencije, otkrivanja i reakcije, minimizacije štete i oporavka, međunarodne saradnje i utvrđivanja kriterijuma za evropsku kritičnu infromacionu infrastrukturu[84]. U daljem normativnom uređenju ove oblasti posebno je značajna Rezoluciji Evropskog parlamenta o zaštiti kritične informacione infrastrukture[85].

Predmetnom Rezolucijom je ukazano na neophodnost definisanja minimalnih standarda za pripremljenost i reakciju na opstrukcije rada, incidente, pokušaje uništenja i napade na informacione sisteme kritičnih infrastruktura, i obezbjeđenje informisanja o rizicima i incidentima. To je ujedno bio i početak definisanja Strategije informacione bezbjednosti EU koja je usvojena 2013. godine[86].

Pomenuta strategija je usmjerena na poboljšanje otpornosti država članica i privatnog sektora na sajber prijetnje, i to podsticanjem većeg stepena saradnje svih uključenih aktera, većim ulaganjima u kapacitete nacionalnog i privatnog sektora da odgovori na napade, daljim razvojem sajber sposobnosti i povećanim angažmanom sa međunarodnim partnerima. Od tada je postignut napredak na političkom i zakonodavnom planu i na nivou sajber sposobnosti, pri čemu je politička dimenzija, sajber bezbjednosti postala jedan od najvažnijih prioriteta EU, s tim da su elementi sajber

---

[83] Program je dostupan na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786

[84] COMMISSION OF THE EUROPEAN COMMUNITIES COM(2009) 149 final Brussels, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection „Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience“, dostupno na: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[85] Critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI)), European Parliament resolution of 12 June 2012, dostupno na: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167

[86] Cybersecurity Strategy of the European Union: An Open, Safe and Secure CyberspaceBrussels, 7.2.2013 JOIN(2013) 1 final, dostupno na: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

bezbjednosti integrisani i u druge politike EU. U stategijskim prioritetima je pomenut i razvoj kapaciteta, ali i primjena osnovnih principa EU kao što su otvorenost i sloboda u sajber prostoru.[87]

Od posebnog značaja je EU Direktiva o mrežnoj i informacionoj bezbjednosti[88]. Direktivom su definisani najvažniji subjekti za obavljanje vitalnih ekonomskih i društvenih aktivnosti u oblastima energetike, saobraćaja, bankarstva, berzi i zdravstva kao operatora kritične infrastrukture. U kasnijoj je razradi došlo do proširenja predmetne definicije na finansijsko tržište, središta za razmjenu interneta, lance snabdijevanja hranom. Pored toga, naglašeno je da su direktivom obavezani samo oni operatori čiji su informacioni sistemi povezani sa njihovim ključnim uslugama i uvela je obaveze izveštavanja o incidentima vezanim za privatni sektor, uključujući operatore osnovnih digitalnih usluga. Direktiva ima posebna značaj jer se radi o obavezujućem dokumentu koji će biti implementiran u nacionalnim normativnim okvirima svih država članica. Države se pozivaju da propišu osnovne standarde bezbjednosti mreža i informacija koje bi definisali nadležni državni organi za ova pitanja, te da uspostave funkcionalni Nacionalni centar za prevenciju bezbjednosnih rizika u informaciono komunikacionim sistemima (*Computer Emergency Response Team-CERT*), uz definisanje nacionalne strategije i plana saradnje u ovoj oblasti. Direktiva upućuje na potrebu da na osnovu procjene rizika budu zasnovane odgovarajuće bezbjednosne mjere. Takođe se naglašava potreba standardizacije u cilju osiguranja zajedničke bezbjednosti na evropskom prostoru. Kao najvažnije tijelo određena je Evropska agencija za bezbjednost mreža i informacija (*European Network and Information Security Agency, ENISA*) koja treba da zajedno sa državama članicama razvije smjernice u tehničkoj oblasti kao i potrebnih standarda. Pored navedenog, Direktiva ima posebnu ulogu i u praćenju razvoja nacionalnih strategija. S druge strane, od država članica se očekuje da stalno prate napredak nacionalne sajber bezbjednosti i podnose godišnje izveštaje. Evropska komisija nakon primljenih izveštaja ima obavezu da ocijeni usaglašenost propisa i prakse članica sa oblastima djelovanja i ciljevima postavljenim i u drugim oblastima, kao što je Digitalna agenda EU[89].

Osnaživanje zaštite u ovoj oblasti u okviru EU je podstaknuto stvaranjem tokova finansiranja istraživanja i inovacija za sajber bezbjednost (600 miliona eura za period 2014.–2020. godine), daljim razvojem nacionalnih infrastruktura (na primjer, kako bi se osiguralo da svaka država članica ima centre za sajber bezbjednost) i uspostavljanjem javno-privatnih partnerstava čiji je cilj omogućavanje jedinstvenog digitalnog tržišta[90].

---

[87] European Commission, Communication from the Commission to the Council, theEuropean Parliament, the Economic and Social Committee and the Committee of the Regions *The European Security Agenda*. COM(2015)185 final, 2015, April 28

[88] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILconcerning measures to ensure a high common level of network and information security across the Union, Brussels, 7.2.2013 COM(2013) 48 final, dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

[89] Nedeljković S., Forca B.: Evropska strategija bezbednosti i sajber pretnje-značaj za Srbiju, *Vojno delo*, br. 3, MC Odbrana, Beograd, 2015, str. 145-146

[90] *EU Cybersecurity Initiatives-Working Towards a more Secure Online Environment. Factsheet*, European Commission. 2017, dostupno na: http://ec.europa.eu/information_society/newsroom/image/document/20173/factsheet_cybersecurity_update_january_2017_41543.pdf

S obzirom na značaj sajber bezbjednosti u funkcionisanju digitalnog tržišta, Strategija jedinstvenog digitalnog tržišta[91] predviđa i proces standardizacije. U vezi sa tim, predmetna strategija ukazuje na potrebu određenja nedostajućih tehnoloških standarda u razvoju digitalnog tržišta uključujući i standarde sajber bezbjednosti. U cilju uspostavljanja jedinstvenog digitalnog tržišta Akcioni plan predviđa i Plan prioritetnih standarda informaciono komunikacionih tehnologija. Pored navedenog, strategija otvara problem stvaranja ugovornog javno-privatnog partnerstva u oblasti sajber bezbjednosti. Navedeni problem je kasnije i razriješen posebnom Direktivom o stvaranju ugovornog javno-privatnog partnerstva za industrijsko istraživanje i inovacije u oblasti sajber bezbjednosti[92].

Takođe, i Evropski savjet je iskazao namjeru da nastavi sa napredovanjem u primjeni Strategije sajber bezbjednosti EU i u zajedničkoj politici EU u sajber bezbjednosti. Ova odluka uključuje proširenje uloge EU u ovoj oblasti i pojednostavljenje zajedničkog pristupa među državama članicama. Konkretno, EU planira da poboljša mandat ENISE, pretvarajući je u Agenciju za sajber bezbjednost EU, uz kreiranje sertifikata sajber bezbjednosti za proizvode, usluge i procese u cilju podrške jedinstvenom digitalnom tržištu.

2.5.2. Organizaciono- institucionalni aspekt zaštite kritične infrastrukture u Evropskoj Uniji

Direktiva Savjeta EU (2008/114/ES) apostrofira tri specifična zahtjeva koji vlasnici i operatori evropske kritične infrastrukture moraju da ispune. Prvi zahtjev predviđa da svaka definisana evropska kritična infrastruktura mora imati uspostavljen Plan zaštite operatora koji identifikuje kritične infrastrukturne resurse evropske kritične infrastrukture, kao i bezbjednosne mjere za zaštitu dotične infrastrukture. Predmetni plan treba da bude uspostavljen u roku od jedne godine nakon što je infrastruktura određena uz obavezu redovnog ažuriranja. Druga obaveza je da se napravi Procjena opasnosti. Treća obaveza koja proizlazi iz Direktive je da vlasnici i operatori određene evropske kritične infrastrukture moraju da imenuju oficire za vezu, zadužene za komunikaciju po pitanjima vezanim za bezbjednost između vlasnika (operatora) i nadležnog organa države članice. Pored toga, svaka država članica mora da uspostavi „mehanizam komunikacije“ između relevantnog organa države članice i oficira za vezu u cilju razmjene informacija, a u vezi sa identifikovanim rizicima i prijetnjama evropskoj kritičnoj infrastrukturi[93].

Sa aspekta upravljanja i praktične implementacija na nivou EU, zaštita evropske kritične infrastrukture predstavlja proces koji je podijeljen u faze identifikacije, određivanja i zaštite evropske kritične infrastrukture (Tabela br. 8).

---

[91] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *A Digital Single Market Strategy for Europe*. 6.5.2015. COM(2015) 192 final, dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN

[92] *The signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation.* Commission Decision of 5.7.2016.C(2016) 4400 final, dostupno na: https://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=3&year=2016&number=4400&version=ALL&language=en

[93] Lindstrom M.: The European Programme for Critical Infrastructure Protection, In: Olsson S. (ed.): *Crisis Management in the European Union, Cooperation in the Face of Emergencies*, Springer, 2009, p. 47

IDENTIFIKACIJA EVROPSKE KRITIČNE INFRASTRUKTURE	– Primjena sektorskih kriterijuma – Primjena unakrsnih kriterijuma – Primjena definicije kritične infrastrukture – Primjena prekograničnih elemenata – Identifikacija potencijalne kritičnu infrastrukture i prelazak na sledeću fazu
ODREĐIVANJE EVROPSKE KRITIČNE INFRASTRUKTURE	– Obavještavanje država članice na koje može uticati kritična infrastruktura – Uključivanje u bilateralne rasprave sa tim zemljama članicama – Dogovor sa državama članicama koje mogu biti pogođene – Određivanje kritične infrastrukture i prelazak na sledeću fazu
ZAŠTITA EVROPSKE KRITIČNE INFRASTRUKTURE	– Provjera postojanja i razvoj plana bezbjednosti operatora – Redovni pregled bezbjednosnog plana operatora – Provjera postojanja i razvoj službenika za bezbjednost – Izveštavanje Evropske komisije svake dvije godine o rizicima, prijetnjama i ugroženosti kritične infrastrukture

Tabela br. 8.: Faze upravljanja i regulisanja zaštite evropske kritične infrastrukture[94]

EU je posebno angažovana na optimizaciji zaštite i otpornosti četiri izabrane evropske kritične infrastrukture:

- Evropska organizacija za bezbjednost vazdušne navigacije (Eurocontrol)
- Galileo - globalna navigaciona infrastruktura pod civilnom kontrolom, koja se sastoji od 30 satelita povezanih sa zemaljskom infrastrukturom,
- mreža za prenos električne energije i
- mreža za prenos gasa[95].

Navedne kritične infrastrukture su izabrane na osnovu činjenica da se nalaze na teritoriji više od jedne države članice i da bi prekid u jednoj državi mogao uticati na nekoliko drugih država članica stvarajući domino efekat, da su po svojoj prirodi međusektorske (pokrivaju prevoz, svemirski i energetski sektor) kao i usled interesovanja operatora za povećanjem otpornosti kritične infrastrukture. To je ujedno predstavljalo nastojanje za stvaranje novog modela upravljanja i zaštite kritične infrastrukture u EU. Generalna direkcija za migracije i unutrašnji poslovi (*Directorate General for Migration and Home Affairs*)[96] je strukturna jedinica Evropske komisije koja upravlja politikama čiji je cilj da obezbijede sve potrebne aktivnosti ekonomskog, kulturnog i socijalnog rasta

[94] The Review of the European Programmefor Critical Infrastructure Protection(EPCIP).” Commission Staff Working Document,SWD(2012) 190 final. Commission of theEuropean Communities, EuropeanCommission, Brussels, 2012, r. 8, dostupno na: http://ccpic.mai.gov.ro/docs/epcip_swd_2012_190_final.pdf

[95] A New Approach to the European Programme for Critical Infrastructure Protection,Making European Critical Infrastructure More Secure.” Commission Staff Working Document,SWD(2013) 318 final, Commission of the European Communities, Brussels, 2013, pp.7-8, dostupno na: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisisand-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf.

[96] Izvor: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

EU. To je vodeći subjekt za formiranje plana zaštite kritične infrastrukture unutar evropske Komisije. U okviru Evropske komisije u istraživanjima u ovoj oblasti poseban značaj imao je Zajednički istraživački centar (*The Joint Research Center-JRC*), koji između ostalog, podržava procjene i analize i određivanja zaštite kritične infrastrukture. Kada se razmatraju nepredviđeni slučajevi i mjere ublažavanja velikih poremećaja u infrastrukturi, Evropska komisija takođe uključuje Generalni direktorat za humanitarnu pomoć i civilnu zaštitu (*Directorate General for Humanitarian Aid and Civil Protection-DG ECHO*) u cilju podrške dugoročnom oporavku kritičnih sektora i službi[97].
Međutim, da bi države EU pristupile implementaciji navedenih zakonskih odredbi i preporuka, bilo je neophodno da izrade nacionalnu listu identifikovanih kritičnih infrastruktura na svojoj teritoriji. Značajno je istraživanje koje je sprovedeno 2007. godine u kome je evidentirano, između ostalog, da su sektori koji se najčešće pojavljuju u nacionalni programima zaštite kritične infrastrukture: snabdijevanje energijom, informacioni i telekomunikacioni sistemi, snabdijevanje prehrambenim proizvodima, transportni i distributivni sistemi, finansije i bankarstvo, zdravstveni i socijalni sistemi i vodosnabdijevanje. To ukazuje da se većina država fokusira na zaštitu onih sektora koji se odnose na pružanje osnovnih društvenih usluga, a manje na zaštitu „simboličke“ infrastrukture kao što su nacionalni spomenici, a što je primjer prisutno u SAD-u, Australiji i Kanadi.

Kada se radi o identifikaciji nacionalnih kritičnih infrastruktura, ona je određena različitim nacionalnim i međunarodnim propisima. U okviru nacionalnog programa zaštite, svaka država članica EU mora da identifikuje „nacionalne kritične oblasti-sektore”, da evidentira i procjenjuje njihove sisteme ili komponente, kao i da evidentira i procjenjuje međuzavisnosti između identifikovanih kritičnih infrastruktura. Takođe, obaveza je država članica da razviju i(ili) ažuriraju plan bezbjednosti operatora i plan za vanredne situacije da bi zaštitili svoje nacionalne kritične infrastrukture[98].

2.5.3. Primjene odredbi EU u praksi – Njemačka i Francuska

U cilju potpunijeg razumijevanja navedenih odredbi kojima je EU uredila predmetnu oblast u narednom dijelu rada poslužićemo se primjerima Francuske i Njemačke koje imaju dugu tradiciju i razvijen normativni i organizacioni aspekt zaštite kritične infrastrukture. Francuska je jedna od prvih evropskih zemalja koja je kreirala i primjenjivala politiku identifikacije i zaštite kritične infrastrukture. Definisala je 12 vitalnih sektora koji su podijeljeni u tri glavne oblasti kako slijedi i to:

- državni sektori (javne službe, vojne operacije, pravosudne funkcije, svemir i istraživanje),
- sektori civilne zaštite (zdravstvo, upravljanje vodama, hrana) i

[97] García Z. A., Inkyung J.: *Best Practices for Critical Information Infrastructure Protection (CIIP): experiences from Latin America and the Caribbean and Selected Countries*, Inter-American Development Bank, Washington, 2016, pp.12-13

[98] Gritzalis D., Theocharidou M., Stergiopoulos G.: *Critical InfrastructureSecurity and ResilienceTheories, Methods, Tools and Technologies*, Springer, Switzerland, 2019, p. 18

– oblasti ekonomskog i društvenog života nacije (energija, elektronske komunikacije, audiovizuelni i informacioni sistemi, saobraćaj, ekonomija, industrija)[99].

Nacionalni pristup identifikovanja kritične infrastrukture dio je strategije nacionalne bezbjednosti, Vlada definiše spisak vitalnih operatora u kome je svaki operator povezan sa jednim kritičnim sektorom. Administrator svakog vitalnog operatora u obavezi je da:

– imenuje oficira za bezbjednost,
– izvrši procjenu rizika da bi identifikovao kritične aktivnosti (sisteme) u svojoj zoni odgovornosti i uspostavi Operativni plan bezbjednosti operatora) u cilju zaštite,
– identifikuje sredstva (sisteme) koji će biti predmet operativnog bezbjednosnog plana, koji će se sprovesti pod odgovornošću operatora, kao i eksterni plan zaštite koji sprovodi odgovorno javno tijelo[100].

U Njemačkoj je kritična infrastruktura definisana kao „organizacione i fizičke strukture i objekti koji su od vitalnog značaja za društvo i privredu države, a u slučaju njihovog nefunkcionisanja ili degradacije to bi rezultirao stalnim nedostatkom snabdijevanja, značajnim poremećajem javne bezbjednosti ili drugim dramatičnim posledicama“. Pri tome, devet sektora je prepoznato kao kritično na nacionalnom nivou i to:

– snabdijevanje energijom,
– informacione i komunikacione tehnologije,
– transport i logistika,
– snabdijevanje vodom i sistem otpadnih voda,
– javno zdravstvo (medicinske usluge)
– hrana,
– javna uprava (uključujući hitne i spasilačke službe),
– ekonomske usluge (finansije, osiguranje) i
– mediji i kulturni objekti (predmeti kulturne baštine).

Njemačka strategija zaštite kritične infrastrukture razlikuje kritičnost sistemske i simboličke prirode. Infrastruktura se smatra sistemski kritičnom kad god je zbog svog strukturalnog, funkcionalnog i tehničkog položaja u ukupnom sistemu infrastrukturnih sektora - izuzetno relevantna u pogledu međuzavisnosti. Primjeri su informacione i telekomunikacione infrastrukture u električnoj energiji, koje su s obzirom na veličinu i gustinu svojih mreža, od posebne važnosti i gdje veliki i dugotrajni prekidi rada mogu dovesti do ozbiljnih poremećaja u životu i procesima u zajednici, javne bezbjednosti i sigurnosti. Infrastruktura može imati i simboličku kritičnost, zbog svog kulturnog značaja ili njegove važne uloge u stvaranju osećaja identiteta, emocionalnog, ili psihološkog efekta na stanje nacije[101]. Iz navedene definicije i definisanih sektora, evidentno je da glavni fokus na poremećaju snabdijevanja i usluga. Interesantno je da infrastrukture u kojima se rukuje sa opasnim

[99] The Critical Infrastructure Protection in France. Secrétariat général de la défense et de la sécurité nationale (SGDSN). Retrieved from Secrétariat général de la défense et de la sécurité nationale, Paris, 2017, dostupno na: http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

[100] Gritzalis D., Theocharidou M., Stergiopoulos G.: *Critical Infrastructure Security and Resilience Theories, Methods, Tools and Technologies*, Springer, Switzerland, 2019, p. 28

[101] *National Strategy for Critical Infrastructure Protection*, Berlin 2009, p. 7

materijama, poput hemijske industrije i fabrika ili lokacija za nuklearni otpad se ne određuju u definiciji. To je posebno zanimljivo, jer neke evropske države imaju znatno šire određenje.

Njemačka je nacionalnu arhitekturu zaštite kritične infrastrukture zasnovala na identifikaciji šest radnih paketa koji odgovaraju različitim fazama ciklusa upravljanja rizikom. Javni sektor pod koordinacijom Federalnog ministarstva unutrašnjih poslova preuzima vodeću ulogu u sprovođenju prva četiri paketa uz saradnju sa privatnim sektorom (operatorima). U implementaciji petog i šestog paketa, uloge su obrnute, jer kompanije i operatori djeluju kao „vodeći subjekti". Radni paketi sadrže:

1. definisanje opštih ciljeva zaštite,
2. analiza prijetnji, ranjivosti i mogućnosti upravljanja,
3. procjena prijetnji koje su uključene,
4. specifikacija ciljeva zaštite, uzimajući u obzir postojeće proaktivne mjere, analiza postojećih propisa i prema potrebi identifikacija dodatnih mjera koje doprinose postizanju ciljeva,
5. sprovođenje mjera za postizanje ciljeva prvenstveno pomoću rešenja specifičnih za asocijaciju i unutrašnjih propisa, ugovora o samopomoći preduzeća i industrije i razvoja koncepata zaštite kompanija,
6. kontinuirani, intenzivni proces komunikacije o riziku (dijalog o nalazima analize, procjenama, ciljevima zaštite i opcijama akcije).

Njemački sistem predviđa brojne institucionalizovane platforme u koje su uključene javne vlasti, kompanije i udruženja. Ove platforme se prvenstveno posmatraju kao bezbjednosno partnerstvo i mogu biti organizovane kao okrugli stolovi od saveznog nivoa do zajedničkih između federacije i lokalne vlasti[102].

Pored navedenih razlika treba napomenuti da u okviru EU imamo i sličnosti kada se analiziraju subjekti zaštite kritične infrastrukture. Naime u svakoj državi je definisano centralno tijelo ili koordinacioni organ zadužen za zaštitu kritične infrastrukture. Iako se ova koordinaciona tijela razlikuju po prirodi, odgovornosti i političkom autoritetu, u nekim državama koordinirajuće tijelo, na primjer, ima sporednu ulogu dok u drugoj ima aktivnu ulogu u postavljanju standarda i ocjeni kriterijuma planova bezbjednosti. Pored toga, u nekim državama, koordinaciono tijelo je dio koji je odgovoran Ministarstvu unutrašnjih poslova ili Ministarstvu odbrane, mada postoje slučajevi da je to tijelo smješteno u nacionalnom centru za civilnu zaštitu. Najzad, različita ministarstva, odjeli i agencije imaju odgovornost da osiguraju zaštitu kritične infrastrukture u okviru podsektora za koje su odgovorni.

U Francuskoj je koordinacija zaštite kritične infrastrukture povjerena Generalnom sekretarijatu za odbranu i nacionalnu bezbjednost. Generalni sekretarijat odobrava smjernice o nacionalnoj bezbjednosti koje su izrađivala ministarstva u svakom kritičnom sektoru. S druge strane, ministarstva su takođe kontaktna tačka operatora i djeluju pod rukovodstvom Ministarstva unutrašnjih poslova kao sveukupnog koordinatora. Operatori imaju obavezu da imenuju delegata za odbranu i bezbjednost i izrade bezbjednosni plan operatora, koji utvrđuje politiku bezbjednosti operatora kao i specifične planove zaštite za svaku od identifikovanih „vitalnih tačaka". Zadatak kontrole je da utvrdi da li su nivoi bezbjednosti na vitalnim tačkama u skladu sa zahtjevima koji se

[102] *The protection of critical infrastructure against terrorist attacks: Compendium ofgood practices,* UN Office Counter-Terrorism, UN Counter-Terrorism Centre, 2018, p. 44-45

očekuju. U svim ovim aktivnostima savjetodavnu ulogu ima Međuministarski komitet za odbranu i bezbjednost kojim predsjedava generalni sekretar za odbranu i nacionalnu bezbjednost. U okviru kritične infrastrukture njegova uloga je imenovanje operatora od vitalnog značaja kao i kontrola bezbjednosnih planova operatora. Pored komiteta posebnu ulogu ima Regionalna komisija za odbranu i bezbjednost koja obavlja neposrednu kontrolnu funkciju u sprovođenju propisanih mjera zaštite kritične infrastrukture[103]. Značajno je napomenuti da kontrolni izveštaji imaju za cilj da istaknu ranjivost u odnosu na identifikovane prijetnje i preporuče preduzmanje mjera za jačanje otpornosti. U ekstremnim slučajevima nepoštovanja, kontrola ima mogućnost upućivanja odgovornih lica pravosudnom organu radi gonjenja i primjene krivičnih sankcija.[104]

Pored navedenih, u Francuskoj i drugi državni organi imaju nadležnost u okviru zaštite kritične infrastrukture. Tako, na primjer, Glavna uprava za bezbjednost informacionih sistema u okviru Generalnog sekretarijata za nacionalnu bezbjednost ima zadatak da omogući sigurnost informacionih sistema francuske države i stvori pouzdano okruženje za razvoj informacionog društva, da doprinese i interresornoj i međunarodnoj državnoj politici u pogledu informacione bezbjednosti, i da bude nacionalni regulatorni organ za sigurnost informacija izdavanjem odobrenja, garancija i sertifikata za nacionalne informacione sisteme, procese šifrovanja i drugo[105].

Nakon sajber napada na Estoniju 2007. godine, Francuska je shvatila da zaostaje za pojedinim državama (SAD, Velika Britanija i Nemačka) kada je riječ o bezbjednosti i odbrani. To je ujedno i početak popravljanja takvog stanja kroz usklađene napore za povećanje svoje nacionalne sajber i odbrambene sposobnosti i traženje efikasnije međunarodne saradnje i koordinacije, naročito sa Evropskom unijom i NATO-om. Zaštita informacione infrastrukture planirana je u okviru sajber-bezbjednosti i odbrane, pri čemu je Francuska to uradila na centralizovan način u skladu sa svojom istorijskom tradicijom. U zaštiti informacione infrastrukture posebno mjesto ima Nacionalna agencija za bezbjednost informacionih sistema kao najstarija agencija za kibernetsku i odbrambenu zaštitu u Francuskoj. S obzirom na važnost sajber bezbjednosti, Nacionalna agencija je pod direktnom nadležnošću premijera, tačnije ona je dio Generalnog sekretarijata za nacionalnu odbranu i bezbjednost. Zadaci ove agencije su višestruki od otkrivanja i primjena ranih mjera na sajber napade, podrške razvoju pouzdanih proizvoda i usluga državnih institucija i ekonomskih aktera, preko savjetodavnih i podrške državnim institucijama i operatorima vitalne infrastrukture, do podizanja nivoa svijesti o sajber prijetnjama. Sama agencija je podijeljena u četiri uprave (pod-direkcije):

- operativni centar za sigurnost informacionih sistema koji je odgovoran za analizu prijetnji, identifikaciju ranjivosti, reagovanje na aktuelne sajber napade, dizajniranje protivmjera i pomoć u njihovom rešavanju,
- stručna uprava koja je odgovorna za održavanje naučne i tehnološke opremljenosti agencije,

[103] INSTRUCTION GENERALE INTERMINISTERIELLE RELATIVE A LA SECURITE DES ACTIVITES D'IMPORTANCE VITALE N°6600/SGDSN/PSE/PSN du 7 janvier 2014, SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE, dostupno na: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf

[104] The protection of critical infrastructure against terrorist attacks: Compendium of good practices, UN Office Counter-Terrorism, UN Counter-Terrorism Centre, 2018, pp. 43-44

[105] Brunner M. E., Suter M.: *International CIIP Handbook 2008 / 2009, an inventory of 25 national and 7 international critical information infrastructure protection policies*, Center for Security Studies, Zurich, 2008, p. 151

- uprava za bezbjednost informacionih sistema koja osmišljava, predlaže i isporučuje bezbjednosne informacione sisteme državnim institucijama i operatorima od vitalnog značaja,
- uprava za spoljne odnose i koordinaciju koja koordinira između Nacionalne agencije i državnih institucija, poslovnog sektora, međunarodnih partnera i javnosti[106].

Za Francusku je karakteristično da Bijela knjiga odbrane iz 2013. godine, kao i Zakon o vojnom planiranju za period 2014.-2019. godine, predviđaju posebne zakone o standardima za sajber bezbjednost, odvojeno za državne mreže i privatne operatore od vitalnog značaja. Francuska broji preko 200 operatora od ključnog značaja, koji su Zakonom o odbrani definisani kao „javni ili privatni operatori koji eksploatišu ili koriste instalacije ili objekte čija nedostupnost može ozbiljno ugroziti ratnu sposobnost ili ekonomske mogućnosti, bezbjednost ili opstanak nacije".

Pored navedene agencije, u ovom domenu su posebno značajni francusko ministarstvo odbrane i Minstarstvo za unutrašnje poslove. Ministarstvo odbrane razvija i upravlja složenim informaciono-komunikacionim sistemima, posebno onima koji se odnose na najsofisticiranija oružja, poput nuklearnog arsenala zemlje. Ministarstvo posjeduje sopstvenu strukturu za sajber bezbjednost i odbranu i ostvaruje saradnju sa Nacionalnom agencijom i drugim ministarstvima koja su zadužena za sajber bezbjednost. Kada je riječ o Ministarstvu unutrašnjih poslova, nekoliko organizacionih cjelina je fokusirano na borbu protiv sajber prijetnji. Najvažniji među njima su Generalni direktorat unutrašnjih snaga bezbjednosti; Generalni direktorat Nacionalne policije koji u svom sastavu ima Upravu za borbu protiv sajber kriminala i Generalni direktorat Nacionalne žandarmerije sa Centrom za borbu protiv digitalnog kriminala.[107].

Suočeno sa rastućim sajber prijetnjama, Ministarstvo unutrašnjih poslova je uspostavilo poziciju „sajber prefekta", u cilju ostvarivanja zajedničkih napora u unapređenju sajber bezbjednosti. „Sajber prefekt" je u stalnom kontaktu i koordinaciji sa svim djelovima MUP-a zaduženim za pojedine aspekte sajber bezbjednosti i odbrane, kao i sa nadležnima iz drugih ministarstava. Njegova primarna misija je poboljšanje institucionalnog uređenja MUP-a na prijetnje sajber-mreži naročito kroz organizacioni aspekt[108].

U Njemačkoj je početak razvoja koncepta kritične infrastrukture vezan za 1997. godinu, kada je Savezno ministarstvo unutrašnjih poslova pokrenulo međuministarsku radnu grupu za kritičnu infrastrukturu koju su činili predstavnici ministara, upravni odbor i Federalni ured za informacionu bezbjednost. Zadatak radne grupe bio je da odredi moguće scenarije prijetnji nacionalnoj kritičnoj infrastrukturi, sprovede analizu ranjivosti ključnih nacionalnih sektora, predloži kontramjere i odredi sistem ranog upozoravanja. Nakon niza internih sektorskih studija o kritičnoj infrastrukturi, vlada je konačno predstavila Nacionalni plan zaštite informacione infrastrukture, kao i osnovni koncept za fizičku zaštitu kritične infrastrukture[109].

Za razliku od Francuske, Njemačka je nacionalni koncept zaštite kritične infrastrukture razvijala u saradnji i koordinaciji između Federalnog ministarstva unutrašnjih poslova, Savezne

---

[106] *Agence nationale de la sécurité des systèmes d'information*, dostupno na: https://www.ssi.gouv.fr/en/

[107] Vitel P., Bliddal H.: French Cyber Security and Defence: an overview, *Information & Security: An International Journal*, vol.32, 2015, pp. 9-10, dostupno na: https://it4sec.org/system/files/3209_france.pdf

[108] Cybersecurity: the Government's strategy, *Government France*, dostupno na:https://www.gouvernement.fr/en/cybersecurity-the-government-s-strategy

[109] Schallbruch M., Skierka I.: *Cybersecurity in Germany*, Springer Briefs, 2018, pp. 17-18

kancelarije za civilnu zaštitu i pomoć u katastrofama, Savezne agencije kriminalističke policije i privatnim bezbjednosnim kompanijama. S obzirom na činjenicu da je oko četiri petine kritične infrastrukture u Njemačkoj u privatnim rukama, posebno se potencira zajednički rad svih subjekata. Navedeno, posebno dolazi do izražaja ako se uzmu u obzir da brojne i raznovrsne usluge javne infrastrukture koje se obezbjeđuju na nivou lokalne uprave, sve češće pružaju kompanije iz privatnog sektora[110].

Okvir za zaštitu kritične infrastrukture u Njemačkoj postavljen je kroz niz dokumenata različitog karaktera. Primarni značaj ima Zakon o civilnoj zaštiti i pomoći u katastrofama donesen 2009. godine, koji daje mandat Civilnoj zaštiti na nacionalnom nivou. Predmetnim zakonom su između ostalog definisani zadaci Savezne kancelarije za civilnu zaštitu i pomoć u nepogodama u okviru sistema civilne zaštite. Osnovna karakteristika ovog sistema je njegovo snažno organizovanje zajedno sa principom supsidijarnosti, davanjem kompetencija lokalnom i regionalnom nivou (pokrajine/savezna država)[111].

Savezna kancelarija za civilnu zaštitu i pomoć u katastrofama osnovana je 2004. godine u okviru Saveznog ministarstva unutrašnjih poslova. Rad Kancelarije obuhvata obaveze i zadatke u domenu civilne zaštite, planiranje i pripremu mjera za obezbjeđenje hitnih potreba, sprovođenje planiranja i pripreme saradnje između Federacije i drugih država u pogledu posebnih opasnosti, kao i planiranje prevencije zaštite kritične infrastrukture[112]. Kancelarija je odgovorna i za podsticanje aktivnosti operatora kritične infrastrukture u smislu da proaktivno obezbjeđuju kritičnu infrastrukturu i pripremaju efikasne planove za upravljanje krizama. Pored toga, Nacionalna strategija za zaštitu kritične infrastrukture uključuje saveznu i lokalne samouprave u cilju poboljšanja primjene zaštite kritične infrastrukture u svojim oblastima odgovornosti. Državna uprava je odgovorna da obezbijedi bezbjednost svojih građana, što se u njemačkom Osnovnom ustavnom zakonu izražava kao pravo na život i fizički integritet. S druge strane, država ne mora da obezbijedi sve potrebne robe i usluge, ali mora da omogući trećim licima (kompanijama) da to urade. U segmentima u kojima država ne preuzima na sebe zadatke, ona postavlja zakone i okvire za potrebne usluge. Takođe, javna vlast i posebno Ured zaštite i pomoći u slučaju katastrofa imaju aktivnu ulogu u zaštiti kritične infrastrukture, (npr. predstavljanje scenarija prijetnji od kojih treba zaštititi infrastrukturu), uključujući i podršku drugim akterima u skladu sa pravnim i strateškim okvirom. Federalni ured i Federalno ministarstvo unutrašnjih poslova, izdaju smjernice i na različite načine podržavaju druge aktere, tako da uspješnost i integracija prevencije, spremnosti, reakcije na incidente i oporavka predstavljaju garanciju efikasnosti upravljanja rizicima i krizama[113].

Kada se radi o informacionoj infrastrukturi, Njemačka je 2016. godine usvojila novu Nacionalnu strategiju sajber bezbjednosti[114] kojom su definisani strateški ciljevi, sredstva i postupci.

---

[110] Brunner E. M., and Suter M.*: International CIIP handbook 2008/2009*, Center for Security Studies, Zurich, 2008, p. 163

[111] Eismann C.: Trends in critical infrastructure protection in Germany, *Safety Engineering Series*, Vol. IX, No. 2, Technical university of Ostrava, 2014, pp. 27-28

[112] Federal Office of Civil Protection and Disaster Assistance (BBK), dostupno na:https://www.bbk.bund.de/EN/Home/home_node.html

[113] Eismann C.: Trends in critical infrastructure protection in Germany, *Safety Engineering Series*, Vol. IX, No. 2, Technical university of Ostrava, 2014, pp. 27-28

[114] Cyber-Sicherheitsstrategie für Deutschland 2016, dostupno na: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html

Predmetna strategija predstavlja proizvod zajedničkog rada Ministarstva unutrašnjih poslova, Ministarstva odbrane i Saveznog ministarstvaza spoljnih poslova.

U funkcionisanju i zaštiti informacione infrastrukture poseban značaj ima Federalni ured za informacionu bezbjednost, koji ima opšti zadatak promovisanja bezbjednosti informacionih tehnologija. Ured ima funkciju centralnog organa za sajber bezbjednost u Njemačkoj, iako nema policijska i obaveštajna ovlašćenja, ali što se tiče sajber prostora, on ispunjava i policijske i obavještajne funkcije. Misija Ureda može se na vrlo pojednostavljen način podijeliti u tri oblasti:

- uspostavljanje i pregled proizvoda i sistema bezbjednosti,
- nadzor nad primjenom mjera sajber bezbjednosti i
- operativna sajber odbrana[115].

Istorijski gledano, Ured je obavljao zadatke vezane za kripto uređaje kojima se štite državne tajne, ali se njegova kompetencija sukcesivno proširila i na čitavo područje kritične infrastrukture. S druge strane privatni operatori infrastrukture moraju da zaštite svoje relevantne informacione sisteme od sajber-napada u skladu sa najsavremenijim rešenjima što moraju i da dokažu Uredu. Pri tome ako mjere bezbjednosti nisu dovoljne, Ured može da podnese žalbe i izrekne novčanu kaznu. Paralelno sa nadležnostima koje se tiču bezbjednosti kritične infrastrukture, Njemačka je takođe delegirala izvršna ovlašćenja za digitalne usluge (mrežna tržišta, pretraživače i drugo) u skladu sa Direktivom Evropske mreže i bezbjednosti informacija. Pored toga, od 2015. godine Ured je uključen u sajber odbranu operatora kritične infrastrukture, koji pored ostalog imaju obavezu prijavljivanja incidenata u sajber-bezbjednosti, a za zauzvrat dobijaju pomoć u informacijama u cilju zaštite informacione infrastrukture. Pored navedenih subjekata, treba pomenuti i Federalnu kriminalističku policiju, koja ima ulogu osnovne jedinice njemačke policije koja prikuplja i obrađuje informacije na nacionalnom nivou. Shodno tome, ta služba objavljuje i godišnje savezne izveštaje o stanju sajber kriminala. Uz to, Federalna kriminalistička policija ima ovlašćenja za sajber bezbjednost. U praksi, nadležna tužilaštva joj povjeravaju istražne postupke u ovoj oblasti, iako su zakonske mogućnosti istraga Federalne kriminalističke policije u sajber-prostoru još uvek dosta ograničene. Naime, nova istražna ovlašćenja, poput praćenja telekomunikacija i tajnog pristupa informatičkim sistemima (tj. onlajn pretraga), koja su dobijena 2017. godine, mogu se koristiti samo za određena krivična djela, kao što je sajber napad ako je u kontekstu špijunaže[116].

Sa Saveznom kancelarijom za zaštitu ustava i kancelarijama za zaštitu saveznih država, Njemačka ima 17 domaćih obavještajnih službi. Federalna kancelarija za zaštitu ustava uglavnom se bavi istragom desničarskog i lijevog ekstremizma, ekstremizma stranaca i terorizma. Međutim, njihova odgovornost za kontraobavještajnu pomoć takođe igra važnu ulogu u oblasti sajber bezbjednosti. Naime, Kancelarija ima specijalizovanu grupu za suprotstavljanje elektronskim napadima. Neke pokrajine, poput bavarske, su takođe postavile specijalizovane organizacione jedinice u svojim ustavnim agencijama za zaštitu. Svojim Centrom za sajber-alijansu osnovanom posebno za ovu svrhu, bavarski Državni ured za zaštitu Ustava zadužen je za odbranu od sajber napada i na privatni sektor. U kontekstu sajber bezbjednosti u kritičnim infrastrukturama, nadzorne agencije osnovane za svaki sektor takođe imaju svoju ulogu. Neki infrastrukturni sektori u principu podležu saveznom nadzoru, kao što su snabdijevanje energijom, telekomunikacije ili finansije, dok

[115] Schallbruch M., Skierka I.: *Cybersecurity in Germany*, Springer Briefs, 2018, p. 32
[116] Schallbruch M., Skierka I.: *Cybersecurity in Germany*, Springer Briefs, 2018, p. 32

vlasti pokrajina u velikoj mjeri nadgledaju druge sektore kao što su zdravstvena zaštita, opskrba hranom ili transport. Svi sektorski nadzorni organi su također odgovorni za pravilno funkcionisanje infrastrukturnih sektora[117].

Kao što je evidentno, zaštita kritičnih infrastruktura je veoma decentralizovana u različitim državama članicama EU. Pored toga, u svakoj državi, značajan dio kritične infrastrukture je u vlasništvu privatnog sektora, zbog čega je potreba za saradnjom između vlasnika i operatora infrastrukture s jedne strane i vlade, s druge strane, priznata od strane svih vladinih zvaničnika. Međutim, nivo i vrsta uključenosti privatnog sektora u zaštiti kritične infrastrukture se razlikuju. Dok su u nekim državama predstavnici privatnog sektora aktivno i sistematski uključeni u razvoj politika, privatni sektor u drugim zemljama je pozvan na *ad hoc* osnovi, a njegove uloge i aktivnosti uglavnom su ograničene na implementaciju minimalnih standarda zaštite koji su postavljeni od strane javnog sektora[118].

2.5.4. Saradnja EU i NATO u zaštiti kritične infrastrukture

U cilju potpunijeg razumijevanja evropske zaštite kritične infrastrukture neophodno je dati i kratak osvrt na ulogu koju ima NATO u ovoj oblasti. Ciljevi bezbjednosne saradnje između EU i NATO-a se poklapaju, a to se zasniva ne samo na činjenici da su 23 države istovremeno članice i EU i NATO-a, već i na njihovoj namjeri da međusobno recipročno popune postojeće praznine u bezbjednosnim sposobnostima. NATO od svog osnivanja reguliše i strogo štiti svoju kritičnu infrastrukturu. U aktivnostima NATO-a, u kojima učestvuju sve države Evroatlantskog savjeta za partnerstvo, zaštita kritične infrastrukture bila je glavni fokus planiranja. Međunarodno partnerstvo pojednostavljuje dijeljenje relevantnih informacija o potencijalnim izvorima prijetnji i njihovim mogućim uticajima, pripremi procjena i razmjeni iskustava, stečenih lekcija i neophodnih osnova za rad na zaštiti kritične infrastrukture.

Inače sam pojam „zaštita kritične infrastrukture“ je nakon terorističkih napada 11. septembra 2001. godine dobio svoje mjesto u planovima NATO-a. Nakon navedenog terorisitičkog napada, samit NATO-a u Pragu pokrenuo je „Akcioni plan za civilne vanredne situacije“, u vezi s čim je predložen spisak svih raspoloživih nacionalnih resursa, kao i nacrt okvira za pomoć. Pored toga, planirane su vježbe za testiranje i eventualno poboljšanje interoperabilnosti. Istovremeno je objavljen „Akcioni plan za borbu protiv terorizma“. Teroristički napad u SAD uticao je i na ispitivanje spremnosti država članica u oblastima zaštite kritične infrastrukture (planiranje i popis infrastrukture). Rezultat je bio dokument „Koncept zaštite kritične infrastrukture“ pripremljen od strane Višeg Komiteta za civilno planiranje vanrednih situacija (*Senior Civil Emergency Planning Committee-SCEPC*). Ključni ciljevi sumirani su u razmjeni informacija između učesnika, pomoći i razvoju programa obuke i obrazovanja koji doprinose identifikaciji kritične infrastrukture, određivanju istraživanja kao podrške zaštiti kritične infrastrukture i drugo.[119]

---

[117] Ibidem, pp. 32-33

[118] Lindstrom M.: The European Programme for Critical Infrastructure Protection, In: Olsson S. (ed.): *Crisis Management in the European Union, Cooperation in the Face of Emergencies*, Springer, 2009, pp. 40-45

[119] Babos T.: The First Critical Infrastructure Protection Research Project in Hungary in: Nádai L., Padányi J.(ed): *Critical Infrastructure Protection Research, Results of the First Critical InfrastructureProtection Research Project in Hungary*, Springer, Switzerland,2016, pp. 9-10

U događajima koji su uslijedili narednih godina, terorističkih napada u Madridu u martu 2004. godine, sajber-napadu na Estoniju 2007. godine, rusko-gruzijskom sukobu 2008. godine, napadima pirata od 2008. godine u Persijskom zalivu i na obalama Somalije, a i tokom rusko-ukrajinskog konflikta, NATO je u kontinuitetu imao značajnu ulogu. NATO operacije u poslednjoj deceniji jasno pokazuju da ta organizacija preuzima odgovornost, ima operativne planove i ako je potrebno umiješa se i u slučajeve kada procijeni da su ugroženi njeni interesi - bilo da su to pomorski pravci, vazdušni koridori, gasovodi, telekomunikacione ili komunikacione mreže, čak i kada su napadnuti izvan teroitorija država članica, pa i na strateškoj udaljenosti[120].

Danas se može reći da NATO nije ostao samo na konceptualnim i strateškim dokumentima o zaštiti kritičnih infrastruktura, već ima svoju politiku i praksu i na operativnom nivou. U Evropi je saradnja kapaciteta i procedura EU i NATO-a posebna prilika za sve nacionalne partnere, kako javne službe, tako i privatne kompanije. To omogućava da se posebna pažnja posveti sertifikaciji osoblja i opreme, kako za zaštitu kritične infrastrukture u unutrašnjoj bezbjednosti, tako i za ekspedicione snage. Vojne operacije u inostranstvu podjednako su zavisne od kritične infrastrukture, mada se koriste i druga sredstva zaštite, budući da je očuvanje pravaca snabdijevanja i komunikacionih linija od presudnog značaja za uspjeh prekograničnih operacija[121].

Sa aspekta zaštite kritične infrastrukture za NATO je posebno značaja samit u Rigi 2006. godine, kada su šefovi država i vlada NATO-a potvrdili ulogu Alijanse u zaštiti kritične infrastrukture, naglašavajući „odlučnost da zaštite stanovništvo, teritorije, infrastrukturu i snage od posledica terorističkih napada, kao i da bezbjednosni interesi Alijanse mogu biti ugroženi prekidom protoka vitalnih resursa“. Samit u Rigi bio je odraz novog razumijevanja vitalnih interesa NATO-a, jer se usredsredio na bezbjednost infrastrukture koja je kritična za energiju, a ne na druge dimenzije energetske bezbjednosti. NATO od svojih članica zahtijeva brz razvoj fizičkih i tehničkih resursa energetske infrastrukture koja štiti mrežu među saveznicima. Čelnici NATO-a su prepoznali neophodne aspekte energetske bezbjednosti između ostalog i na samitu u Lisabonu u novembru 2010. godine, na kome su identifikovali pet ključnih oblasti u kojima NATO može da pruži dodatnu vrijednost:

- fuzija i dijeljenje informacija i obavještajnih podataka,
- projektna stabilnost,
- unapređenje međunarodne i regionalne saradnje,
- podrška upravljanju posledicama i
- podrška zaštiti kritične infrastrukture.

NATO bi mogao poslužiti kao snažna platforma za razvoj takvih aktivnosti za odbranu od energetskih prijetnji, a takođe bi mogao biti važan element za razmjenu informacija i najboljih praksi,

[120] *ISAF's Mission, NATO and Afghanistan*, North Atlantic Treaty Organization, dostupno na www.globalresearch.ca/rendition-and-the-global-war-on-terrorism-28-nations-have-supported-theus-in-the-detention-and-torture-of-suspects/18419

[121] Smedts B.: *NATO's Critical Infrastructure Protection and Cyber Defense*, Royal High Institutefor Defense Center for Security and Defense Studies, Brussels, 2010, p. 27.

podizanje svijesti i usklađivanje pristupa saveznika u zaštiti kritične infrastrukture, kao i za pružanje savjeta i obuke za poboljšanje spremnosti i izgradnju otpornosti[122].

NATO je prvi put raspravljao o sajber odbrani na samitu u Pragu 2002. godine. Na samitu u Velsu 2014. godine, NATO je odobrio unaprijeđenu politiku sajber odbrane i odgovarajući akcioni plan za njeno sprovođenje. Ovom politikom definisane su aktivnosti Alijanse u oblastima obrazovanja, obuke i vježbi. Suprotstavljanje sajber prijetnjama je uvedeno po članu 5 Sporazuma, što je veoma važna odluka, jer sajber-napad na jednu zemlju ima uticaj na kompletan NATO[123].

Na samitu u Varšavi 2016. godine, Alijansa se fokusirala na jačanje sajber odbrane nacionalnih mreža i industrije. Istovremeno, potvrđen je mandat NATO-a za operacije u sajber prostoru, kojim se one izjednačavaju sa drugim oblastima operacija - kopnom, vazduhom i morima. Na samitu u Briselu[124] 2018. godine, sajber napadi su uvršteni među glavne hibridne prijetnje, pri čemu je NATO iskazao potrebu da se operacije sajber odbrane dovedu do nivoa operacija u ostale tri oblasti, kako u ukupnoj koordinaciji Saveza, tako i u okviru odvojenih grupa saveznika.

Sjevernoatlantski savjet sprovodi sveukupnu primjenu NATO politika sajber bezbjednosti, pri čemu Odbor za sajber bezbjednost upravlja ovom politikom. Na operativnom nivou, NATO Upravni odbor za sajber odbranu odgovoran je za koordinaciju aktivnosti na sajber odbrani između različitih NATO institucija i zemalja članica. Ovo tijelo uključuje visoke političke, vojne, operativne i tehničke organe Saveza, koji su odgovorni za sajber odbranu. NATO takođe ima Odbor za konsultacije, kontrolu i komandu NATO-a i druga tijela odgovorna za različita pitanja sajber-odbrane.Operativna tijela Saveza u oblasti sajber bezbjednosti su:

- Operativni centar za sajber prostor, uspostavljen deklaracijom na samitu u Briselu 2018. godine,
- NATO centar za reakcije na računarskena incidente - obavlja zadatke zaštite NATO mreža i pružanja centralizovane podrške savezničkim računarskim resursima i
- NATO sajber timovi za brzo reagovanje, koji su stalno spremni pomoći saveznicima[125].

Pored navedenih organizacija djeluje i zajednički NATO centar za sajber odbranu koji je osnovan 2008. godine u Estoniji (Talin), koji realizuje istraživanja, obuku i vježbe u sajber bezbjednosti. Odluke NATO-a i njegovih tijela ukazuju da koncept „sajber bezbjednosti“ primorava Alijansu da konstantno proširuje domete djelovanja i suzbijanja sajber prijetnji. Da bi se postigla povećana saradnja s industrijom i privatnim sektorom razvijen je i implementiran NATO program za sajber partnerstvo. U isto vrijeme, NATO razvija blisku saradnju sa EU i partnerskim zemljama, jer je i za NATO i za EU sajber bezbjednost strateško pitanje koje utiče na bezbjednost i odbranu država članica i samih organizacija. I NATO i EU daju prioritet otpornosti i odbrani sopstvenih mreža, organizacija i misija, a ostavljaju sajber bezbjednost pojedinačnih članica u domenu nacionalne odgovornosti. Njihove misije su komplementarne, pri čemu se NATO fokusirao na

[122] Caşın H.M.: Understanding NATO's New CIP Policies: Common Efforts and Solidarity, In: Gluschke G., Casin H.M., Macori M.(eds): *Cyber security policies and critical infrastructure protection*, Institute for Security and Safety, Germany, 2018, p. 315

[123] *Press conference, by NATO Secretary General Jens Stoltenberg ahead of the meeting of NATO Defence Ministers*, 2017, dostupno na: https://www.nato.int/cps/en/natohq/opinions_145415.htm?selectedLocale=en

[124] *Brussels Summit Declaration,* dostupno na: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=uk

[125]*Ukraine – EU – NATO Cooperationfor Countering Hybrid Threats in the Cyber Sphere*, Centre for Global Studies "Strategy XXI" Kyiv, 2019, p. 8

bezbjednosne i odbrambene aspekte sajber bezbjednosti, dok se EU bavi širim, uglavnom nevojnim rasponom sajber mreže i pitanjima sloboda i upravljanje internetom, mrežnih prava i zaštite podataka sa aspekta interne zaštite.

2.6. Zaštita kritične infrastrukture u pojedinim državama

Istočno, egipatsko, grčko i rimsko carstvo podjednako su štitile svoje glavne transportne mreže, puteve za snabdijevanje hranom, materijalne resurse i držale ih u tajnosti. Unapređenje kvaliteta zaštite nacionalne kritične infrastrukture vezuje se za 1648. godinu i Vestfalski mirovni ugovor sa uspostavljanjem nacionalnih država, koje su na raspolaganje dobile potrebne strukture u obliku državnih sistema, pri čemu su stvorile strukturu i mehanizme slične današnjim[126]. Tadašnje države su se bavile svojim kritičnim sistemima na sličan način kao danas i branile ih sredstvima koje su imale na raspolaganju. Kada je riječ o današnjoj zaštiti kritične infrastrukture, ona se može posmatrati kao proizvod dva svetska rata i hladnog rata.

Potrebno je istaći da ne postoji jedinstveni, unaprijed utvrđeni institucionalni model, koji ukazuje kako država treba da štiti svoju kritičnu infrastrukturu. Od vlada država se očekuje da odaberu okvir koji najbolje odgovara njihovim karakteristikama u pogledu prijetnji, veličine i strukture njihovih ekonomija, kao i njihove kulture javnih politika i ustaljenih institucionalnih praksi. Sa aspekta upravljanja kritičnom infrastrukturom posebno treba uzeti u obzir osnovnu ustavnu strukturu države. U vezi sa tim, od posebnog je značaja da li se radi o unitarnim centralizovanim ili federalnim decentralizovanim državama, jer je to od ključne važnosti u određivanju uloga i odgovornosti na različitim nivoima vlasti.

U savremenoj praksi, arhitektura kritične infrastrukture obično varira između dva osnovna modela. Jedan od modela upravljanja kritičnom infrastrukturom zasniva se na principima samoregulacije, podsticaja i dobrovoljnog poštovanja. To je takozvani „dobrovoljni pristup“ kao proizvod politike koja je fokusirana na neobavezujućim smjernicama. Prema ovom modelu, sve zainteresovane strane (bez obzira da li su iz javnog ili privatnog sektora) podstiču se da doprinose definisanju i primjeni politike zaštite kritične infrastrukture putem preporuka, dogovaranja i stvaranja zajedničke percepcije za ostvarivanje zajedničkog cilja. Obvezujuća snaga zakonodavnih i regulatornih odnosa koristi se samo kao dopunsko sredstvo, osim u određenim sektorima (kao što je nuklearni sektor) gjde imaju glavnu ulogu.

Drugi model je takozvani „mandatni pristup“, zasnovan na ideji da će se saradnja na polju zaštite kritične infrastrukture najbolje postići uspostavljanjem obavezujućih pravnih okvira praćenih sankcijama za operatore kritične infrastrukture koji ne udovoljavaju traženim standardima u okviru zadatih rokova. U stvarnosti, države ne slijede navedene pristupe u njihovim „čistim“ oblicima, već usvajaju elemente i jednog i drugog modela. Njihovi se sistemi mogu definisati samo kao pretežno „dobrovoljni“ ili „mandatni“. Primjeri prvih su SAD, Velika Britanija, Kanada i Švajcarska, a drugih Francuska, Španija, Belgija i Estonija.[127]

---

[126] Babos T.:*The Five Central Pillars of European Security*, NATO Public Diplomacy Division, Brussels, 2007, p. 14.
[127] Setola R., Luiijf E., Theocharidou M.: Critical Infrastructures, Protection and Resilience, In: Setola R., Rosato V., Kyriakides E., Rome, E. (eds): *Managing the Complexity of Critical Infrastructures*, Springer Nature Switzerland AG, Basel, 2019, pp. 7-12.

Za države poseban izazov predstavlja izbor najboljeg modela koji odgovara nacionalnim potrebama. To je posebno značajno prilikom uspostavljanja modela, jer se mogu usvojiti strukture i procesi koje se u praksi pokažu neodgovarajućim ili neadekvatnim. Iz tog razloga, države često uspostavljaju mehanizme kojima se osigurava da se politike i strategije u ovoj oblasti povremeno podvrgavaju reviziji. SAD je primjer države koja je počela sa čistim konceptom dobrovoljnog učešća operatora kritične infrastrukture u tom procesu. Međutim, vremenom je uočena potreba za jačanjem pravnog okvira za zaštitu kritične infrastrukture.

I pored teškoća u generalizaciji, možemo uočiti jedan trend arhitekture kritične infrastrukture država. Uobičajeno je da se u centru zaštite nacionalne kritične infrastrukture nalazi vladina agencija koja ima ulogu koordinatora u definisanju i sprovođenju nacionalnog strateškog pristupa zaštiti kritične infrastrukture. Države obično dodjeljuju odgovornost za određeni sektor pojedinim ministarstvima na osnovu utvrđene stručnosti i kompetencije (npr. bezbjednost hrane ministarstvima poljoprivrede, zdravstvo ministarstvima zdravlja i slično) i definiše obim i modalitete interakcije između uključenih vladinih agencija i operatora kritične infrastrukture.

Percepcija kritične informacione infrastrukture varira među državama u skladu sa njenim prioritetima i uticajem. U većini slučajeva, ovaj značajan segment infrastrukture je jedan od ciljeva nacionalne strategije za sajber-bezbjednost radi bolje koordinacije javnog i privatnog sektora. U manjem obimu kritična informaciona infrastruktura nije dio nacionalne strategije sajber bezbjednosti, već samostalno područje politike[128].

Na osnovu navedenog, a u cilju objektivnog i metodološki korektnog upoređivanja u narednom dijelu rada analiziraćemo zaštitu kritične infrastrukture u Holandiji, Republici Sloveniji i Republici Slovačkoj. Pri izboru navedenih država rukovodili smo se određenim opštim karakteristikama Crne Gore. Prema površini teritorije i broju stanovnika Crna Gora spada u grupu malih evropskih država, sa izlaskom na more. Njena bliska prošlost vezana je za bivšu SFRJ, dok je u aktuelnom trenutku Crna Gora članica NATO saveza i nalazi se na putu da postane punopravna članica Evropske unije.

2.6.1. Zaštita kritične infrastrukture u Holandiji

U Holandiji se zaštita kritične infrastrukture sve više doživljava kao ključno pitanje nacionalne bezbjednosti. Od kraja 1990-ih uloženo je mnogo napora za bolje upravljanje zaštitom kritične infrastrukture. Prve inicijative i politike bile su usmjerene na bezbjednost informacija uopšte, jer nije postojala jasna definicija kritične infrastrukture. To se promijenilo projektom zaštite kritične infrastrukture, koji je započet 2001. godine i koji je formulisao politiku zaštite u toj oblasti[129]. Najvažnije je bilo utvrditi od čega se sastoji holandska nacionalna kritična infrastruktura i odrediti šta je „kritično“, što je predstavljalo problem jer je nedostajalo jasno određenje onoga što je „kritično“ za društvo. Nacionalna kritična infrastruktura Holandije danas obuhvata „proizvode, usluge i prateće

[128] Critical Information Infrastructures Protection approaches in EU, p. 17, dostupno na: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf

[129] Voeller G. J.: *Wiley handbook of science and technology for homeland security*, John Wiley & Sons, Hoboken, New Jersey, 2010, p. 794

procese koji, u slučaju prekida rada ili neuspjeha, mogu da izazovu velike socijalne nemire.“ Procjena je i da bi prekid njihovog rada doveo do velikog broja žrtava i velike ekonomske štete“.[130]

Holandija je 2002. godine definisala da nacionalna kritična infrastruktura obuhvata 11 sektora i 31 kritični proizvod i uslugu, a od aprila 2004. godine, lista je sadržavala 12 kritičnih sektora i 33 kritična proizvoda i usluge. Infrastrukture se smatraju kritičnim ako predstavljaju ključnu, neophodnu uslugu za društvo i ako bi njihov poremećaj brzo doveo do vanrednog stanja ili bi dugoročno mogao imati štetne efekte na društvo[131].

Novi integrisani pristup zaštite kritične infrastrukture Holandija je uspostavila u maju 2015. godine kao dio Nacionalne strategije bezbjednosti, koju je razvilo holandsko Ministarstvo bezbjednosti i pravde. Navedena reforma nacionalne kritične infrastrukture je dovela do preokreta, od „kritičnih sektora“ do „kritičnih procesa“. U vezi sa tim, kritični procesi su oni koji mogu dovesti do ozbiljnih društvenih poremećaja u slučaju njihovog neuspjeha ili poremećaja. Pošto nisu svi procesi u sektoru kritični, fokus je na kritičnim procesima umjesto na kritičnim sektorima. Prepoznavanje kritičnog procesa omogućava adekvatnu upotrebu resursa na efikasniji i ciljani način. Procjena nivoa kritičnosti vrši se na osnovu utvrđenih kriterijuma uticaja, kao što su ekonomska šteta i fizičke posledice. Kriterijumi su razvijeni na osnovu procesa nacionalne procjene rizika. Stepen kritičnosti zavisi od posledica neuspjeha identifikovanih kritičnih sektora. Napravljena je razlika između kategorije A, gdje poremećaji mogu imati veliki uticaj i kaskadne efekte i kategorije B, gdje uticaji mogu biti niži, kako bi se odrazila raznolikost unutar kritične infrastrukture i odredili prioriteti. Razlika između kategorija kritičnosti A i B može biti od pomoći u određivanju prioriteta incidenata i omogućava prilagođavanje rešenja i mjera za povećanje otpornosti (Tabela br. 9).

KATEGORIJA A	KATEGORIJA B
nacionalni transport i distribucija električne energije	regionalna distribucija električne energije i gasa
proizvodnja prirodnog gasa	upravljanje avio saobraćajem
zalihe nafte	upravljanje pomorskom i unutrašnjom plovidbom
skladištenje, proizvodnja ili prerada nuklearnih materijala	skladištenje, proizvodnja ili prerada petrohemijskih resursa velikih razmjera
snabdijevanje vodom za piće	finansijski sektor (bankarske usluge, elektronski transferi između banaka i između banaka i javnosti)
vodoprivreda	komunikacija sa hitnim službama i između njih
	mobilizacija policije
	vladine usluge koje zavise od pouzdanih, dostupnih digitalnih informacija i sistema podataka

Tabela br.9.: Podjela kritične infrastrukture Holandije[132]

[130] Hämmerli B.: *Protecting critical infrastructure in the EU, Task Force Report*, Centre for European Policy Studies, Brussels, 2010, p. 22

[131] Voeller G. J.: *Wiley handbook of science and technology for homeland security*, John Wiley & Sons, Hoboken, New Jersey, 2010, p. 795

[132] Castellon N., Frinking E.: *Securing Critical Infrastructures inthe Netherlands: Towards a National Testbe*, Hague 2015, p. 9

U Holandiji postoji nekoliko kritičnih procesa čije nefunkcionisanje ili poremećaj u kratkom vremenskom roku mogu imati destabilizujuće posledice za društvo. To se prvenstveno odnosi, na energiju (nacionalna i regionalna distribucija električne energije, proizvodnje gasa i nacionalnog transporta i regionalna distribucija gasa, snabdijevanja naftom), informaciono-komunikacione tehnologije i telekomunikacije (Internet i data servisi, pristup Internetu i saobraćaj podataka, govorne usluge i SMS - mobilne i fiksne mreže), satelit-vrijeme i GPS (pozicioniranja sateliti), pijaću vodu (snabdijevanje pitkom vodom), finansijski sektor (transakcije na malo, finansijske transakcije potrošača, transakcije velike vrijednosti između banaka, trgovina hartijama od vrijednosti) i vode (odbrana voda i upravljanje)[133].

Mnogo aktera je uključeno u zaštitu kritične infrastrukture u Holandiji, ali primarnu odgovornost za kontinuitet i otpornost kritičnih procesa snose stvarni operatori. To uključuje sticanje uvida u prijetnje, ranjivosti i rizike, kao i razvoj i održavanje kapaciteta koji povećavaju i čuvaju otpornost kritičnih procesa. Nadležno ministarstvo uspostavlja opšte okvire za sektore koji spadaju u njegovu nadležnost (u politici ili u zakonima i propisima). Ministarstva, u saradnji sa operatorima kritičnih procesa, odgovorna su za očuvanje i inspekciju sposobnosti povezanih sa kritičnom infrastrukturom. Pored toga, i regionalne organizacije pružaju podršku operatorima kritičnih procesa u slučaju neposrednog poremećaja ili nefunkcionisanja, a u skladu sa svojim mogućnostima. To se odvija u koordinaciji sa operatorima kritičnih procesa i ministarstvima. Činjenica da postoji mnogo različitih interesnih grupa upućuje na potrebu koordinacije i upravljanja. Nacionalni koordinator za bezbjednost i protivterorizam u okviru Ministarstva pravde i bezbjednosti odgovoran je za upravljanje i obezbjeđenje zajedničkih mjera za sve učesnike u cilju povećanja otpornosti[134]. Odgovornost za zaštitu kritične infrastrukture je podijeljena među subjektima, što uključuje i javni i privatni sektor. Na primjer, u zaštitu kritične infrastrukture uključena su ministarstva ekonomskih poslova, saobraćaja, javnih radova i vodoprivrede, zdravlja, zaštite i sporta, kao i Generalna obaveštajna i bezbjednosna služba, koja je odgovorna za zaštitu informacione sigurnosti[135].

Kada se razmatra zaštita kritične informacione infrastrukture, Holandija je dugo unapređivala i ovaj segment. Tako je 2001. godine usvojila Nacionalni plan za obezbjeđivanje telekomunikacija u slučaju nastanka nepredvidivih situacija u tom sektoru. Predmetni plan je dorađivan, a 2006. godine je zamijenjen Nacionalnom platformom za konsultacije, kada je istovremeno osnovan i Strateški odbor za zaštitu kritične infrastrukture. To tijelo čine predstavnici svih kritičnih sektora, koji se sastaju dva do tri puta godišnje i razmatraju aktuelna pitanja iz ovog domena. Pored toga, Holandija je usvojila i Nacionalnu strategiju sajber bezbjednosti. Strategija se između ostalog zasniva i na identifikaciji kritičnih sistema, usluga i procesa koji zavise od informaciono-komunikacionih tehnologija i uspostavljenih osnovnih bezbjednosnih zahtjeva na osnovu analiza rizika. Najvažniji

[133] *National Risk Profile 2016, An All Hazard overview of potential disasters and threats in the Netherlands, The National Network of Safety and Security Analysts*, National Institute for Public Health and the Environment The Netherlands, 2016, p. 93

[134] *Resilient critical infrastructure*, National Coordinator for Security and Counterterrorism Ministry of Justice and Security, dostupno na: https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf

[135] Vidriková D., Boc K., Dvořák Z., Řehák D.: *Critical Infrastructure and Integrated Protection*, The Association of Fire and Safety Engineering, Ostrava, Czech Republic, 2017, pp. 28-29

razlozi za uvođenje nove strategije ticali su se potrebe efikasnijeg reagovanja vladinih tijela i privatnih organizacija na rastuće digitalne prijetnje u Holandiji, kao i unapređenja saradnje, te razvijanja odgovarajućih kapaciteta i resursa[136]. U okviru zaštite kritične infrastrukture, Vlada, radeći sa vitalnim operatorima, identifikuje kritične sisteme, usluge i procese koji zavise od informaciono-komunikacionih tehnologija. Ovi napori povezani su sa programom koji na osnovu analize rizika utiče na uspostavljanje osnovnih bezbjednosnih zahtjeva.

Uloge i odgovornosti u području sajber bezbjednosti u Holandiji podijeljene su između brojnih aktera, uključujući ministarstva holandske vlade i aktere iz privatnog sektora. Nacionalna strategija identifikuje više od dvadeset tijela sa individualnim i kolektivnim odgovornostima za dostizanje ciljeva sajber bezbjednosti koji su postavljeni Strategijom. Na nivou države, u ova tijela spadaju ministarstva bezbjednosti i pravde, odbrane, spoljnih i unutrašnjih poslova, ekonomskih pitanja i istraživanja, obrazovanja i nauke. Kada je riječ o državnim agencijama, definisani su zadaci i odgovornosti službi za sprovođenje zakona i unutrašnju bezbjednost (Policijska služba, Javna tužilaštvo, Inspektorat bezbjednosti i Obaveštajno-bezbjednosna služba) kao i Agencije za zaštitu podataka, sektorskih regulatornih tijela (na primjer za telekomunikacije) i Centralne banke. Takođe, u to su uključene i regionalne i lokalne vlasti. U privatnom sektoru najveći dio odgovornosti pada na finansijski sektor (komercijalne banke, Holandsko bankarsko udruženje i Platforma elektronske trgovine Holandije), posebno na pružaoce vitalnih usluga, dok određene odgovornosti zahtijevaju uključivanje poslovne zajednice uopšte. Akademija nauka je takođe uključena preko holandske Organizacije za naučno istraživanje i kroz vladino finansiranje nezavisnih istraživačkih tijela, kao što je Holandska organizacija za primijenjena naučna istraživanja[137].

2.6.2. Zaštita kritične infrastrukture u Republici Sloveniji

Za Republiku Sloveniju kritična infrastruktura od nacionalnog značaja uključuje sposobnosti i usluge od ključnog značaja za državu i čija bi disfunkcija ili uništavanje imali ozbiljan i značajan uticaj na nacionalnu bezbjednost, ekonomiju, suštinske funkcije društva, zdravstvo, bezbjednost i zaštitu kao i socijalnu zaštitu. U skladu sa osnovnim i sektorskim kriterijumima koji se koriste za identifikaciju kritične infrastrukture od nacionalnog značaja, nadležna ministarstva su identifikovala i dala obrazloženje za postojeću kritičnu infrastrukturu Republike Slovenije. Vladinom odlukom naložena je obaveza nosilaca kritične infrastrukture od nacionalnog značaja da razviju odgovarajuće mjere zaštite[138].

Vlada Republike Slovenije je Odlukom iz 2017. godine utvrdila kritičnu infrastrukturu od nacionalnog značaja. Identifikovano je 9 kritičnih infrastrukturnih sektora, njihove funkcije i zadaci, te je formiran spisak ministarstava, organizacija, agencija i drugih državnih i privatnih udruženja koje su odgovorne za funkcionisanje i zaštitu kritične infrastrukture[139].

---

[136] *The National Cyber Security Agenda*, Ministry of Justice and Security, 2018, dostupno na:https://www.enisa.europa.eu/news/member-states/new-national-cyber-security-agenda-published-by-the-netherlands

[137] Kaska K.: *National Cyber Security Organisation: the Netherlands*, NATO Cooperative Cyber Defence Centre of Excellence Tallinn, 2015, p. 10

[138] Republic of Slovenia's, Ministry of defence, dostupno na: http://www.mo.gov.si/en/areas_of_work/critical_infrastructure/

[139] Zakon o kritični infrastrukturi (ZKI), *Uradni list RS*, št. 75/2017

Analiza svih kritičnih sektora ukazuje na njihovu veliku povezanost, što posebno dolazi do izražaja kada su u pitanju sektori saobraćaja i transporta, energetike, informacionih i komunikacionih tehnologija, finansija, vode i hrane. Međusektorski kriterijumi za identifikaciju kritične infrastrukture definisani su na osnovu procjene potencijalnih posledica, ozbiljnosti kvarova ili poremećaja kritične infrastrukture za sve sektore kritične infrastrukture. Pri tome su zakonom posebno određeni parametri koji definišu poremećaje kritične infrastrukture kao što su broj žrtava (broj mrtvih ili povrijeđenih), ekonomski uticaj (potencijalni ekonomski gubici) i uticaj na širu javnost kao što su povjerenje javnog mnjenja, fizičke patnje i poremećaj pružanja osnovnih usluga. Zakonom je posebno definisano da nacionalna kritična infrastruktura „sadrži one objekte koji su od vitalnog značaja za zemlju i koji bi u slučaju prekida rada uzrokovali ozbiljne posledice ponacionalnu bezbjednost, ekonomiju i druge ključne društvene funkcije“.[140]

Pored toga određeno je da je nacionalna kritičnih infrastruktura dio evropske kritične infrastrukture i da njena zaštita podleže propisima koji regulišu evropsku kritičnu infrastrukturu. Najvažniji subjekti u zaštiti kritične infrastrukture su: Vlada, Ministarstvo odbrane, nosioci najvažnijih infrastrukturnih sektora, državni organi koji sarađuju sa nosiocima ključnih infrastrukturnih sektora u obavljanju svojih zadataka, Nacionalni centar za upravljanje krizama i Inspektorat odbrane. Ovoj grupi pripadaju i vlasnici i/ili menadžeri objekata i resursa kritične infrastrukture kao što su: kompanije, institucije, javni i bankarski sektor Slovenije. Vlada Slovenije utvrđuje kritičnu infrastrukturu i određuje menadžere kritičnih infrastruktura koji izrađuju i čuvaju planska dokumenta. Ministarstvo odbrane usmjerava i koordinira aktivnosti u identifikovanju i zaštiti kritičnih infrastruktura u Sloveniji. Inspektorat nadležan za odbranu vrši kontrolu sprovođenja zaštite kritične infrastrukture. Vlada Republike Slovenije i nadležni organi su u obavezi da donesu podzakonska akata koja će detaljno definisati ključne faktore u oblasti zaštite kritičnih infrastruktura[141]. U tom cilju je Vlada Slovenije posebnim aktom odredila nosioce kritičnih infrastrukturnih sektora Republike Slovenije i državnih organa koji međusobno sarađuju[142].

U identifikaciji kritične infrastrukture Republika Slovenija ima izrađene kriterijume koji obuhvataju i njihove granične vrijednosti i prioritete za rad kritičnih infrastrukturnih sektora[143]. Posebno su razrađeni osnovni kriterijumi koji se koriste za utvrđivanje kritične infrastrukture kao i sektorski kriterijumi. Tako je, na primjer, za sektor zdravstvene zaštite definisana situacija u kojoj je onemogućeno pružanje hitnih medicinskih usluga i medicinske zaštite više od nedelju dana na području sa preko 100.000 stanovnika, a slični kriterijumi su utvrđeni i za sektor snabdijevanja pitkom vodom i sektor prehrane. Kada se radi o sektoru informacione komunikacije kriterijum identifikovanja kritične infrastrukture obuhvata nefunkcionisanje sredstava elektronske komunikacije, mreža i usluga koje su neophodne za rad sistema nacionalne bezbjednosti, energetskog sistema i finansijskog sistema više od šest sati.

---

[140] Zakon o kritični infrastrukturi (ZKI), *Uradni list RS*, št. 75/2017, čl.3

[141] Trbojević M.: Zaštita kritičnih infrastruktura-iskustva tranzicionih zemalja, *Politička revija*, br. 2, Beograd, 2018, str. 107-108

[142] Sklep o določitvi nosilcev sektorjev kritične infrastrukture Republike Slovenije in z njimi sodelujočih državnih organov, *Vlada Republike Slovrenije, št. 80200-1/2018/*, dostupno na: http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/zki/SprejetoBesediloAkta_Nosilci_sektorjev_KI.pdf

[143] *Sklep o določitvi kriterijev za ugotavljanje kritične infrastrukture Republike Slovenijein njihovih mejnih vrednosti ter prioritete delovanja sektorjev kritične infrastrukture*, Vlada Republike Slovenije, Št. 80200-2/2018/4, dostupno na: http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/zki/SprejetoBesediloAkta_Kriteriji.pdf

U procesu utvrđivanja nacionalne kritične infrastrukture, međuresorska koordinaciona grupa definisala je značaj rada kritičnih infrastrukturnih sistema, u skladu sa prioritetima djelovanja ili neposrednom uticaju na rad drugih sektora. Tako se kritična infrastruktura klasifikuje prema sledećem redosledu prioriteta i to: energija, informacioni i komunikacione mreže i sistemi; snabdijvanje pijaćom vodom i prehrambeni sektor; zdravstveni sektor; snabdijevanje naftnim proizvodima; željeznički, vazdušni i rečni saobraćaj; snabdijevanje gasom; platni promet, obezbjeđenje snabdijevanja gotovinom; funkcionisanje državnog budžeta; zaštita životne sredine[144].

Na polju zaštite kritične informacione infrastrukture Slovenija je usvojila Nacionalnu strategiju za sajber bezbjednosti i uspostavila nacionalnu mrežu vlasnika (operatora) kritične infrastrukture, timova za hitno reagovanje, novoosnovanog Nacionalnog tijela za sajber bezbjednost, kao i Obavještajne agencije. Pored toga, strategijom za sajber bezbjednost Slovenija nastoji da ojača nacionalne kapacitete u kritičnim infrastrukturama, a posebno u dvije najvažnije - snabdijevanje električnom energijom i komunikacije u informaciono komunikacionim sistemima[145].

Slovenija planira da do 2020.godine uspostavi efikasan sistem osiguranja sajber bezbjednosti, koji će spriječiti i otkloniti posledice bezbjednosnih incidenata. Ovaj cilj obuhvata osam podciljeva, među kojima je i osiguranje rada kritične infrastrukture u sektoru podrške informaciono-komunikacionih tehnologija. U vezi sa tim, posebna pažnja će se posvetiti zakonodavnom i regulatornom okviru koji se bavi pitanjima zaštite kritične infrastrukture u sektoru podrške informacionim komunikacijama. Plan je da kritična infrastruktura sektora podrške za informaciono-komunikacione tehnologije bude tako projektovana i vođena da pruža sistemsku podršku na različitim nivoima. To podrazumijeva osiguranje nesmetanog rada infrastrukture, što zahtijeva funkcionisanje internet sistema, kao i hardvera i softvera koji podržavaju kritične funkcije na nacionalnom nivou.

Operativni kapaciteti za odgovor na sajber prijetnje u Sloveniji trenutno čine Nacionalni centar za odgovore na mrežne incidente, Sektor za bezbjednost informacija u sastavu direkcije u Ministarstvu javne uprave, Ministarstvo odbrane (za sistem odbrane i zaštite od prirodnih i drugih katastrofa), Slovenačka obavještajna agencija (SOVA) i policija u okviru svoje Kancelarije za informacione tehnologije i telekomunikacije i Uprava kriminalističke policije, uglavnom preko Centra za računarske istrage u domenu borbe protiv sajber kriminala. Nacionalni centar za reagovanje na incidente u elektronskim mrežama i bezbjednosti informacija, koordinira rešavanje incidenata, pruža tehničke savjete u slučaju upada, infekcije računarskim virusima i drugih zloupotreba. Pored toga, Centar izdaje upozorenja mrežnim administratorima i široj javnosti o trenutnim prijetnjama u elektronskim mrežama. Nacionalni centar trenutno obavlja i zadatke vladinog centra za reagovanje na oštećene mreže i koordinira u uspostavljanju nezavisnog centra koji će biti odgovoran za zaštitu informaciono-komunikacione infrastrukture državne uprave[146].

[144] Ibidem
[145] *Critical Information Infrastructures Protection approaches in EU*, European Union agency for cybersecurity, 2015, p.13
[146] *Cyber Security Strategy, establishing a system to ensure a high level of cyber security*, 2016, pp. 4-7

2.6.3. Zaštita kritične infrastrukture u Slovačkoj Republici

Geneza razvoja zaštite kritične infrastrukture Slovačke počinje stvaranjem Nacionalnog programa zaštite i odbrane kritične infrastrukture u cilju procjene postojećeg stanja i identifikacije najvažnije infrastrukture kao i uspostavljanjem programskih koraka za povećanje kvaliteta zaštite i odbrane. Nacionalni program je detaljno identifikovao i razradio 9 osnovnih sektora i 14 podsektora kritične infrastrukture (voda, hrana, zdravlje, energija, informacione i komunikacione tehnologije, prevoz, javni red i unutrašnja bezbjednost, industrija, sektor finansija)[147].

Republika Slovačka, kao dio severnoatlantske alijanse, posvećuje stalnu pažnju pitanjima koja se odnose na kritičnu infrastrukturu i njenu zaštitu. Dokument „Predlog koncepta kritične infrastrukture u Slovačkoj i sredstva za njenu zaštitu“ obrađen je na osnovu usvojene Bezbjednosne strategije Slovačke Republike 2005.godine. Nacionalni program zaštite i odbrane kritične infrastrukture u Slovačkoj donesen je 2008. godine, dok je Zakon o kritičnoj infrastrukturi usvojen 2011. godine. Jedan od glavnih razloga fokusiranja na ovo pitanje u Slovačkoj bilo je nedovoljno razrađeno zakonodavstvo u prethodnom periodu. Naime, ranija zakonska regulativa bila je samo usredsređena na odbrambenu infrastrukturu koja se odnosi na potrebe odbrane zemlje. Novi koncept kritične infrastrukture proširuje ovo područje dodatnim elementima i takođe uzima u obzir rizike nevojne prirode[148].

U Slovačkoj Republici Zakon o kritičnoj infrastrukturi usvojen je 8. februara 2011. godine. Zakonodavac je odredbama precizirao organizaciju i obim ovlašćenja državnih organa u oblasti kritične infrastrukture, postupak utvrđivanja elemenata kritične infrastrukture, dužnosti operatora u oblasti zaštite kritičnih elemenata infrastrukture i odgovornost za kršenje ovih dužnosti. U hijerarhiji zaštite posebno mjesto zauzima Vlada koja je, između ostalog, zadužena za odobravanje koncepta kritične infrastrukture kojim se određuju ciljevi, prioriteti, zadaci i metode za njihovo ostvarenje u odgovarajućem vremenskom periodu, kao i za odobravanje programa zaštite kritične infrastrukture na nivou različitih ministarstava, u cilju finansijskog pokrića izvršavanja zadataka proisteklih iz zakona o kritičnoj infrastrukturi i definisanja kriterijuma za rad nadležnih ministarstva u ovoj oblasti.

Definisanje kritične infrastrukture u Slovačkoj je različito u odnosu na većinu drugih država (Tabela br. 10). U određenju predmetne sintagme počinje se od elemenata kritične infrastrukture kao objekta (konstrukcije), javnog servisa i informacionog sistema u sektoru kritične infrastrukture, a čije bi narušavanje ili uništavanje imalo ozbiljne štetne posledice po ekonomsku i socijalnu funkciju države i zaštitu života, zdravlja, sigurnosti, imovine građana i životne sredine. S druge strane, sektor kritične infrastrukture se definiše kao dio kritične infrastrukture kome su dodijeljeni pripadajući elementi i može sadržati jedan ili više kritičnih podsektora infrastrukture. Na osnovu navedenog, dolazi se da je kritična infrastruktura u Slovačkoj sistem koji je podijeljen na sektore i podsektore[149]

---

[147] Vidriková D., Boc K., Dvořák Z., Řehák D.: *Critical Infrastructure and Integrated Protection*, The Association of Fire and Safety Engineering, Czech Republic, 2017, p. 31

[148] Sventekova E., Leiitner B., Dvorak Z.: Transport Critical Infrastructure in Slovak Republic, *Proceedings of The 8th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2017)* , p. 213, dostupno na:http://www.iiis.org/CDs2017/CD2017Spring/papers/ZA357XP.pdf

[149] Zákon o kritickej infraštruktúre, *Zbierka zákonov č. 45/2011*, § 2, dostupno na: https://www.zakonypreludi.sk/zz/2011-45

R.br.	Sektor	Podsektor
1.	Transport	Drumski transport Avio saobraćaj Vodeni transport Željeznički transport
2.	Elektronske komunikacije	Satelitska komunikacija Mreža i usluga fiksne i mobilne elektronike komunikacije
3.	Energetika	Rudarstvo Električna energija Gasna industrija Nafta i naftni proizvodi
4.	Informacione i telekomunikacione tehnologije	Informacioni sistemi i mreže Internet
5.	Pošta	Pružanje poštanskih usluga, plaćanja i nabavke
6.	Industrija	Framaceutska, metalurška i hemijska industrija
7.	Voda i atmosfera	Meteorološka služba Vodovod i snabdijevanje pijaćom vodom
8.	Zdravstvene usluge	
9.	Finansije	Bankarstvo Finansijsko tržište Sistem upravljanja javnim finansijama

Tabela br. 10.: Sektori i podsektori kritične infrastrukture Slovačke Republike[150]

Ministarstvo unutrašnjih poslova Slovačke Republike je ovlašćeno da koordinira aktivnosti državne uprave u oblasti zaštite kritične infrastrukture koju sprovode odabrana ministarstva prema djelokrugu njihove nadležnosti. Ministarstva su odgovorna za sektore kritične infrastrukture koji su im dati u nadležnost. Ministarstvo unutrašnjih poslova u saradnji sa drugim ministarstvima, u čijoj su nadležnosti pojedini sektori kritične infrastrukture, izrađuje nacrt koncepata kritične infrastrukture koji podnosi Vladi na odobrenje. Pored toga, u saradnji sa nadležnim ministarstvima, učestvuje u izradi nacrta sektorskih kriterijuma kao i sa odgovarajućim ministarstvima u donošenju odluka u nadležnosti vlade. Analizirajući zakonodavni okvir Slovačke, uočljiva je usklađenost sa odredbama Direktive EU o utvrđivanju i označavanju evropske kritične infrastrukture. Tako je, na primjer, posebna pažnja posvećena bezbjednosnim planovima, licima za kontakt kao i postupku za određivanje elemenata evropske infrastrukture i slično.

Kao i mnoge druge države, i Slovačka je posebnu pažnju posvetila kritičnoj informacionoj infrastrukturi. Tako je „kritična informaciona i komunikaciona infrastruktura“ definisana kao skup sistema, infrastrukture, mreža i usluga informacionih i komunikacionih tehnologija koje bi, ako bi bili poremećeni, oštećeni ili nedostupni, ozbiljno uticali na rad drugih sektora kritične infrastrukture i društvenih funkcija od vitalnog značaja, uključujući nacionalnu, ekonomsku i javnu bezbjednost“[151].

[150] Ibidem, pp. 5-6
[151] *Cyber Security Concept of the Slovak Republic for 2015 – 2020*, p. 21

Centralni strateški dokument za sajber-bezbjednost je Nacionalna strategija za informacionu bezbjednost Slovačke Republike. Strategiju je izradilo Ministarstvo finansija koje je nadležno za bezbjednost informacija koje se odnose na sve nerazvrstane informacije u javnoj administraciji i široj javnosti[152]. Predmetni dokument ističe strateške prioritete sa definisanim ključnim zadacima među kojima je i osiguranje dovoljne zaštite kritične informacione infrastrukture. To obuhvata identifikaciju nacionalne kritične infrastrukture i osiguranje njene bezbjednosti povećanjem informacione bezbjednosti u državnim agencijama, kao i primjenom bezbjednosnih proizvoda, sistema i uslova za uvođenje novih mjera. Kao rezultat toga, donijet je interresorni program finansijske podrške mjerama za zaštitu kritične infrastrukture.

Ključ organizacione strukture za sajber bezbjednost i sajber odbranu u Slovačkoj je razlika između upravljanja i informacione bezbjednosti klasifikovanih i neklasifikovanih informacija. Prvim pitanjem se bavi Nacionalna agencija za bezbjednost, a drugim Ministarstvo finansija. Srodne oblasti podložne su sektorskom zakonodavstvu, koje takođe naglašava odgovornosti specijalizovanih vladinih agencija za ove oblasti. Na primjer, integrisano upravljanje krizom i zaštitu kritične infrastrukture koordinira Sektor za upravljanje krizama Ministarstva unutrašnjih poslova. Međusobnu komunikaciju olakšava Odbor za bezbjednost informacija Ministarstva finansija, koji ima savjetodavnu i koordinacionu ulogu, pripremajući strateške i tehničke materijale o bezbjednosti informacija. Odbor sačinjavaju predstavnici Sektora za informaciono društvo Ministarstva finansija, Ured Vlade, Ministarstvo unutrašnjih poslova, Nacionalna agencija za bezbjednost, Slovačka asocijacija za informatiku, Slovačko udruženje za bezbjednost informacija i predstavnik akademske institucije u oblasti informacione bezbjednosti[153].

2.7. Stanje zaštite kritične infrastrukture u Crnoj Gori

Kao i za ostale države bivše Jugoslavije, i za Crnu Goru značenje nacionalne kritične infrastrukture obuhvatalo je sva "državna preduzeća", odnosno sva preduzeća i ustanove koje su se nalazile u državnom vlasništvu (energetski sektor, telekomunikacije, transport, pošta i drugo). Sredinom 1950-ih ovi subjekti su bili zaštićeni internom bezbjednošću, uz pomoć policijskih, bezbjednosnih i obavještajnih službi. Od druge polovine sedamdesetih godina XX vijeka, kritične infrastrukture i sva druga državna ili javna imovina, bili su zaštićeni sveobuhvatnom mrežom poznatom kao sistem društvene samozaštite. Pored unutrašnje službe bezbjednosti, taj sistem je obezbijedio dva dodatna sloja zaštite imovine preduzeća: unutrašnju finansijsku kontrolu i kontrolu udruženih radnika. Uprkos činjenici da su postojala tri stepena zaštite (kontrole), krađe, štete i drugi gubici i ugrožavanja imovine su ipak bili stalno prisutni.[154]

Sistem zaštite kritične infrastrukture veoma je složen proces koji se u Crnoj Gori još uvijek razvija. Pitanje kritične infrastrukture u Crnoj Gori dugo je bilo vezano za oblast odbrane. Tako je

---

[152] Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, Ministerstvo financií, 2008, p. 6, dostupno na:www.informatizacia.sk/ext_dok-narodna_strategia_pre.../6167c

[153] Hriciková L., Kaska K.: *National Cyber Security Organisation: Slovakia*, NATO Cooperative Cyber Defence Centre of Excellence the Centre, Tallinn, 2015, pp. 9-10

[154] Davidovic D., Kesetovic Z., Pavicevic O.: National Critical Infrastructure Protection in Serbia: The Role of Private Security, *Journal of Physical Security* 6(1), 2012, p. 60, dostupno na: http://rbsekurity.com/JPS%20Archives/JPS%206(1).pdf

Vlada Crne Gore definisala infrastrukturu od posebnog značaja za odbranu, u koju su uključeni veliki tehnički sistemi od posebnog značaja za odbranu, izgrađeni komandni punktovi, elektronski komunikacioni centri, radio-relejni čvorovi, radarski i elektronski sistemi, fortifikaciona infrastruktura, aerodromi, luke (baze), eksperimentalni prostori i laboratorije, magacini za naoružanje, municiju, gorivo i vojnu opremu, posebne prostorije za čuvanje Plana odbrane Crne Gore, vojne arhive i server za vojno računarsku mrežu i operativni centri, plan za organizaciju, razvoj, opremanje, modernizaciju i raspoređivanje oružanih snaga Crne Gore, kripto-uređaji i šifre[155].Veliki tehnički sistemi od posebnog značaja za odbranu definišu se kao složeni ili sastavljeni od djelova i postupaka koji su međusobno povezani koji obezbjeđuju tehničko i tehnološko jedinstvo i nezavisnost sistema ili njegovu funkcionalnu povezanost sa drugim tehničkim sistemima koji su važni za odbranu. Odlukom Vlade Crne Gore, u oblasti telekomunikacija, informatike, saobraćaja, elektroenergetike, vodosnabdijevanja i drugih područja od značaja za odbranu posebno su navedeni veliki tehnički sistemi[156].

Bezbjednost infrastrukture od posebnog značaja za odbranu uključuje organizovanje i realizaciju mjera za njihovu zaštitu od oštećenja ili uništavanja ili otkrivanja povjerljivih podataka o infrastrukturi ili lokaciji. Posebnim dokumentima definišu se postupci primjene bezbjednosnih mjera zaštite infrastrukture od posebnog značaja za odbranu. Iako je ova tema prisutna poslednjih godina, očigledno je da, za razliku od razvijenih evropskih zemalja, Crna Gora nije razvila politiku u ovoj oblasti. S obzirom da Crna Gora želi da bude dio Evropske unije, zaštita kritične infrastrukture može predstavljati važan element u procesu evropskih integracija. Stoga je na nacionalnom nivou napravljen niz koraka u smjeru definisanja politike i zaštite kritične infrastrukture radi određenja ciljeva, principa, smjernica i mehanizama.

Strategija nacionalne bezbjednosti Crne Gore ukazuje da je povećanom upotrebom informacionih tehnologija Crna Gora postala ugrožena u domenu informatičke bezbjednosti. Pri tome se navode i određena područja čija funkcija može biti ograničena ili potpuno paralizovana u slučaju djelovanja iz sajber prostora. Strategija posebnu pažnju posvećuje i kritičnoj infrastrukturi sa aspekta ugrožavanja nacionalne bezbjednosti, i naglašava značaj zaštite kritične infrastrukture kao obaveze svih elemenata sistema. „ Identifikovanjem i popisom kritičnih infrastruktura na kopnu, moru, pod morem, u vazduhu i u sajber prostoru, definisanjem odgovornih nosilaca zaštite i koordinacijom aktivnosti na svim nivoima obezbjeđuje se kvalitetno planiranje, efikasnost odgovora, a time i otpornost kritične infrastrukture“.[157]

Evidentno je da je Crna Gora poslednjih godina znatno veću pažnju posvetila kritičnoj informacionoj infrastrukturi. Značajna je Strategija sajber bezbjednosti Crne Gore 2018-2021. godine, kao nastavak strategije čiji je ciklus završen 2017. godine. Strategija predstavlja strateški okvir u ovoj oblasti, kojom se između ostalog, definišu ključni koraci u jačanju izgradnje kapaciteta za efikasnu borbu protiv računarskog kriminala. Načini i uslovi sprovođenja ciljeva definisanih strategijom jasno su definisani u Akcionom planu. Posebnim zakonom koji obrađuje informacionu bezbjednost definisano da „kritičnu informatičku infrastrukturu čine informacioni sistemi organa

[155] Bigović M., Rakočević A.: Challenges in Definning Critical Infrastructure in Montenegro, in: Čaleta D., Radović V. (ed): *Comprehensive Approach as „Sine Qua Non“ for Critical Infrastructure Protection*, IOS Press BV, Amsterdam, 2015, p. 273

[156] Odluka o određivanju velikih tehničkih sistema od značaja za odbranu, „*Službeni list Crne Gore*“, br. 15/08, čl. 2

[157]Strategija nacionalne bezbednosti Crne Gore, „*Službeni list Crne Gore*“, br. 085/18, str. 3-6

čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa".[158] Zakon pored ostalog predviđa formiranje Savjeta za informacionu bezbjednost i zaštitu kritične informatičke infrastrukture, u skladu sa Direktivom EU o mjerama za obezbjeđivanje najvećeg nivoa bezbjednosti mrežnih i informacionih sistema širom EU. Savjet između ostalog prati realizaciju Strategije sajber bezbjednosti, kroz dostavljanje kvartalnih izveštaja od strane nosilaca aktivnosti definisanih Strategijom i pratećim akcionim planovima, i jednom godišnje podnosi izveštaj o raduVladi[159].

Pored navedenih normativnih dokumenata, od značaja je i Metodologija izbora kritične infrastrukture, kojom je identifikovana kritična informaciona infrastruktura, kao i nosioci zaštite (Tabela br. 11). Prema toj metodologiji, „kritična infrastruktura se odnosi na imovinu, sisteme, usluge ili njihov dio, čijim bi se prekidom rada ili uništenjem, ugrozile ključne društvene funkcije: zdravlje, mir, bezbjednost, ekonomsko i socijalno blagostanje ili normalno funkcionisanje države".[160]

KRITIČNI SEKTORI INFORMACIONE INFRASTRUKTURE	NOSIOCI SEKTORA KRITIČNE INFORMACIONE INFRASTRUKTURE
Informatičke i komunikacione tehnologija	Ministarstvo za informaciono društvo i telekomunikacije
Bankarstvo i finansije	Ministarstvo finansija
Energetika	Ministarstvo ekonomije
Zdravstvo	Ministarstvo zdravlja
Poljoprivreda, bezbjednost hrane, šumarstvo i vodoprivreda	Ministarstvo poljoprivrede i ruralnog razvoja
Nacionalna odbrana i bezbjednost	Ministarstvo odbrane/Ministarstvo unutrašnjih poslova/Ministarstvo pravde/ Agencija za nacionalnu bezbjednost
Transport	Ministarstvo saobraćaja i pomorstva
Državni organi /Usluge Vlade CG	Ministarstvo za informaciono društvo i telekomunikacije

Tabela br. 11.: Kritični sektori i nosioci sektora kritične informatičke infrastrukture[161]

Po pitanju informacione infrastrukture u institucionalnom smislu od značaja je Direkcija za informatičku bezbjednost i odgovor na kompijuterske incidente, koja pripada Ministarstvu javne uprave. Primarni zadatak Direkcije je da omogući rano otkrivanje sajber prijetnji i incidenata i adekvatno reaguje i odgovori na iste[162]. To je ujedno i centralni organ sa zadatkom koordinacije,

[158] Zakon o informacionoj bezbednosti „*Službeni list Crne Gore*", br. 014/10, 040/16, čl. 14a
[159]Odluka o obrazovanju savjeta za informacionu bezbjednost, „*Službeni list Crne Gore*", br. 48/17, čl. 3
[160]*Metodologija izbora kritične infrastrukture*, Ministarstvo za informaciono društvo i telekomunikacije, Podgorica, 2014, str. 4
[161] Ibidem, str. 11-12
[162]Pravilnik o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave, str. 5, dostupno na:http://www.mju.gov.me/organizacija

prevencije i zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema Crne Gore. Navedeno ukazuje da procesom zaštite kritične informacione infrastrukture upravlja država Crna Gora, što ujedno predstavlja jedan od modela upravljanja na nivou Evropske unije.

Pored navedenog, i drugi državni organi jačaju svoje kapacitete, pa je tako u Upravi Policije formirana Grupa za borbu protiv visokotehnološkog kriminala, sistematizovana u okviru Odsjeka za borbu protiv organizovanog kriminala i korupcije.

U daljem razvoju koncepta zaštite kritične infrastrukture, Crna Gora je pristupila izradi zakonske osnove. U toku izrade ovog rada ušao je u Skupštinsku proceduru Nacrt Zakona o kritičnoj infrastrukturi, što ujedno predstavlja i prvi pokušaj da se predmetna oblast uredi odgovarajućim zakonom. S obzirom da je posebna cjelina rada posvećena zaštiti kritične infrastrukture u Crnoj Gori u ovom dijelu daćemo opšti osvrt, dok će u poslednjem dijelu biti dat kritički osvrt na navedeni Nacrt i ovu problematiku.

Na osnovu opšte analize predmetnog zakona evidentno je nastojanje da bude usklađen sa Direktivom Savjeta EU (2008/114/EZ), u kontekstu usklađivanja ukupnog zakonodavstva Crne Gore u procesu pristupanja Evropskoj uniji.

Navedenim dokumentom definisano je da kritična infrastruktura sadrži „sisteme, mreže, objekte ili njihove djelove, čiji prekid funkcionisanja ili prekid isporuka roba, odnosno usluga može imati ozbiljne posledice na nacionalnu bezbjednost, zdravlje i život ljudi, imovinu, životnu sredinu, bezbjednost građana, ekonomsku stabilnost, odnosno može ugroziti funkcionisanje Crne Gore“[163]. Iz navedenog određenja uočljiv je pristup da se kritična infrastruktura posmatra iz ugla posledica prekida ili nefunkcionisanja kritične infrastrukture. Crna Gora prepoznaje devet sektora kritične infrastrukture (energija, saobraćaj, snabdijevanje vodom, zdravstvo, finansije, telekomunikacione i infromacione tehnlologije, zaštita životne sredine i funkcionisanje državnih organa). U cilju bolje koordinacije i prilikom ugrožavanja funkcionisanja kritične infrastrukture, predlagač je predvidio Koordinaciono tijelo za zaštitu kritične infrastrukture koje povezuje različita ministarstva nadležna za određene sektore kritične infrastrukture. Usklađenost sa evropskom legislativom u ovoj oblasti ogleda se i u prepoznavanju koordinatora za zaštitu kritične infrastrukture i bezbjednosnih planova, kojima je predlagač posvetio posebnu pažnju s obzirom da je detaljnije definisao predmetnu tematiku.

[163] *Nacrt Zakona o kritičnoj infrastrukturi*, čl. 3, Ministarstvo unutrašnjih poslova, Podgorica, 2019, dostupno na: https://www.paragraf.me/nacrti_i_predlozi/nacrt-zakona-o-kriticnoj-infrastrukturi.pdf

TREĆI DIO

JAVNO-PRIVATNO PARTNERSTVO

Države su kroz istoriju oduvijek ostvarivale saradnju sa privatnim sektorom u realizaciji širokog spektra poslova koji su po svojoj prirodi imali javni značaj. U savremeno doba koncept javno-privatnog partnerstva predstavlja sistemski pristup mnogih država u svijetu, prvenstveno u procesu finansiranja infrastrukture. Međutim, najveći problemi i neslaganja u ekonomskoj sferi od nastanka moderne države vezani su za dozvoljivi stepen miješanja i uticaja države na privredu i tržište. Inače, tendencija pojačanog državnog uticaja na ekonomiju vezuje se za završetak Drugog svetskog rata, a svoj maksimum je državni intervencionizam zabilježio u socijalističkom bloku za vrijeme hladnog rata.

Preovlađujući trend od kraja 70-tih godina XX vijeka je da se uloga države u sferi ekomomije usmjerava prema tržišno orijentisanoj privredi, što je uticalo na mnogobrojne i suštinske promjene u toj oblasti. Naime, državni aparat koji je razvijan u prethodnom periodu, nesumnjivo je bio je glomazan i neefikasan, a što je posebno značajno i preskup. Takav naslijeđeni model države, koji je zaokupljen pravilima i nefleskibilnom hijerarhijom, u uslovima ubrzanog tehnološkog razvoja, a posebno upotrebe informacionih tehnologija, nije mogao da zadovolji kriterijume efikasnosti. Promjene na tom planu, koje su započete u SAD i Velikoj Britaniji, obuhvatile su smanjenje državnog aparata, transfer nadležnosti ka nižim jedinicama lokalne uprave, te privatizaciju javnih preduzeća, a samim tim i njihovih usluga. To je uticalo i na promjenu načina poslovanja, posebno na nivou lokalnih vlasti, što je podrazumijevalo započinjanje saradnje sa privatnim sektorom u cilju smanjenja nedostatka finansijskih sredstava, povećanja kvaliteta usluga i stvaranja mogućnosti da i privatni sektor učestvuje na tenderima za komunalne i druge usluge, koje su do tada predstavljale monopol države. To su ujedno bili i počeci javno-privatnog partnerstva u modernom dobu.

3.1. Pojmovno određenje javno-privatnog partnerstva

Nastojanje da se saradnja javnog i privatnog sektora u ostvarivanju javnih usluga definiše na jedinstven i opšteprihvatljiv način nije lak zadatak, za što postoje brojni razlozi. Kao prvo, istorijska geneza ovog fenomena ukazuje da kooperativnost između državnog i privatnog sektora postoji vjekovima, ali da su motivi i interesi bili različiti. Posledica toga je da se sadržaj pojma javno-privatnog partnerstva bitno razlikuje od onog iz prošlosti. Drugi razlog je takođe veoma značajan, jer ukazuje na promjenljivost političkih stanovišta nosilaca vlasti prema privatnim inicijativama u ovoj oblasti, a posebno prema ideji udruživanja. U tom kontekstu, nesumnjivo je da su socijaldemokratske političke opcije po pravilu bile naklonjene tradicionalnom modelu isporuke javnih usluga. S druge strane, neoliberalni koncept je u kontinuitetu bio sklon većem značaju privatne inicijative u obezbjeđenju javnih usluga. Pored toga, iz tehničko-tehnološkoga ugla, odnosi dva sektora mijenjali su se zavisno o složenosti medija posredstvom kojega je isporučivana javna usluga. Sa finansijskog aspekta je taj odnos bio određen dostupnošću različitih oblika izvora finansiranja izgradnje javnih građevina.

U početku je koncept javno-privatnog partnerstva prvenstveno uključivao projekte urbane izgradnje koji su olakšavali zajednički razvoj i obnovu problematičnih urbanih zona. Savremena verzija tog koncepta, prema kojoj angažovanu privatnu kompaniju plaća vlada, a ne potrošači, evoluirala je u Velikoj Britaniji osamdesetih godina prošlog vijeka. Cilj je bio da se vladi omogući da što uspješnije razvije infrastrukturu, a da se istovremeno pridržava strogih ograničenja zaduživanja ili fiskalnih pravila za rešavanje rastućeg javnog duga. Vremenom se pomenuti koncept proširio i na zajedničke tehnologije, ekološke projekte, kao i na javno-privatna partnerstva u oblasti obrazovanja, zdravstvene zaštite i izvršenja zatvorskih kazni. Danas je to postao veoma heterogen koncept, za koji kritičari kažu da je evoluirao u pravcu svih mogućih novih ili poznatih oblika saradnje između javne administracije i privatnog sektora[164].

Koncept povezivanja javnog i privatnog sektora u teoriji i praksi se označava jedinstvenim nazivom javno-privatno partnerstvo (*Public Private Partnership*), odnosno njegovim akronimom PPP. Međutim, i u ovom slučaju postoje izuzeci kao što je na primjer Kanada, u kojoj se upotrebljava skraćenica P3, ili Australija, gde se koristi sintagma privatno finansiranje projekata (*Privately-Financed Projects - PFP*). S druge strane, izraz inicijativa za privatno finansiranje (*Private Finance Initiative - PFI*) upotrebljava se u Velikoj Britaniji, Japanu i Maleziji, a privatno učešće u infrastrukturi (*Private Participationon Infrastructure - PPI*) uobičajeno je u Južnoj Koreji[165].

Evropska komisija (EK) je javno-privatno partnerstvo definisala kao „investicione projekte transferisane privatnom sektoru koje je tradicionalno izvršavao ili finansirao javni sektor“[166]. U dokumentu Evropske komisije pod nazivom „Zelena knjiga“, objašnjeni su najvažniji elementi javno-privatnog partnerstva. Tako se, između ostalog, naglašavaju vremenski rok trajanja partnerstva, izvori finansiranja, odgovornost između partnera, kao i rizici koje javno-privatno partnerstvo sa sobom nosi[167]. Slično tome je određenje po kome je javno privatno partnerstvo usmjereno na razvoj infrastrukturnih projekata kroz dugoročnu saradnju javnog i privatnog sektora. Na ovaj način se posebno naglašava značaj holističkog pristupa koji se proteže tokom cjelokupnog ciklusa realizacije partnerstva[168].

Evropska komisija je u svojim „Smjernicama za uspješna javno-privatna partnerstva“[169] pomenuti pojam definisala kao „partnerstvo između javnog i privatnog sektora u svrhu realizacije projekta ili usluga koje tradicionalno pruža javni sektor”, koje karakterišu podjela investicija, rizika, odgovornosti i dobiti među partnerima. Uz to, javno-privatno partnerstvo karakteriše odnos koji uključuje dijeljenje moći, rada, podrške i (ili) informacija sa drugima radi postizanja zajedničkih

---

[164] Jomo K. S, Chowdhury A., Krishnan S., Platz D.: *Public-Private Partnerships and the 2030 Agenda for Sustainable Development: Fit for purpose?*, Department of Economic & Social Affairs, DESA Working Paper No. 148, 2016, p. 3

[165] Swapnil G., Sachin G.: *Rethinking Public-private Partnerships: An Unbundling Approach*, Transportation Research Procedia 25, 2017, pp. 3792- 3793

[166] European PPP Expertise Centre(EPEC), PPP Guide, p. 1, dostupno na: http://www.eib.org/epec/g2g/intro2-ppp.htm

[167] Stakić B., Vasić D., Ćurković V.: *Ulaganje kapitala putem javno-privatnog partnerstva i koncesija*, Fakultet za poslovne studije i pravo, Beograd, 2015, str. 70

[168] German Transport, Construction and Housing Ministry (Bundesministeriumfür, Verkehr, Bauenand Wohnen) dostupno na: http://www.bmvi.de/DE/Home/homenode.html

[169] *Guidelines for Successful Public – Private Partnerships,* European commission, March 2003, dostupno na: http://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf

ciljeva i (ili) obostrane koristi.[170] Na ovaj način se posebno potenciraju odnosi između organizacija, kao i saradnja i zajednički ciljevi.

Uprkos nespornoj činjenici da savremena pravna i ekonomska literatura obiluje teorijskim i empirijskim raspravama o ulozi i značaju javno-privatnog partnerstva, taj koncept je i dalje suočen sa problemom jasnog određenja. Naime, osnovna razilaženja se tiču razgraničenja da li određeni konkretni slučaj predstavlja oblik javno-privatnog partnerstva, odnosno šta određeni projekat kvalifikuje da bude okarakterisan kao predmetni oblik partnerstva[171].

Na osnovu karakteristika javno-privatnog partnerstva, taj koncept je pogrešno poistovećivati sa privatizacijom, koja po svojoj prirodi predstavlja nepovratno ustupanje prava isporuke javne usluge privatnom sektoru. Preciznije, javno-privatno partnerstvo se zasniva na bližem povezivanju određenih subjekata iz javnog i privatnog sektora, odnosno na zajedničkom nastupu radi ostvarivanja javne usluge i utvrđivanju optimalnog načina ostvarivanja te isporuke. Naime, za javno-privatno partnerstvo je ključna odrednica zajedničko odlučivanje o procesu isporuke javne usluge, a u cilju postizanja željene efikasnosti za obije strane.

Primjena mehanizama javno privatnog partnerstva pruža brojne prednosti, kako za državu, tako i za privatne kompanije. U tom kontekstu, privatni sektor dobija nove izvore prihoda i mogućnosti za učešće u velikim projektima. S druge strane, javno privatno-partnerstvo podrazumijeva upotrebu intelektualnih i stručnih potencijala i drugih resursa privatnog sektora u oblastima tradicionalne državne odgovornosti. U vezi sa tim, neka od ograničenja koja se odnose na implementaciju javno-privatnog partnerstva u savremenoj praksi uključuju:

- poteškoće sa procjenom državnih koristi od ugovora o partnerstvu;
- nedostatak jasne politike koja se odnosi na razmatranje interesa preduzetnika i transparentnosti javno-privatnih alata za interakciju,
- poteškoće sa procjenom pouzdanosti i zahtijevane efikasnosti projekata,
- povećane troškove zbog složenosti konkurencije i harmonizacije ugovora u poređenju sa utvrđenim procedurama javnih nabavki,
- poteškoće u predviđanju rizika povezanih sa projektima javno-privatnog partnerstva,
- potreba za temeljnim pregledom projekata, jer nisu svi projekti pogodni za javno -privatno partnerstvo i
- nedovoljno razvijene mehanizme primjene ovog koncepta i procjene njegove efikasnosti[172].

Za potpunije razumijevanje javno-privatnog partnerstva neophodno je uočiti i nedostatke tradicionalnog načina pružanja javnih usluga. U vezi sa tim, evidentan je stalni rast izdataka za javne usluge i nedostatak inovativnosti u poboljšanju kvaliteta javnih usluga. S druge strane, kao prednosti privatnog sektora uočavaju se sposobnost upravljanja troškovima, fleksibilnost, inovativnost, posjedovanje specifičnih znanja i vještina i slično.

Prilikom započinjanja partnerstva potrebno je da javni sektor uspostavi potrebnu ravnotežu, koja podrazumijeva zaštitu prava i interesa građana, kao i stvaranje uslova za efikasno i efektivno

[170] Kernaghan K.: Partnerships and public administration: conceptual and practical considerations. *Canadian Public Administration*, Vol. 36, Issue 1, Institute of Public Administration of Canada,1993, pp. 59-63.
[171] De Bettignies J. E., Ross T. W.: The economics of public–private partnerships: some theoretical contributions, *International Handbook on Public–Private Partnerships*, Cheltenham, UK Northampton, 2010, pp. 134-138
[172] Sarsengali A. et all: Development of Public-Private Partnership in the Republic of Kazakhstan, *IEJME—Mathematics education* , Vol. 11, No. 5, 2016, p. 1114

funkcionisanje privatnih partnera. Da bi partnerstvo bilo uspješno i ostvarilo postavljene ciljeve uz ostvarivanje veće sigurnosti obije strane, potrebno je zaključiti ugovore na duži vremenski period uz definisanje integracije svih faza projekta tokom trajanja ugovora. Pored toga, značajno je i razvijanje mehanizma u cilju osiguranja da organizacija koja je davalac usluge bude odgovorna prema svojim korisnicima bez obzira da li su iz javnog ili privatnog sektora. Principi pravičnosti, transparentnosti, kao i zajednički interes predstavljaju osnovu istinskog partnerstva. Pored toga u bilo kom projektu povjerenje i sigurnost su od posebnog značaja za uspješno partnerstvo[173]. Kada se radi o subjektima koji su uključeni u predmetno partnerstvo, onda su to profitna i neprofitna preduzeća vladinog i nevladinog sektora, vlada i lokalna samouprava. Razlog njihove saradnje je realizacija infrastrukturnih projekata, kao i unapređenje legislative za uspješno povezivanje zainteresovanih subjekata i grupa, kroz različite forme umrežavanja[174].

I pored različitog određenja javno privatnog partnerstva, ipak se mogu uočiti neka zajednička obilježja. Osnovno obilježje je postojanje dva ili više subjekata od kojih je jedan iz javnog, a drugi iz privatnog sektora. Pored toga, predmetna saradnja može obuhvatiti i učesnike iz domena nevladinih organizacija. Druga značajna karakteristika je da učesnici ugovaraju svoje učešće za sopstveni račun u odnosu na ostale učesnike i u odnosu na projekat. Treća karakteristika je da se predmetno partnerstvo uspostavlja na dugoročni period što ujedno podrazumijeva i stabilnu saradnju među učesnicima. U praksi postoje brojni primjeri dugoročne saradnje javnog sektora s određenim dobavljačem iz privatnog sektora. Takva se saradnja ne može nazvati modelom javno-privatnog partnerstva zbog više razloga. Neki od razloga su da se saradnja uvijek može prekinuti bez posebnih obrazloženja, te da partneri nijesu zajednički učestvovali u osmišljavanju cijelog procesa isporuke i eksploatacije usluge, već je javni sektor definisao sve potrebne elemente o usluzi i odabrao najpovoljnijeg dobavljača. Pri tome javni sektor preuzima rizike za dobavljeno dobro nakon isporuke i slično. Značajna karakteristika je i da svaki od učesnika ulaže nešto u partnerstvo. Da bi partnerstvo bilo uspješno, svaki od partnera mora uložiti neki materijalni ili nematerijalni resurs u cilju ostvarivanja sinergijskog efekta za sve učesnike u projektu. Na kraju, bitna karakteristika partnerstva je podijeljena odgovornost za isporučene usluge. Takav je odnos bitno različit u odnosu na tradicionalnu poziciju javnog sektora, gdje on zadržava sva ovlašćenja i odgovornosti za isporuku javne usluge i sprovođenju javnih politika. Zbog velikog značaja podjele odgovornosti, javno-privatno partnerstvo se uspostavlja posredstvom nezavisnog ekonomskog subjekta umjesto direktnim ugovorom. Utvrđivanje standarda javne usluge, odnosno izlaznih karakteristika koje određeni proizvod partnerstva mora da zadovolji, kao i povezana podjela rizika i podjela koristi nakon implikacije rizičnih situacija, osnovni su elementi savremenog shvatanja pojma javno-privatnoga partnerstva[175].

[173] Leković V, Ivanović V.: *Javno-privatno partnerstvo u funkciji obezbeđenja kvalitetnije infrastrukture*, Festival kvaliteta, Kragujevac, 2009, str. 97

[174] Staković Lj., Cvetanović S.: Javno privatna partnerstva – faktor unapređenja konkurentske prednosti, *Ekonomika preduzeća*, *br. 3-4*, Savez ekonomista Srbije, Beograd, 2011, str. 167

[175] Akintoye A., Beck M., Hardcastle C.: *Public-Private Partnerships Managing Risk and Opportunities*, Blackwell, Science, Oxford, 2006, pp. 5-7

3.2. Karakteristike javno-privatnog partnerstva

Javno-privatno partnerstvo, kao savremeni način finansiranja javnog sektora uz pomoć privatnog partnera, omogućava uspostavljanje saradnje javnog i privatnog sektora na ostvarivanju zajedničkih ciljeva, naročito u investiranju i podjeli rizika, a sve kako bi javna usluga bila dostupnija, kvalitetnija i naročito jeftinija za poreskog obveznika. Pored toga, osnova na kojoj počiva javno-privatno partnerstvo predstavlja aranžman javnog i privatnog partnera, u kojem se ostvaruju različiti modeli partnerstva, od kojih finansiranje javnog uključivanjem privatnog sektora predstavlja samo jedan od oblika. Ostala područja saradnje na kojima se zasniva javno-privatno partnerstvo obuhvataju: projektovanje, izgradnju, upotrebu i održavanje javne infrastrukture i usluga. Javni i privatni sektor nastoje da unaprijede ekonomski rast i razvoj kroz ostvarivanje svojih ciljeva, uz obostrano utvrđenu odgovornost partnera i definisan rizik. S druge strane, u stalnom porastu je potreba za bržim lokalnim razvojem, koji je, međutim, sve teže ostvariti uzimajući u obzir ograničene finansijske, materijalne i kadrovske resurse javnog sektora[176].

U naučnoj i stručnoj literaturi najšće se pominje nekoliko tipova javno-privatnog partnerstva. Jedan od njih je ugovorno javno-privatno partnerstvo, u kome su međusobna prava i obaveze u realizaciji projekta definisani javnim ugovorom. Javnim ugovorom se definišu prava i obaveze, koncesionara kao i davaoca koncesije koja su usklađena sa odgovarajućim zakonima kojim je uređena ova oblast.

Drugi model je institucionalno javno-privatno partnerstvo, koje uključuje formiranje zajedničke projektne kompanije kao privrednog društva sa jedinstvenim ciljem sprovođenja koordinacije i zastupanja aktivnosti koje su određene ugovorom između projektne kompanije i javnog sektora. U vezi sa tim, projektna kompanija čije je postojanje višestruko korisno, predstavlja centar organizacione strukture svakog javno-privatnog partnerstva. Time se, između ostalog, izbjegava dolaženje u zavisnost od sponzora i osigurava da na poslovanje projektne kompanije ne utiču problemi sa bilo kojim nepovezanim subjektom[177].

Poseban oblik ugovornog javno-privatnog partnerstva predstavljaju koncesije. Ugovorom se uređuje komercijalno korišćenje prirodnog bogatstva i dobara u opštoj upotrebi koja su u javnoj svojini, ili ostvarivanje djelatnosti od opšteg interesa, a koje nadležni državni organ ustupa, na određeno vrijeme, pod posebno propisanim uslovima, uz plaćanje koncesione naknade privatnog, odnosno javnog partnera. U navedenim okolnostima, privatni partner snosi rizik komercijalnog korišćenja koncesije. Pored navedenog, postoje i koncesije za javne radove koje su u sve široj primjeni, naročito u nerazvijenim državama. I u ovom slučaju osnovu partnerstva predstavlja ugovorni odnos. Predmetni ugovorni odnos je istovetan kao i kod ugovora kojim se regulišu javne nabavke u skladu sa zakonom. Ali postoji jedna specifičnost koja se odnosi na naknadu za javne radove, ona se sastoji od samog prava na komercijalno korišćenje izvedenih radova ili od tog prava zajedno s plaćanjem[178].

---

[176] Plumer J.:*Focusing Partnership: A Sourcebook. for Municipal Capacity Building in Public - Private Partnership*, Earthscan, London, 2002, p. 33.

[177] Yescombe R. E., Farquharson E.: *Public-private partnerships for infrastructure, principles of policy and finance*, Butterworth-Heinemann, Oxford, 2018, p. 290

[178] Stakić B., Vasić D., Ćurković V.: *Ulaganje kapitala putem javno-privatnog partnerstva i koncesija*, Fakultet za poslovne studije i pravo, Beograd, 2015, str. 84

U zavisnosti od stepena uključenosti partnera u procese kao što su projektovanje, izgradnja, održavanje, finansiranje i upravljanje, uz dodatak rizika kod pružanja javnih usluga ili izgradnje javne infrastrukture, postoje specifični modeli javno-privatnog partnerstva. Jedan od njih je privatno finasiranje (*FO-finance only*), u kome privatni sektor (najčešće banke i fondovi) direktno finansira izgradnju javne infrastrukture, pri čemu svi troškovi finansiranja idu na teret javnog sektora, koji je ujedno i nosilac rizika izgradnje i eksploatacije. S druge strane, kod primjene modela projektuj-pobijedi u takmičenju-izgradi (*DBB-design-bid-build*), javni sektor definiše potrebne zahtjeve vezane za projekt, obezbjeđuje njegovo finansiranje i projektovanje, a postupkom javne nabavke vrši odabir privatnog partnera koji je ujedno i najpovoljniji ponuđač. Privatni partner ima odgovornost za izgradnju, a javni partner je vlasnik i ujedno održava izgrađeni objekat. Ipak, predmetni model u mnogim slučajevima nije najefikasniji ili najisplativiji način za isporuku određenog projekta. To posebno dolazi do izražaja kod dovršavanja određenih projekata, kada je pogodniji model po principu „ključ u ruke“[179].

Sličan navedenom je i model projektuj-izgradi-održavaj (*DBM - design-build-maintain*) u kome po zahtjevu i specifičnostima javnog sektora, privatni sektor realizuje projektovanje, izgradnju i održavanje infrastrukture prema ugovorenom novčanom iznosu. To znači da su troškovi rizika kao i rizik vezan za kvalitet i održavanje objekta u nadležnosti privatnog sektora. S druge strane, znatno je jednostavniji model upravljaj-održavaj (*OM - operate-maintain),* zasnovan na ugovornim uslovima u kojima privatni sektor upotrebom javnih dobara (čije vlasništvo ostaje u javnom sektoru) pruža određene usluge. Ovakav model se najčešće naziva i *outsourcing* ugovor. Pored navedenih modela, privatni sektor može od javnog da dobije dozvolu za pružanje javnih usluga sa ograničenim trajanjem, što se naziva operativna licenca (*OL - operation license*)[180]. Znatno složeniji je model je projektuj-izgradi-upravljaj (*DBO - design-build-operate*), koji započinje projektnim zahtjevom i specifikacijama od strane javnog sektora, koji je ujedno i finansijer. Privatni sektor u ovom slučaju ima obavezu projektovanja i izgradnje javnog dobra po fiksnoj cijeni. Nakon završetka izgradnje projekta privatni partner uzima dugoročno objekat u zakup koristeći ga za pružanje usluga[181].

Poseban model je izgradi-upravljaj-prenesi (*BOT - build-operate-transfer*) u kome privatni partner na osnovu projekta javnog sektora izgrađuje javno dobro i pruža usluge (pod kontrolom javnog sektora) koristeći predmetni objekat. Privatni partner naknadu za pruženu uslugu naplaćuje od javnog sektora ili krajnjih korisnika. Nakon isteka određenog perioda, javno dobro se vraća javnom partneru[182].

Poseban model obuhvata projektovanje, izgradnju, finansiranje i korišćenje (*DBFO - design-build-finance-operate*) od strane privatnog partnera. Pri tome korišćenje podrazumijeva dugoročni najam kroz upravljanje pružanjem usluga na osnovu ugovorenog broja godina. To je složeniji model u odnosu na izgradi-poseduj-upravljaj i prenesi (*BOOT - build-own-operate-transfer*). U ovom modelu na osnovu projekta javnog sektora, privatni sektor izgrađuje javno dobro. Nakon toga isto

[179] Schneider J.: *Public Private Partnerships for Urban Rail Transit*, Deutscher Universitats-Verlag, Wiesbaden 2004, p. 70

[180] Kačer H., Kružić D., Perković A.: Javno-privatno partnerstvo: atraktivnost DBFOOT modela, *Zbornik radovabr.3*, Pravni fakultet, Split, 2008, str. 610

[181] Hodge G., Greve C.: *The Challenge of Public–Private Partnerships, Learning from International Experience*, Edward Elgar Publishing, UK, 2005, p. 64

[182] Cartlidge D.: *Public Private Partnerships in Construction*, Taylor & Francis, 2006, p. 30

zadržava u vlasništvu, ali na određeno vrijeme i na osnovu ugovora za pružanje usluga. Treba napomenuti da se navedena naknadu naplaćuje od javnog sektora ili krajnjih korisnika. Kao i u prethodnom modelu nakon vremenskog perioda definisanog ugovorenim rokom, vlasništvo se prenosi javnom partneru i bez naknade[183].

Iz navedenih modela javno-privatnog partnerstva nedvosmisleno se može zaključiti da međusobne razlike proizilaze prvenstveno iz obima podjele uloga partnera u realizaciji projekta. Pored toga ne trebamo zaboraviti i ugovoreni način finansiranja, upravljanja, održavanja, podjele rizika i vlasničkog statusa izgrađene infrastrukture ili javnog objekta. Može se uočiti da ne postoji univerzalni model ili jedinstveni standard javno-privatnog partnerstva. Drugim riječima, svako javno-privatno partnerstvo je specifično, pri čemu je potrebno uzeti u obzir brojne faktore i parametre, a naročito spremnost partnera na saradnju i dogovornu alokaciju rizika.

Sprovođenje javno-privatnog partnerstva postalo je uobičajena strategija upravljanja u mnogim zemljama, posebno kada je u pitanju težnja za poboljšanjem javnih usluga i izgradnja velikih projekata javne infrastrukture. Partnerstvo u najširem poslovnom značenju predstavlja oblik poslovnog poduhvata i egzistira ako postoji dobrovoljno udruživanje dva ili više subjekata zajednički angažovanih kao poslovnih partnera u cilju sticanja dobiti. Pretpostavlja se da partnerstva postoje tamo gdje angažovani subjketi stvarno proporcionalno dijele profit i gubitke. U slučajevima uspostavljanja partnerstva, to podrazumijeva i sklopljen pisani sporazum o partnerstvu. Partnerstvo bez pismenog sporazuma, je u današnjoj praksi rijtko, podrazumijeva poslovni odnos dva ili više lica sa ciljem da se ostvari profit, a u zakonom dozvoljenim okvirima[184].

Argumenti u korist javno-privatnog partnerstva obično se odnose na uslove ugovora. Njihov relativno nedvosmislen karakter, sa jasnim odredbama vezanim za nadzor i sankcionisanje neizvršavanja ugovornih obaveza, daje im posebnu snagu.[185] Pored navedenog, u stručnoj literaturi se naglašava i značaj dužine trajanja ugovora, jer je u praksi privatnim partnerima potreban određeni period da povrate svoju početnu investiciju. U tom smislu, ugovori na dugi rok mogu doprinijeti ukupnom kvalitetu proizvoda ili usluga. Budući da javno-privatni projekti integrišu različite faze, izvođači su u mogućnosti i podstaknuti su da investiraju u bolje materijale u fazi izgradnje, kako bi kasnije imali manje troškove održavanja. To ukazuje da dugi ugovorni rokovi mogu biti povezani sa dobrim ukupnim performansama kao što su niži troškovi (ekonomičnost), bolji kvalitet usluga i proizvoda i inovativnija rešenja kao i savremeniji proizvodi. Dužina ugovornog perioda takođe stvara uslove za inovacije pružajući privatnim partnerima podsticaje da se pojave sa novim, inovativnim rešenjima u pogledu načina organizovanja procesa i proizvoda i usluga koje pružaju. Dodatne investicije potrebne za ove inovacije biće pristupačnije sa dugim ugovornim periodima tokom kojih postoji zagarantovani priliv sredstava.[186]

Uloga transakcionih troškova i vrsta odnosa ugovornih strana su bitna pitanja koja treba uzeti u obzir pri izboru tipa ugovora ili vrste upravljanja. U tom smislu, kada transakcije nisu česte i

---

[183] Konrad S. T.: *Management Control in Public-Private Partnerships, Between International Governmental Actors and the Private Sector,* Springer, 2018, p. 15

[184] Cartlidge D.: *Public Private Partnerships in Construction*, Taylor & Francis, 2006, p. 2

[185] Weihe G. : *Public–Private Partnerships: Meaning and Practice,* Copenhagen Business School, 2009, pp. 36-46

[186] Lenferink S., Tillema T., Arts, J.: Towards sustainable infrastructure development through integrated contracts: experiences with inclusiveness in Dutch infrastructure projects,*International Journal of Project Management*, 31 (4), 2013, pp. 615–627.

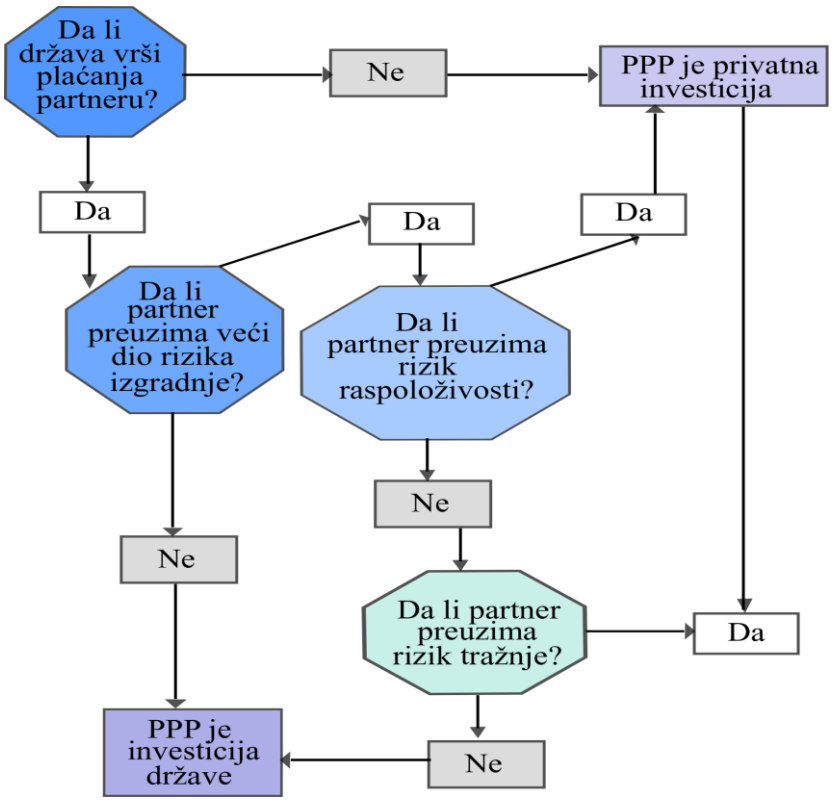
investicije preduzimaju unaprijed određeni partneri, postoji potreba za složenim i detaljnim ugovorima kojima se predviđaju sve moguće eventualnosti, ili uvode dodatni mehanizmi upravljanja. Treba imati u vidu da složeni projekti kojima se bavi javno-privatno partnerstvo nesumnjivo zahtijevaju određene transakcije. Shodno tome, potrebni su složeniji i razrađeniji ugovori kako bi se upravljalo ovim projektima ili, alternativno, predviđanje različitih oblika upravljanja (na primjer, veće učešće relacionih ugovora, kod kojih su stranke saglasne da je nemoguće ili neefikasno ugovorno definisanje potencijalnih teškoća i oklnosti realizacije ugovora). Prednost složenih ugovora je u tome što se njima mogu ugovoriti brojne različite stvari. U nedostatke takvih ugovora spada to što je njihovo sastavljanje skupo, jer je potrebno mnogo informacija i pregovora, što su manje fleksibilni i dovode do visokih transakcionih troškova za nadgledanje i implementaciju. Stoga se može pretpostaviti da je ugovor složeniji što je manja njegova ukupna efikasnost[187]. Na osnovu navedenog, može se zaključiti da složenost ugovora negativno utiče na ukupni učinak javno-privatnog partnerstva, dok s druge strane ugovori dužeg trajanja se pozitivno odražavaju na bolje performanse i omogućavaju inovacije u ostvarivanju projekata javno-privatnog partnerstva.

Jedna od karakteristika ugovora javno-privatnog partnerstva je primjena sankcija. Imajući u vidu mogućnost nepredviđenih budućih dešavanja, država mora da ima instrumente da utiče na ponašanje i performanse privatnog partnera tokom perioda ugovora. Da bi se to postiglo, ugovori mogu da uključe i primjenu pozitivnih i negativnih mjera (sankcija) tokom primjene ugovora[188]. To znači da u ugovoru moraju biti navedeni indikatori performansi, kao i sistem praćenja. Osnovne ideje o tome uglavnom potiču iz neoinstitucionalističke ekonomije. Sa te tačke gledišta, specifične investicije (znanje, novac, materijal) koje partneri ulažu u javno-privatno partnerstvo čine ove partnere ranjivim. Naime, u pitanju su specifična ulaganja usmjerena u aktivnosti ili proizvode koji se ne mogu lako koristiti u drugim projektima. To čini partnera koji investira zavisnim od druge ugovorne strane, što može dovesti do oportunističkog ponašanja, poput smanjenja ili ušteda na kvalitetu. Stoga je od presudne važnosti da izvođač radova (glavni nalogodavac) bude u mogućnosti da kontroliše i sankcioniše izvođača ugovora ako isti ne isporuči obećani proizvod i obećani kvalitet. Iz tih razloga se pretpostavlja da ugovorna prijetnja sankcijama doprinosi uspješnosti javno-privatnog partnerstva[189].

[187] Klijn H. E., Koppenjan J.: The impact of contract characteristicon the performance of public–private partnerships (PPPs), *Rublic Money & Management*, 36(6), 2016, pp. 455-462

[188] Velde van de D., Veeneman W.,Schipholt L. L. : Competitive tendering in The Netherlands: central planning vs. functional specifications,*Transportation Research Part A: Policy and Practice*, 42, (9), 2008, pp. 1153–1160

[189] Koppenjan J. F. M.: The formation of public–private partnerships: lessons from nine transport infrastructure projects in The Netherlands, *Public Administration*, 83, (1),Blackwell Publishing, Oxford 2005, pp. 144–150



Šema br. 1.: Odlučivanje u postupku podjele rizika[190]

Pored navedenih, jedna od bitnih karakteristika je da pri udruživanju svaki od navednih sektora preuzima one rizike kojima najefikasnije upravlja (Šema br. 1). Rizik se definiše kao neizvjesnost ishoda, bilo da je u pitanju pozitivna prilika, ili je riječ o negativnim prijetnjama, akcijama i događajima. U pristupu upravljanju projektom rizik predstavlja događaj koji se može ali ne mora dogoditi, a koji bi mogao dovesti do prekoračenja troškova, kašnjenja u završetku projekta ili neispunjavanja nekih projektnih zahtjeva. U području ekonomije i finansija rizik ima nešto drugačije značenje, pri čemu ima jaču i slabiju stranu. Naime, strana suočena sa rizikom trpi posledice negativnih događaja, ali može imati koristi od pozitivnog razvoja situacije. Na ovaj način će ugovorna strana imati veće podsticaje i motive za ulaganje napora u sprečavanju negativnih ishoda[191].

U procesu ostvarivanja javno-privatnog partnerstva egzistira veliki broj rizika koji se mogu svrstati u određene kategorije. U grupu projektovanja, izgradnje i vođenja poslova spadaju rizici vezani za eventaulna kašnjenja, te prekoračenje planiranih troškova projektovanja i izgradnje. Pri tome se najveći broj ovih rizika prebacuje na privatni sektor, uz korišćenje različitih mehanizama kao što je specifikacija proizvoda ili način na koji se plaćaju završni radovi. Rizici iz grupe operative i održavanja se takođe po pravilu dodjeljuju privatnom sektoru. Ova grupa obuhvata rizike koji se odnose na okolnosti da vođenje posla i održavanje koštaju više od planiranog. Finansijski rizici čine posebnu kategoriju i odnose se na povećanje kamatnih stopa, inflacije i stope poreza. Nosilac ove

[190] *The EIB role in Public-Private Partnerships*, European Investment Bank, Luxembourg, 2004, p. 20
[191] Graeme A. H. Carsten G., Anthony E. B. : *International Handbook onPublic–Private Partnerships*, Edward Elgar Publishing, UK, 2010, p. 263

grupe rizika je obično privatni sektor, pri čemu kod dugoročnih projekata rizik od inflacije snose zajednički javni i privatni partneri. Pored navedenih, često se definišu i rizici zbog više sile koji se odnose na vremenske neprilike ili druge događaje koji mogu biti uzročnici materijalnih gubitaka, štete na imovini ili koji na drugi načini sprečavaju izvršavanje posla, a koji su po svojoj prirodi izvan kontrole partnerskih strana. Zbog toga se rizici više sile uglavnom dijele zajednički[192].

3.3. Načelna organizaciona struktura javno-privatnog partnerstva

Fleksibilna priroda javno-privatnog partnerstva ohrabruje razvoj i prilagođavanje postojećih struktura kao odgovor na pojedinačne potrebe i specifikacije svakog projekta i projektnog partnera. Modeli koji se koriste u javno-privatnom partnerstvu u skladu su sa predviđenim funkcijama i spektrom relevantnih faktora, što uključuje sektor u kojem se projekat odvija i rizike povezane sa projektom, kao i pitanja da li je infrastruktura sposobna da sama generiše prihod ili će uvijek biti obezbijeđena po trošku vlade, da li postoje mogućnosti da infrastrukturu koriste nedržavni subjekti, da li postoje aspekti projekta koji su u vlasništvu ili pod nadzorom vlade (na primjer, zemljište) i da li postoji konkurencija u pogledu infrastrukture i potreba za regulisanjem pristupa i cijena[193].

Sa aspekta organizacione strukture, javno-privatno partnerstvo okuplja brojne subjekte vezane za investiranje u infrastrukturu, obično u formi projektne kompanije (*special purpose vehicle - SPV*), koja se osniva samo u tu svrhu. Posmatrano pojedinačno, najvažniji subjekti u određenom projektu JPP su:

- partner iz javnog sektora (javno tijelo ili vlada, lokalne samouprave i agencije, preduzeća u državnom vlasništvu) koji ugovara nabavke usluge ili javnog dobra,
- privatni partner koji zaključuje ugovor sa javnim sektorom
- finansijeri,
- podizvođači i
- drugi učesnici kao što su pravni, finansijski, tehnički savjetnici, osiguravači, rejting agencije i drugi[194].

U projektu javno-privatnog partnerstva svaki od učesnika koji se uključuje u projektnu kompaniju zadržava svoj identitet i odgovornost, i u *SPV* djeluje na osnovu jasno definisane podjele zadataka i rizika (Šema br.2). Projektna kompanija je posebno pravno lice koje se osniva za sprovođenje aktivnosti definisanih ugovorom između kompanije i klijenta, u ovom slučaju javnog partnera. S obzirom da je za realizaciju javno-privatnog partnerstva neophodno uključiti više strana, projektna kompanija sklapa podugovore sa različitim organizacijama i drugim subjektima u cilju izvršenja planiranih aktivnosti. Razlozi za korišćenje organizacionog oblika kakva je projektna kompanija su:

---

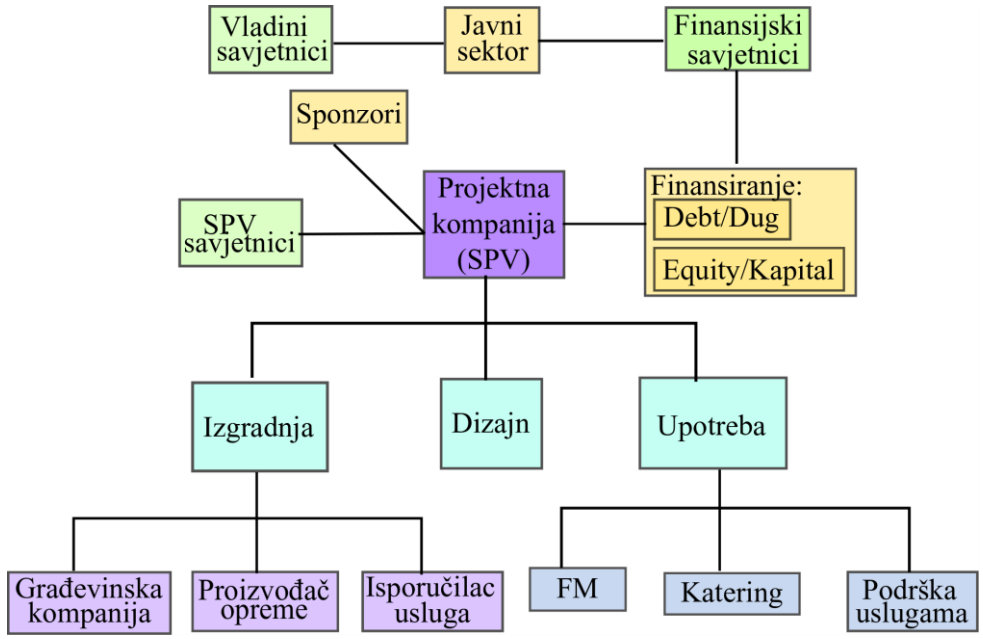
[192] Persoli M.A.: Javno-privatno partnerstvo u funkciji zadovoljavanja javnih potreba, *Hrvatska javna uprava, br.4*, Pravni fakultet, Zagreb, 2010, str. 1025-1026

[193] Graeme H., Carsten G.: *The Challenge of Public–Private Partnerships, Learning from International Experience*, Books Ltd, Bodmin, Cornwall, 2005, p. 63

[194] Grimsey D., Lewis K. M.: *Public private partnerships-the world wide revolution in Infrastructure Provision and project Finance*, Edward Elgar Publishing Limited, UK, p. 108

- da omogući da kreditiranje projekta ne bude dozvoljeno sponzorima sa strane zbog same prirode ograničene odgovornosti projektne kompanije,
- da obezbijedi da se kao sredstva i obaveze projekta ne pojavljuju sponzorski bilansi stanja, zbog toga što nijedan učesnik u projektu nema više od 50 % udjela u projektnoj kompaniji, kao i da osigura i primjenu opštih principa konsolidacije prilikom pripreme grupnih računa, i
- da brine o interesima projektnih zajmodavaca, kako bi se pomoglo da projekat ne uđe u rizik od potencijalnog bankrota bilo kojeg od investitora („udaljenost od bankrota“)[195].

Dva pristupa ilustruju generički oblik konzorcijuma koji obično uključuje finansijere duga (često u konzorcijumu koji djeluje preko određene banke), ulagače u kapital i sponzore (koji ulažu u očekivanu dobit projekta i stoga su izloženi i rizicima), projektante i (ili) građevinske izvođače i operatore. U pogledu toga koje strane preuzimaju vodeću ulogu u organizovanju aranžmana i sastavljanju ponuda, postoje dva alternativna pristupa: tradicionalni pristup upravljanju izgradnjom i objektima i novi pristup, koji karakteriše vodeća uloga finansijera.



Šema br. 2.: Uobičajena organizacija javno-privatnog partnerstva[196]

U organizacionom pogledu javno-privatno partnerstvo može imati dva pristupa koja zavise od toga koje strane predvode organizaciju realizacije projekta. Tradicionalni pristup (karakterističan za Veliku Britaniju) podrazumijeva da ugovorne strane imaju većinski udio u kapitalu projektne kompanije od početka do okončanja projekta. Shodno tome, one preuzimaju i ključnu odgovornost i obaveze prema projektu, posebno u vezi sa rokovima i finansijskom konstrukcijom. Manjinski udio

[195] Graeme H., Carsten G.: *The Challenge of Public–Private Partnerships, Learning from International Experience*, Books Ltd, Bodmin, Cornwall, 2005, p. 109
[196] Grimsey D., Lewis K. M.: *Public private partnerships-the world wide revolution in Infrastructure Provision and project Finance*, Edward Elgar Publishing Limited, UK, p. 110

u dioničkom kapitalu projektne kompanije imaju finansijeri, a ukoliko se radi o investitorima na dugi rok, koji su pritom i posebno finansijski zainteresovani, može im se prepustiti ključna uloga u projektu JPP nakon što faza izgradnje bude okončana.

Finansijski vođeni pristup javno-privatnom partnerstvu (karakterističan za Australiju) do izražaja je došao u poslednjih nekoliko godina. Za taj pristup je karakteristična mnogo izraženija uloga specijalizovanih investicionih banaka, koje su uključene od samog početka realizacije projekta kroz upravljanje projektnom kompanijom. Uloga tih banaka je posebno značajna ne samo zbog investiranja kapitala u projektnu kompaniju već i zbog učešća u raspisivanju tendera, odlučivanja o cijenama, davanja garancija za komercijalne prihode od projekta, kao i garancija za dug *(senior debt)* i učešća u angažovanju kompanija izvođača putem akreditiva izdatog držaocima duga i slično. S obzirom na činjenicu da investiciona banka nije u mogućnosti da samostalno realizuje navedene obaveze, prinuđena je da zaključuje ugovore sa ostalim zainteresovanim subjektima za formiranje konzorcijuma projekta. S druge strane, specijalizovana investiciona banka je jedini ulagač kapitala u projektnu kompaniju i ujedno garant svih aktivnosti vezanih za projekat koje se odnose na tržište kapitala[197].

Opredeljivanje o tome koji je od navedenih pristupa prihvatljiviji sa aspekta javno-privatnog partnerstva, uz vaganje njihovih prednosti ili nedostataka, veoma je nezahvalno zbog činjenice da je tu riječ o aranžmanima koji se protežu na duge rokove, često i na 20-30 godina. U vezi sa tim, moguće je uočiti i potencijalne probleme s obzirom na prirodu partnerstva u dugom vremenskom okviru, kao i rizike koji se tiču performansi projekta, posebno u okolnostima decentralizovanog finansiranja i disperzije obaveza kroz sistem podugovora. Ako posmatramo iz ugla prirode partnerstva, prednost bi trebalo da ima tradicionalni pristup. Jedan od razloga za to je uravnoteženo učešće u kapitalu projektne kompanije, u okviru koje se usaglašavaju interesi zainteresovanih strana, uz vođenje računa o javnom interesu, što predstavlja pouzdan osnov za kvalitetno i u dužem vremenu održivo partnerstvo. Pored toga, kod ovog pristupa postoji veza između realizacije projekta, odnosno kvaliteta isporučenih usluga, sa učešćem u kapitalu projektne kompanije i rizicima koje snose ugovorne strane. U odnosu na finansijski vođen model JPP ove veze su znatno transparentnije. Kada se radi o finansijski vođenom pristupu, gledano sa aspekta smanjenja transakcionih troškova, evidentna je prednost postupka koji je pod nadležnošću i kontrolom poslovne investicione banke. Naime, objedinjeni proces ima svoje prednosti jer omogućava banci da u potpunosti kontroliše finansijski aranžman koji se odnosi na projekat. O tome svedoče i aktuelni trendovi na tržištu kapitala namijenjenog finansiranju projekata javno-privatnog partnerstva. U novije vrijeme su uočljiva značajna pomjeranja od tradicionalnog projektnog finansiranja preko metoda korporativnog finansiranja ka emisiji obveznica institucionalnih investitora. Zato nije slučajnost da pojedine banke imaju posebne fondove namijenjene društvenoj infrastrukturi radi lakšeg povezivanja novčanih tokova projekata javno-privatnog partnerstva sa ovim fondovima[198].

Savjetnici kao strana u projektima javno-privatnog partnerstva imaju ulogu da obezbeđuju i pružaju finansijske, pravne, tehničke i ostale savjete, kako javnom tako i privatnom partneru u procesu strukturisanja projekata JPP. Nacionalne vlade se oslanjaju na savjetnike u sprovođenju i obezbjeđivanju nezavisne kontrole svakog projekta predmetnog partnerstva, doprinoseći na taj način

[197] Ibidem, pp. 110, 229
[198] Ibidem, p. 111

stvaranju dodatne vrijednosti u postupku javnih nabavki. Sponzori za pripreme učešća na tenderu koriste kako spoljne savjetnike, kao i ekspertske timove iz redova sopstvenih zaposlenih. Finansijeri se obično oslanjaju na svoje timove savjetnika, uz povremeno angažovanje spoljnih konsultanata, radi procjene finansijske opravdanosti projekta i rizika u vezi s prihodima, kao i instrumenata obezbjeđenja.[199]

Javni sektor je jedno ili više javnih tijela, odnosno pravno lice koje je u skladu sa zakonom nadležno za davanje koncesije, koje s privatnim partnerom zaključuje javni ugovor, ili jedno ili više javnih tijela koje je s privatnim partnerom povezano članstvom u zajedničkom privrednom društvu. U organizacionoj strukturi javno-privatnog partnerstva javni sektor može imati različite odgovornosti. I pored toga, vlada zadržava stalni interes za kvalitet i održivost usluge, jer je odgovorna za definisanje ciljeva, kao i za procjenu da li su projekat i usluge isporučene u skladu sa definisanom politikom, standardima i javnim interesom uopšte. Nezavisno od različitih modela organizacione strukture javno-privatnog partnerstva, javni sektor ima odgovornost za određivanje potrebnog projekta ili usluge, prioriteta, ciljeva i rezultata, kao i mogućnosti izdvajanja iznosa sredstava javnog sektora. Pored navedenog, javni sektor ima posebno značajnu ulogu u nadgledanju implementacije ugovora putem primjene pomenutih standarda, kao i preduzimanja adekvatnih mjera i aktivnosti ukoliko one nisu ispunjene. Nadležnost javnog sektora je i u određivanju načina mjerenja performansi putem uspostavljanja monitoring sistema, kao i sistema evaluacije kvaliteta i ispunjavanja standarda. Kada se razmatra javni sektor iz ugla organizacije, od velikog su značaja razna regulatorna tijela i pojedine institucije javnog sektora, posebno u različitim fazama implementacije javno-privatnog partnerstva. Njihova uloga je evidentna i prilikom izdavanja raznih vrsta dozvola, licenci i potvrda neophodnih za realizaciju projekata javno-privatnog partnerstva. Uopšteno posmatrano, regulatorna tijela kreiraju cjelokupni okvir u kojem se implementira javno-privatno partnerstvo[200].

Privatni partner je svako domaće ili strano fizičko, odnosno pravno lice, ili konzorcijum jednog ili više takvih fizičkih ili pravnih lica odabranih u postupku javne nabavke ili u postupku davanja koncesije. Privatni partner s javnim partnerom zaključuje javni ugovor, ili u tu svrhu osniva društvo posebne namjene, ili sa javnim partnerom osniva zajedničko privredno društvo.

Kao učesnici u postupku i podnosioci ponude mogu se pojaviti i grupe privrednih subjekata. Javna tjela nisu u obavezi da od istih zahtijevaju da imaju određenu pravnu formu radi učestvovanja u postupku. Kada se u postupku ponuda učesnika ocijeni kao najpovoljnija, po dodjeli javnog ugovora, zahtijeva se određena pravna forma. Projektna kompanija se osniva u cilju realizacije javnog ugovora, kao i u slučajevima institucionalnog javno-privatnog partnerstva, kada takvo društvo ne postoji, i može učestvovati isključivo u sprovođenju projekta predmetnog partnerstva u čiju svrhu je osnovano, osim ako predlogom projekta nije drugačije određeno. Projektna kompanija je posebno pravno lice osnovano kao privredno društvo, s jedinstvenim ciljem sprovođenja koordinacije i zastupanja aktivnosti precizno definisanih ugovorom između projektne kompanije i javnog sektora[201].

---

[199] Yescombe R. E.: *Public–Private Partnerships Principles of Policy and Finance*, Elsevier Published, 2007, p. 111.
[200] Cvetković P., Sredojević S.: *Javno-privatno partnerstvo, priručnik za sprovođenje na nivou lokalne samouprave*, Stalna konferencija gradova i opština, Beograd, 2013, str. 19
[201] Sredojević S.: *Javno-privatno partnerstvo,* Arhipelag, Institut ekonomskih nauka, Beograd, 2010, str. 29-30

S obzirom na činjenicu da obavljanje različitih aktivnosti u realizaciji projekta zahtijeva uključenost brojnih aktera, na bazi podugovora projektna kompanija prenosi izvršenje niza zadataka drugim organizacijama. U tom smislu, projektna kompanija predstavlja centar organizacione strukture svakog javno-privatnog partnerstva. U vezi sa tim, ističe se da predstavljanje projektne kompanije kao akcionarskog društva obezbjeđuje neometano finansiranje projekta od strane sponzora, te da projektna kompanija daje sigurnost i zaštitu kreditorima (finansijerima), jer otklanja rizike neuspjeha projekta usled potencijalnog bankrotstva bilo kojeg od sponzora. Osnovne odgovornosti sponzora i ostalih akcionara u projektnoj kompaniji odnose se na ispunjavanje ugovornih obaveza koje uključuju izradu i dostavljanje definisanog projekta izgradnje ili obezbjeđenja usluga u skladu sa postavljenim standardima, planiranje i izgradnju projekta infrastrukture, prikupljanje sredstava za kapitalne potrebe projekta i usmjerenost na ciljeve vlade, posebno u okolnostima kada dolazi do promjene okruženja u kome se projekat realizuje[202].

U sprovođenju aktivnosti na projektu javno-privatnog partnerstva, ponuđač ima pravo da angažuje podizvođače. U konkursnoj dokumentaciji i nacrtu javnog ugovora, javno tijelo može da zahtijeva od ponuđača da u ponudi navede dio vrijednosti ugovora u procentima za koji namjerava da zaključi ugovor sa podizvođačima. U tom slučaju, ponuđač je neograničeno solidarno odgovoran za izvršenje ugovornih obaveza.U okolnostima kada podugovaranje nije navedeno u ponudi, podugovor se ne može zaključiti bez prethodne saglasnosti javnog partnera. Kada se radi o podugovaranju takva mogućnost postoji u okolnostima kada podizvođač ispunjava uslove iz ugla ekonomskog i finansijskog stanja za izvršenje profesionalne djelatnosti. Pored toga značajne su i njegove tehničke i/ili stručne osposobljenosti za ostvarivanje svog dijela ugovornih obaveza. Treba napomenuti da projektna kompanija preko specijalizovanih podugovarača izvršava obaveze i odgovornosti prema javnom sektoru. Podugovarači u tradicionalnom modelu strukture javno-privatnog partnerstva najčešće imaju učešće u njenom kapitalu. Aktivnosti koje su obično prenijete podugovaračima su izgradnja, nabavka opreme, funkcionisanje i održavanje, ali je značajno da je svaka od navedenih aktivnosti na njih prenijeta posebnim ugovorom[203].

Organizaciona struktura javno-privatnog partnerstva podrazumijeva da je projektna kompanija akcionarsko društvo u čijem kapitalu učešće mogu da imaju jedna ili više banaka, građevinska kompanija i sponzori. Aranžmani za finansiranje projektne kompanije obično se sklapaju u trenutku kada se zaključuju i ugovori i podugovori. Ovaj trenutak se zove zatvaranje finansijske konstrukcije, za čiju realizaciju je neophodno ispunjenje osnovnog preduslova koji zahtijeva da projekcija prihoda mora da omogući obezbjeđenje finansijskim institucijama i podsticaj za učešće u kapitalu. Drugim riječima, neophodno je formirati kompaniju kao privredno društvo, jer ona može da predstavlja i zastupa samu sebe, ali i da ima nivo rizičnosti koji je prihvatljiv za finansijere. Učešće duga u odnosu na kapital određuje se za svaki projekat ponaosob, tako da 80% sredstava može da ima porijeklo u dugu, a 20% u obliku učešća u kapitalu koji obezbjeđuju investitori projektne kompanije. Pored navedenog, može se pojaviti i subordinirani dug u obliku zajma ili hartija od vrijednosti koje imaju nižu kategoriju u odnosu na ostale zajmove, sa aspekta prioriteta u naplati. Kreditori koji u svojim bilansima imaju subordinirani dug nemaju prioritet u naplati svojih potraživanja sve dok se u

[202] Grimsey D., Lewis K. M.: *Public private partnerships-the world wide revolution in Infrastructure Provision and project Finance*, Edward Elgar Publishing Limited, UK, p. 26
[203] Yescombe R. E.: *Public–Private Partnerships Principles of Policy and Finance*, Elsevier Published, 2007, pp. 86-87

potpunosti ne izvrši isplata primarnim kreditorima. To znači da je subordinirani dug rizičniji od ostalih dugova. Ipak, nesumnjivo je pravilo da sve finansijske obaveze moraju biti izmirene u vrijeme trajanja ugovora. Usled činjenice da je izvjestan dio troškova izgradnje finansiran neobezbijeđenim dugom, tržišta privatnog kapitala moraju biti u stanju da obezbijede značajne sume kapitala unaprijed. Strukture javno-privatnog partnerstva su veoma pogodne za kapitalno intenzivne infrastrukturne projekte. Razlog tome treba tražiti u činjenici da podjela rizika projekta između brojnih učesnika stvara atmosferu uzajamnog interesa, jer svako gubi ako projekat bude neuspješan. S druge strane, finansijeri su sigurni da su svi učesnici veoma zainteresovani da rade zajedno u cilju rešavanja spornih pitanja koja će se javiti u toku implementacije projekta[204].

3.4. Razvoj javno-privatnog partnerstva u Evropi

Francuska je po pitanju javno-privatnog partnerstva specifična, jer u toj državi ne postoji posebna politika u ovoj oblasti. To je posledica činjenice da se predmetni koncept smatra starim i dobro poznatim i razrađenim. Naime, francuski model javno-privatnog partnerstva nastao je prije više od sto godina u različitim formama, pri čemu je model koncesija ostao jedan od najzastupljenijih načina izgradnje i upravljanja javnim uslugama i javnom infrastrukturom u Francuskoj. Inače, počeci javno privatnog partnerstva u toj zemlji zabilježeni su još u XVII vijeku.

Prvi koncesioni ugovori u Francuskoj dodijeljeni su za izgradnju i finansiranje kanala de Brijar 1638. godine i Mediteransko-Atlantskog kanala 1666. godine, a potom i raznih drugih oblika infrastrukture, kao što su mostovi i tuneli. Na osnovu koncesionog ugovora, privatnim kompanijama je bila omogućavana franšiza za obezbjeđenje javnih usluga na određeni vremenski period. Dugogodišnje francusko iskustvo sa koncesijama u sektoru vodovoda potiče još iz 1782. godine. Naime, tada je braći Perije dodijeljena prva koncesija za obezbjeđenje sistema distribucije vode u sve djelove Pariza. Jedan od najpoznatijih primjera partnerstva sa privatnim sektorom putem sistema koncesija u području infrastrukture predstavlja Suecki kanal. Koncesija je dodijeljena od strane turskog vicekralja Egipta 1854. godine, a kanal je završen 1869. godine. Koncesija je imala period trajanja od 99 godina, sa početkom od dana otvaranja kanala za saobraćaj. Zbog političkih okolnosti koje su nastale polovinom XX vijeka u Egiptu, ovaj ugovor je prekinut prije isteka koncesije, jer je Kompanija Sueckog kanala bila nacionalizovana 1956. od strane egipatske vlade[205]. Treba napomenuti i da su od XVII vijeka mnogi kanali i mostovi u Francuskoj izgrađeni davanjem vladinih koncesija za saobraćajnu infrastrukturu privatnim firmama. Međutim, u toj zemlji na taj način funkcionišu i brojne druge javne službe, kao što su vodovod, kanalizacija, odvoz i tretman smeća, gradski prevoz, objekti za kulturu, sport i socijalna pitanja, kojima upravljaju privatne kompanije. Od ovih kompanija se očekuje da posluju u okviru javnog interesa utvrđenog u nacionalnom zakonodavstvu. Najvažniji institucionalni oblik privatnog učešća u javnim službama u Francuskoj odavno je Société d`économie mixte (SEM), koji datiraju od takozvanog Poenkareovog dekreta iz 1926. godine, kada su lokalne vlasti dobile opštu nadležnost u području upravljanja uslugama na tim područjima, direktno ili kroz finansijsko učešće u firmama.

[204] Sredojević S.: *Javno-privatno partnerstvo,* Arhipelag, Institut ekonomskih nauka, Beograd, 2010, str. 31-32
[205] Sredojević S.: *Javno-privatno partnerstvo,* Arhipelag, Institut ekonomskih nauka, Beograd, 2010, str. 66

Njemačka od 1945. godine razvija tradiciju „državnog partnerstva“ sa privatnim sektorom, o čemu svedoče brojni primjeri uticaja državnog vlasništva u glavnim industrijskim preduzećima kao što su Folksvagen i Lufthansa na nacionalnom nivou, kao i brojni primjeri na regionalnom nivou. Iako su njemački primjeri možda najpoznatiji, državni holding je uobičajen i u drugim evropskim zemljama, poput Italije i Francuske, dok u Austriji glavne nacionalizovane banke služe kao državni holding za privatne firme[206]. Međutim, kada se radi o njemačkom slučaju, u odnosu između javnog i privatnog sektora nedostaje prava partnerska podjela. Naime, takvo partnerstvo je uglavnom održavano u cilju ostvarivanja većeg stepena kontrole države nad strateškim odlukama koje utiču na određene grane industrije i privrede, a koje su od posebnog značaja za budućnost cjelokupne nacionalne ekonomije.

U cilju potpunije slike razvoja koncepta javno-privatnog partnerstva neophodno je napomenuti da je kroz veći dio XX vijeka angažman privatnog sektora realno opadao. Kao osnovni razlozi za to uzimaju se svetski ratovi koji su zaustavili opšti rast i razvoj, povećana državna kontrola i nedostatak slobodnog tržišta u mnogim zemljama, naftna kriza 1970-ih godina, te periodi ekonomskog pada. Počev od kasnih 80-ih godina prošlog vijeka došlo je do pomaka u smislu povećavanja uloge privatnog sektora u obezbjeđenju infrastrukturnih sredstava i pružanju socijalnih usluga. U ovom periodu su mnoge države poboljšale svoje pravne okvire i odgovarajuće procedure kako bi pomogle jačanju javno-privatnog partnerstva i procesa privatizacije, što je doprinijelo većoj primjeni finansiranja infrastrukture korišćenjem modela saradnje javnog i privatnog sektora[207].

Na razvoj javno-privatnog partnerstva u mnogome je uticala i makroekonomska kriza 1970-ih i početkom 1980-ih godina XX vijeka, koja je zbog narastanja javnih dugova stvorila pritisak na vlade mnogih zemalja da revidiraju uobičajeni model javnih nabavki i da u sve većoj mjeri prihvataju koncept javno-privatnog partnerstva. Sam termin javno-privatno partnerstvo se masovnije koristi od 1980-ih godina, kada je privatni sektor aktivnije uključen u kontekst definisanja tendencija urbanog razvoja u SAD i Velikoj Britaniji. Krajem XX vijeka, trend privatizacije u tom području je u određenoj mjeri izgubio na popularnosti, ali je opšta potreba za infrastrukturnim razvojem ostala. To je uticalo da saradnja javnog i privatnog sektora postane prijeko potrebno sredstvo za angažovanje privatnih ulaganja u cilju infrastrukturnih investicija. Navedeno upućuje na zaključak da značaj modela javno- privatnog partnerstva leži u mogućnosti da se javne investicije u manjoj mjeri nego do sada prevaljuju na budžetske troškove. Po ocjeni relevantnih međunarodnih organizacija, i pored određenih kritika koje mu se mogu uputiti, najbolje razvijeni model u toj oblasti je britanski program, koji pokriva preko 14% javnih investicija u najvažnijim infrastrukturnim oblastima[208].

Uopšteno posmatrano, koncept javno-privatnog partnerstva se vezuje za proces reforme države. S druge strane, praksa s kraja prošlog vijeka pokazuje da je ovaj model saradnje u većini država imao uticaj i primjenu prvenstveno u malim i srednjim kompanijama. Uglavnom izvan njegovog dometa ostale su pojedine grane (struja, gas, voda, nafta i avio saobraćaj i slično) koje preko javnih preduzeća i dalje kontroliše državni aparat. Razloge za to treba tražiti prvenstveno u strateškom značaju ovih oblasti za državu, monopolskom položaju tih preduzeća, pa i lobiranju sindikata u njima

[206] Bing L., Akintoye A.: An overview of public–private partnership, In: Akintoye A., Beck M., Hardcastle C. (eds): *Public–Private Partnerships: Managing Risks and Opportunities*, Blackwell Oxford, 2003, p. 13.
[207] *Public-Private Partnerships A Basic Introduction for Non-Specialists*, Economics and Private Sector Professional Evidence and Applied Knowledge Services UK, 2017, p.11
[208] International Monetary Fund: *Public-private partnerships*, 2004, p. 5

protiv javno-privatnog partnerstva. Ipak, i ovdje postoji jedan izuzetak koji se odnosi na područje telekomunikacija i informatike, a posledica je ubrzanog tehnološkog razvoja, kao i činjenice da se privatni sektor znatno brže prilagođava novonastalim promjenama uopšte, pa i u ovoj oblasti.[209].

3.4.1. Normativni aspekt javno-privatnog partnerstva u Evropskoj uniji

Evropska komisija je u dosadašnjem periodu preduzimala različite inicijative u vezi s procedurama za javne nabavke u pogledu definisanja zakonskog okvira za PPP. Tako je 2000. godine Evropska komisija objavila dokument pod nazivom „Tumačenje saopštenja o koncesijama u zakonu o javnim nabavkama Evropske zajednice“ (*Interpretive Communication of the Commission on concessions in Community Public Procurement Law*)[210]. Dokument naglašava da bilo koji ugovorni akt kojim javni sektor povjerava izvođenje ekonomskih aktivnosti trećoj strani mora biti u skladu s pravilima i principima izvedenim iz Rimskog ugovora, a naročito sa principima slobode osnivanja kompanije i slobode obezbjeđivanja usluga[211], čime se podržavaju načela transparentnosti, jednakosti tretmana, proporcionalnosti i uzajamnog raspoznavanja.

Insistiranjem na poštovanju ovih principa dokument definiše okvire koncepta koncesija u zakonu o javnim nabavkama i propisuje obaveze kojih su dužni da se pridržavaju predstavnici javnog sektora kada vrše selekciju koncesionara i dodjeljuju koncesiju. Dalje detaljne inicijative u cilju koordinacije procedura za dodjeljivanje javnih ugovora uslijedile su 31. marta 2004. godine, kada su objavljene Direktive Evropskog parlamenta i Savjeta, izrađene u cilju modernizacije i pojednostavljivanja pravnog okvira EU:

1. Direktiva 2004/18/ES Evropskog parlamenta i Savjeta u vezi s koordinacijom procedura za dodjeljivanje ugovora o javnim radovima, nabavkama i uslugama[212],
2. Direktiva 2004/17/ES Evropskog parlamenta i Savjeta u vezi s koordinacijom procedura za dodjeljivanje ugovora u sektorima vodosnabdijevanja, energetike, transporta i poštanskih usluga[213].

Pojava nove, inovativne procedure selekcije poznate pod nazivom „konkurentni dijalog“ (*competative dialogue*) koju ove direktive uvode, omogućila je ispunjavanje specifičnih zahtjeva dodjeljivanja kod "posebno kompleksnih ugovora", što se direktno odnosi na određene forme PPP. Ova nova procedura omogućava javnom sektoru (vladama) da održava pregovore s prijavljenim kandidatima u cilju postizanja rešenja koja na najpovoljniji način zadovoljavaju potrebe javnog sektora. Ove Direktive imaju za cilj da:

– zaštite interese kompanija osnovanih u nekoj zemlji članici EU, koje žele da ponude dobra ili usluge institucijama javnog sektora osnovanih u drugoj zemlji članici EU,

---

[209] Ibidem, p. 4

[210] *Interpretive Communication of the Commission on concessions in Community Public Procurement Law*

[211] *Treaty establishing the European Economic Community*, art. 43, 49, dostupno na: http://data.europa.eu/eli/treaty/teec/sign

[212] Directive 2004/l8/EC of the European Parliament and of Council of 31 March 2004 relating to the coordination of procedures for the award of public works, supply and services contracts

[213] Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 relating to the coordination of procedures for the award of contracts in the water, energy, transport and postal services sectors

- izbjegnu rizik preferencije koju uživaju domaći učesnici na tenderu kada se ugovor dodeljuje od strane javnog sektora,
- izbjegnu mogućnosti da institucija koja pripada javnom sektoru u toku procesa selekcije bude rukovođena bilo kojim drugim kriterijumima osim ekonomskim.

Navedne direktive su doprinijele određenom stepenu harmoizacije zakonodavstva u ovoj oblasti. Međutim, ispostavilo se da su mnoga pravila o slobodnom izboru kompanija u ovim partnerskim projektima ostala nejasna, što je ukazalo na potrebu potpune usklađenosti među državama članicama Unije. U cilju otklanjanja neusklađenosti i prisutnog stepena neizvjesnosti, kao i uklanjanja uočenih prepreka za uspješnu realizaciju projekta javno-privatnog partnerstva, Evropski parlament je pozvao Evropsku komisiju da ispita mogućnosti za usvajanje direktive čiji bi cilj bio uvođenje homogenih pravila za koncesije i ostale oblike javno-privatnog partnerstva.

Evropska komisija je pristupila izradi dokumenta konsultativnog karaktera, tzv. Zelene knjige o PPP i Zakonu Evropske zajednice o javnim ugovorima i koncesijama[214] (*Green Paper on PPPs and Community Law on public contracts and concessions*), koja je u isto vrijeme i aktivnost predviđena Evropskom inicijativom za postizanje rasta. Cilj ovog konsultativnog procesa je da otvori debatu o primjeni koncepta javno-privatnog partnerstva u zakonu Evropske zajednice o javnim ugovorima i koncesijama, koja se koncentriše na pravila koja javni sektor treba da poštuje kada se donosi odluka o dodjeli posla nekoj trećoj strani. Ovo se odnosi isključivo na ekonomski i organizacioni aspekt, ali ne i na samu projcenu vrijednosti odluke o tome da li će upravljanje javnom uslugom biti dato trećoj strani ili ne, jer ova odluka isključivo ostaje u nadležnosti javnog sektora. Zato je zakon Evropske zajednice o javnim ugovorima i koncesijama neutralan u vezi sa izborom koji se nalazi pred zemljom članicom EU da li će javno dobro ili uslugu obezbijediti sama ili će njenu realizaciju povjeriti trećoj strani (partneru privatnog sektora). Zelena knjiga je posebno značajna jer je njena svrha određivanje pravila prilikom dodjele partnerstva privatnim partnerima i postizanje otvorenijeg pristupa partnerstva u tržišnom nadmetanju u transparentnijem pravnom okruženju[215]. U vezi sa tim je i činjenica da se razvoj javno-privatnog partnerstva morati odvijati u fer tržišnim uslovima, a posebno u kontekstu pravne jasnoće u oblasti javnih nabavki. Iz ove perspektive, nije puka slučajnost što je skoro istovremeno Komisija uvela paket evropskih direktiva o koordinaciji postupaka za dodjelu ugovora o javnim radovima, ugovora o javnim nabavkama i ugovora o javnim uslugama.

Međutim, pravila EU koja regulišu izbor privatnog partnera koordinisana su u Zajednici na različitim nivoima, tako da je na nacionalnom nivou i dalje moguć širok izbor pristupa. Zelena knjiga posebno analizira[216]:

- okvir za postupke izbora privatnog partnera (procedura konkurentskog dijaloga za pojedina javno-privatna partnerstva kvalifikovana kao javni ugovori, minimalni okvir u sekundarnom zakonodavstvu za koncesije za radove, pri čemu ne postoji okvir u sekundarnom zakonodavstvu za koncesije za usluge),
- privatno iniciranje javno-privatnog partnerstva,
- ugovorni okvir i izmjene ugovora tokom realizacije partnerstva i

[214] COM (2004) Green Paper on PPPs and Community Law on Public Contracts and Concessions.
[215] Green Paper on PPP and Community law on public contracts and concessions, 2004, COM(2004)327, part 1.3, art. 18.
[216] Bult-Spiering M., Dewulf G.: *Strategic issues in public–private partnerships: an international perspective*, Blackwell Publishing, Oxford, 2006, p. 62

– podugovaranje.

Javno-privatna partnerstva koja su stvorena na osnovu čisto ugovornih veza (ugovorna javno-privatna partnerstva ili koncesije) i partnerstva koja uključuju zajedničko učešće javnog partnera i privatnog partnera u pravnom licu sa mješovitim kapitalom (institucionalna partnerstva ili zajednička ulaganja) su obrađena u Zelenoj knjizi koja takođe definiše koncept koncesije u pravu Zajednice i obaveze javnih vlasti prilikom izbora koncesionara. U koncesijskim ili ugovornim, javno-privatnim partnerima, partnerstvo između javnog i privatnog sektora zasniva se isključivo na ugovornim vezama. Privatnom partneru dodjeljuje se jedan ili više zadataka koji mogu da uključuju dizajn, finansiranje, izvršenje, obnovu ili eksploataciju djela ili usluge. U koncesivnom modelu postoji direktna veza između privatnog partnera i krajnjeg korisnika jer privatni partner pruža javnu uslugu pod kontrolom javnog partnera. Naknada se naplaćuje korisnicima usluga ili ima oblik redovnih plaćanja od strane javnog partnera[217].

Javno-privatno partnerstvo sa zajedničkim ulaganjem uključuje saradnju između javnog i privatnog sektora u okviru trećeg entiteta, koji drže zajednički javni i privatni partner i ima zadatak da osigura isporuku djela ili usluge u korist javnosti. Zakon o javnim ugovorima i koncesijama ne odnosi se na ove subjekte iz mješovitog kapitala, ali opšti principi Ugovora EU i dalje ostaju na snazi. Pri odabiru privatnog partnera trebalo bi razmotriti karakteristike njegove ponude (ekonomski najpovoljnije), pored kriterijuma na osnovu kapitalnog doprinosa i iskustva. Ako mješoviti subjekt ima kvalitet ugovornog tijela, on treba da se pridržava zakona koji se primjenjuje na javne ugovore i koncesije prilikom dodjeljivanja zadataka. Drugim riječima, privatni partner ne treba da profitira od svog povlašćenog položaja u mješovitom entitetu da bi rezervisao za sebe određene zadatke bez prethodnog poziva za nadmetanje[218].

Posebna cjelina Zelene knjige obrađuje praksu privatne inicijative u sklapanju javno-privatnih aranžmana. U takvim slučajevima privatni sektor ima pravo da predlaže projekte javnom sektoru. Međutim, ovakvi postupci posebno moraju biti transparentni, kako ne bi došlo do favorizovanja pojedinačnih partnera, pogotovo zbog mogućnosti subvencionisanja inicijatora javno-privatnog partnerstva od strane javnog partnera. Dalje se analizira faza koja slijedi nakon odabira privatnog partnera. Ugovorne odredbe koje se odnose na fazu sprovođenja PPP predmet su nacionalnih zakonodavstava, ali moraju biti u skladu sa načelima Ugovora o EU u principima jednakog tretmana i transparentnosti. U tom kontekstu, pomenuti principi su važni u pogledu procjene trajanja ugovora i raspodjele rizika, tako da pitanja trajanja i rizika moraju biti dio poziva na tender, kako bi potencijalni ponuđači mogli da ih uzmu u obzir prilikom pripremanja svojih ponuda. Nakon dodjele ugovora, pravo EU odbacuje mogućnost izmjene ugovora bez raspisivanja novog tendera, osim u slučajevima neprofitnih aktivnosti.

[217] Stanghellini S., Copiello S.: Urban Models in Italy: Partnership Forms, Territorial Contexts, Tools, Results, In: Dalla Longa R.(ed.): *Urban Models and Public-Private Partnership*, Springer, Heidelberg-Dordrecht-London-New York, 2011, pp. 48-41

[218] Yescombe R. E.: *Public–Private Partnerships, Principles of Policy and Finance*, Butterworth-Heinemann is an imprint of Elsevier, Oxford, 2007, p. 81

3.4.2. Najvažnije organizacije Evropske unije u realizaciji javno-privatnog partnerstva

Evropska unija ima razrađen institucionalni okvir javno-privatnog partnerstva koji se ogleda u velikom broju subjekata. Tu su prvenstveno Evropska komisija, Evropski parlament, Evropski sud pravde i Evropsko vijeće. Pored toga, tu su i druga tijela, ustanove i specijalizovane agencije, a prvenstveno Evropska banka za obnovu i razvoj, Evropska centralna banka, Evropska investiciona banka i Eurostat, koji zajedno predstavljaju institucionalni okvir podrške javno-privatnim partnerstvima. S obzirom na veliki broj institucija u narednom dijelu rada analiziraćemo ulogu i značaj Evropske investicione banke i Eurostata.

Evropska investiciona banka *(European Investment Bank)* osnovana je Rimskim ugovorom 1957. godine sa osnovnim zadatkom da obezbijedi dugoročno finansiranje za projekte koji će omogućiti realizaciju ciljeva raznih politika EU. Pored osnovne uloge katalizatora ekonomskih integracija i ekonomske i socijalne kohezije, banka obezbjeđuje i neophodni kapital za projekte javno-privatnog partnerstva. Banka je podrška investicijama u onim oblastima u kojima su značajno zastupljena javno-privatna partnerstva, kao što su izgradnja saobraćajne infrastrukture, telekomunikacije, proizvodnja i distribucija energije, prirodni izvori, gradsko okruženje i socijalna infrastruktura (ljudski kapital) poput bolnica, škola, univerziteta i naučno-istraživačkih centara. U poslednjih dvadeset godina Banka je jedan od najvećih evropskih finansijera projekata javno-privatnog partnerstva sa razvijenom ekspertizom u ovoj oblasti[219].

Kada je riječ o procjeni podobnosti nekog projekta u cilju njegovog finansiranja od strane Banke, ona je standardnog tipa ali se evaluira za svaki projekat. U cilju transparentnosti, Banka je formirala standarde da bi određeni projekat bio prihvatljiv za finansiranje od strane Banke. U slučajevima javno-privatnog partnerstva, to obuhvata:

- ekonomsku i tehničku opravdanost;
- ispunjenje zahtjeva Banke u pogledu očuvanja životne sredine;
- finansijsku snagu;
- tendersku proceduru koja je konkurentna i usklađena s pravilima javnih nabavki EU.

Što se tiče zajmova za finansiranje projekata javno-privatnog partnerstva, većina je tipa projektnog finansiranja. Pri tome Banka zajam odobrava kompaniji posebne namjene koja realizuje projekat. Nema sumnje da je Banka u pojedinim slučajevima izložena riziku u finansiranju kao i drugi finansijeri, dok u drugim slučajevima zahtijeva garancije od strane banaka privatnog sektora ili drugih finansijskih institucija. Pored toga, Evropska investiciona banka sarađuje sa javnim sektorom, naročito u predtenderskoj fazi, kako bi se identifikovali projekti koje će ona finansijski podržati. Uloga Banke u ovoj fazi je veoma često i savjetodavnog karaktera s obzirom da pomaže pri razvoju strukture javno-privatnog partnerstva i finansijske strategije. Na kraju klijent Banke je ujedno i pobjednik na tenderu. U cilju efikasne pomoći javnom sektoru, Banka razvija veoma konkurentske odnose između konzorcijuma koji učestvuju na tenderu i sarađuje s njima u toku tenderske faze, pridržavajući se principa jednakog tretmana svih učesnika odnosno bez diskriminacije učesnika[220].

[219] Financing PPPs with project bonds, Issues for public procuring authorities, The European PPP Expertise Centre, 2012, p. 2

[220] Thomson C., Goodwin J.: *Evaluation of PPP projects Financed by the EIB*, European Investment Bank, 2005, pp. 12,13

Kada se radi o tržištu javno-privatnog partnerstva uloga Banke je posebno značajna i višestruka. Njena uloga se posebno ogleda kroz:

- kreditiranje projektnih kompanija ili konzorcijuma koji pobijede na tenderu,
- omogućavanje ekspertiza kreditorima privatnog sektora detaljnim provjeravanjem projekta,
- pružanje uvjerenja javnom sektoru da je izabrana odgovarajuća struktura, zahvaljujući direktnom učešću Banke u identifikovanju projekata prije konkurentske nabavke.

I pored nesporne činjenice da Evropska investiciona banka ima kvalitativno i kvantitativno značajnu ulogu u primjeni projekata javno-privatnog partnerstva u EU, ona nema politiku kojom bi favorizovala predmetne projekte u odnosu na ostale forme finansiranja ili nabavke. Pored toga, značajno je naglasiti da kada se radi o involviranosti Banke, odluku da li se projekat implementira na tradicionalan ili neki alternativni način, uključujući i javno-privatno partnerstvo, donosi isključivo klijent Banke bez obzira da li se radi o javnom ili privatnom sektoru.

Sa aspekta javno-privatnog partnerstva Banka u svom sastavu ima Evropski stručni centar (*European PPP Expertise Centre*) koji ostvaruje savjetodavne usluge Evropskoj investicionoj banci. To je dio inicijative koja takođe uključuje Evropsku komisiju, države članice EU, države kandidate i pojedine druge zemlje. Centar je u sjedištu Odjeljenja za savjetodavne usluge Evropske investicione banke. U svom sastavu ima 41 člana, uključujući EIB i Evropsku komisiju, te nacionalna ili regionalna javna tijela odgovorna za politiku ili programe javno-privatnog partnerstva u državama članicama Evropske unije, zemljama kandidatima i nekim drugim zemljama koje ispunjavaju uslove. Centar pomaže da se ojača kapacitet članova javnog sektora za zaključivanje transakcija javno-privatnog partnerstva. Uz podršku tima koji čine iskusni profesionalci za javno-privatno partnerstvo, Centar razmjenjuje iskustva i ekspertize, analize i najbolju praksu u vezi sa svim aspektima javno-privatnog partnerstva[221].

Zadaci i uloga Eurostata proizilaze iz Mastrihtskog ugovora, kojim je sačuvana fiskalna stabilnost i ujedno sprečavanja prekomjernog državnog deficita članica Evropske unije. Predmetni ugovor uspostavlja stroga ograničenja državnog deficita i duga država članica EU i pruža uporedni okvir za nadzor njihovih javnih finansija. Od država članica se očekuje da održavaju godišnji budžetski deficit manji od 3% BDP-a i javni dug manji od 60% BDP-a. Prilikom ocjene fiskalne stabilnosti uzimaju se u obzir rizici koje snose vladine aktivnosti. S druge strane, opšte pravilo je da vlade treba da u Nacionalnim računima izveštavaju o imovini za koju one snose najveći dio rizika, pri čemu su javno-privatna partnerstva relevantna u mjeri u kojoj spadaju u nadležnost ovog pravila. Važno je napomenuti da se tretman javno-privatnog partnerstva od strane Eurostata ne zasniva na procjeni troškova i koristi od vrijednosti partnerstva. Naime Eurostat kroz tretman javno-privatnog partnerstva samo nastoji da obezbijedi ujednačene cifre duga i deficita koji su uporedivi u svim državama članicama. Cilj je analiziranje finansijske stabilnosti privrede tako da je određujući faktor rizik kojem je vlada, u principu, izložena kao rezultat određenog projekta. Eurostatovo postupanje u ovom slučaju služi za mjerenje da li i kada prema trenutnim pravilima Eurostata cjelokupna kapitalna investicija određenog projekta javno-privatnog partnerstva treba da se izračuna kao javni rashod i stoga se doda državnom deficitu ili suficitu i da li ukupnost duga datog za finansiranje investicije

[221] *European PPP Expertise Centre*, dostupno na: https://www.eib.org/en/publications/epec-european-ppp-expertise-centre.htm

treba prijaviti kao državni dug i dodati opštem državnom dugu. Eurostatski tretman takođe može imati uticaja na manevarski prostor koji bi nacionalne vlade imale u pružanju mjera podrške (npr. direktno pozajmljivanje, garancije, povoljni ugovorni uslovi) u doba tržišnih poremećaja, poput finansijske krize iz 2008. godine[222]. Pored toga, tretman javno- privatnog partnerstva zavisi i od klasifikacije imovine pojedinačnih partnera u projektu. Prema Evrostatu ova klasifikacija ima tri koraka:

- razlikovati javno-privatna partnerstva od ostalih dugoročnih javno-privatnih aranžmana koji imaju različit računovodstveni i statistički tretman (npr. ugovori o dizajniranju, izgradnji ili outsourcing-u)
- utvrditi da li je partnerska jedinica koja razvija projekat ili dio projekta javni partner. Ovo odlučivanje zasniva se na stvarnim ekonomskim tokovima, nezavisno od bilo koje pravne strukture i
- procijeniti rizik koji snose javni i privatni partneri. Klasifikacija imovine određuje koji partner (državni ili nevladin) snosi najveći dio projektnog rizika, kao što je određivanje koji partner ima ekonomsko vlasništvo nad imovinom uključenom u javno-privatno partnerstvo.

Kada nevladin partner ne objedini svoje račune sa vladom, klasifikacija imovine mora da slijedi „klasifikaciju institucionalnog sektora“, a kada konsoliduje svoje račune na državnim računima, klasifikacija imovine nije potrebna i ukupna investicija se računa se kao državni deficit i dug[223].

Pored navednih ustanova, i Eurostat je imao značajan uticaj u stvaranju adekvatnih uslova za implementaciju javno-privatnih partnerstva na evropskom prostoru. Naime, Evropska komisija je, u saradnji sa ekspertima Eurostata (nacionalnih statističkih instituta zemalja članica i pristupajućih zemalja), Evropske centralne banke i Evropske investicione banke, uspostavila Radnu grupu čiji je cilj bio da objasni računovodstveni tretman javno-privatnog partnerstva u okviru pravila ESA 95[224], kao i set kriterijuma kojima će javni sektor moći da se rukovodi u donošenju odluke da li će projekat predmetnog partnerstva biti tretiran kao obaveza države i budžetski rashod ili će biti tretiran vanbilansno. Evrostat je donio odluku koja se oslanja na ključni princip da bi imovina javno-privatnog partnerstva trebalo da bude klasifikovana kao nedržavna i time prikazana vanbilansno, ukoliko su ispunjeni sledeći uslovi:

- partner privatnog sektora preuzima rizike izgradnje,
- partner privatnog sektora preuzima najmanje još jedan od sledećih rizika: rizik raspoloživosti koji zavisi od učinka partnera i (ili) rizik tražnje.

U složenim aranžmanima kao što je javno-privatno partnerstvo javljaju se mnogi rizici. U cilju sprečavanja različitih tumačenja i otklanjanja konfuzije, Eurostat je odabrao tri osnovne kategorije

---

[222] *Eurostat Treatment ofPublic-Private Partnerships, Purposes, Methodology and Recent Trends*, European PPP Expertise Centre, 2010, p. 13

[223] Ibidem, p. 15

[224] Evropski sistem računa (*European System of Accounts - ESA 95*), osnova za kriterijume iz Mastrihta, postavlja statistička pravila za evidentiranje različitih tipova troškova u okviru nacionalnih računa i za tretman obaveza države koje utiču na budžetski deficit i javni dug. Suštinski je u stavu da ekonomski tretman imovine(projekta) zavisi od toga koja strana preuzima rizike i prihode. Implementacija ovog stava bila je kompleksna, naročito u tretmanu budućeg projekta u javno-privatnom partnerstvu, odnosno da li će obaveze i sredstva po osnovu projekta pripisati javnom ili privatnom sektoru.

rizika. Pored toga, određen je i stepen prihvatanja rizika, kada se kaže da jedna strana preuzima neku kategoriju rizika, to znači da ta strana preuzima znatan dio tog rizika.

Prva kategorija je „rizik izgradnje“ (*construction risk*) koji se odnosi na kasnu isporuku, nepoštovanje određenih standarda, dodatne troškove, tehničke nedostatke i negativne eksterne efekte. Javni sektor ima obavezu da počne s redovnim plaćanjem partneru privatnog sektora tek nakon uzimanja u obzir faktičkog stanja imovine (projekta)[225].

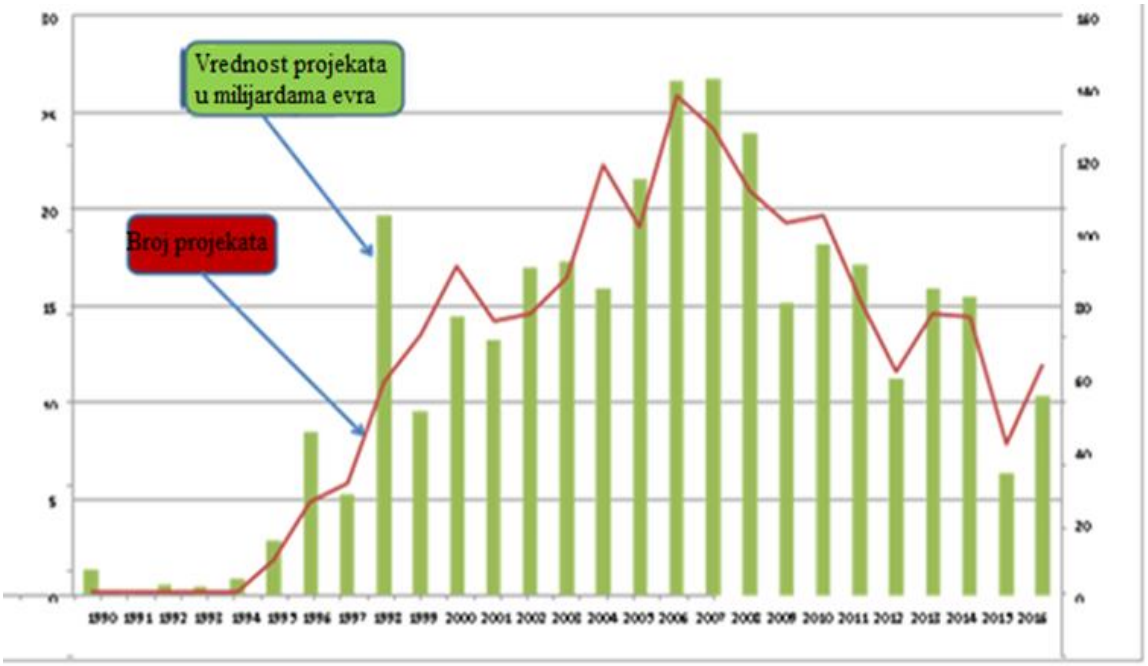
Druga kategorija je „rizik raspoloživosti“ (*availability risk*) gde je odgovornost partnera u privatnom sektoru evidentna. Privatni sektor se može naći u okolnostima da nije u mogućnosti da isporuči ugovorom dogovorenu količinu ili da ispuni dogovorene standarde. Država će izvršavati plaćanja tokom dogovorenog perioda samo u onoj mjeri u kojoj su ispunjeni dogovoreni nivoi raspoloživosti od strane partnera privatnog sektora. Primjena penala kada partner kasni sa isporukom trebalo bi da bude automatska i trebalo bi da ima značajan efekat na prihode (profit) partnera. Drugim riječima, penali ne smiju biti simbolični[226].

Treća kategorija je „rizik tražnje“ (*demand risk*) koji pokriva promenljivost tražnje. Rizik se odnosi na promjenu tražnje koja nije nastala usled neadekvatnog ili niskog nivoa kvaliteta usluga, niti usled bilo koje aktivnosti koja je dovela do promjene kvantiteta (kvaliteta) obezbijeđenih usluga. Naprotiv, ovo su rizici koji nastaju usled eksternih faktora, kao što su poslovni ciklus, novi tržišni trendovi, direktna konkurencija ili tehnološka zastarelost. Država preuzima rizik kada je obavezna da obezbijedi plaćanje partneru privatnog sektora nezavisno od efektivnog nivoa tražnje na strani krajnjih korisnika, sprečavajući time da fluktuacije u nivou tražnje utiču na profitabilnost partnera[227].

3.4.3. Kvantitativni prikaz javno-privatnog partnerstva u Evropskoj uniji

U cilju potpunije analize u ovoj cjelini rada ukazaćemo na trendove i rasprostaranjenost koncepta javno-privatnog partnerstva na prostoru Evropske unije. U tom cilju poslužićemo se izvještajem Evropskog revizorskog suda (Javno-privatna partnerstva u EU: Široko rasprostranjeni nedostaci i ograničene koristi)[228]

[225] Cartlidge D.: *Public Private Partnerships in Construction*, Taylor & Francis, New York, 2006, p. 84
[226] Hemming R.: PPPs: Some Accounting and Reporting Issues, In: Schwartz G., Corbacho A., Funke K.: *Public investment and public-private partnerships : addressing infrastructure challenges and managing fiscal risks*, Palgrave Macmillan, New York, 2008, p. 238
[227] Monteiro S. R.: PPPs and Fiscal Risks: Experience of Portugal In: Schwartz G., Corbacho A., Funke K.: *Public investment and public-private partnerships: addressing infrastructure challenges and managing fiscal risks*, Palgrave Macmillan, New York, 2008, pp. 129, 130, 133
[228] Public Private Partnerships in the EU: Widespread shortcomings and limited benefits, European court of auditors, 2018.



Grafikon br. 1.: Evropsko tržište javno-privatnog partnerstva u periodu 1990-2016 prema vrijednosti i broju projekata[229]

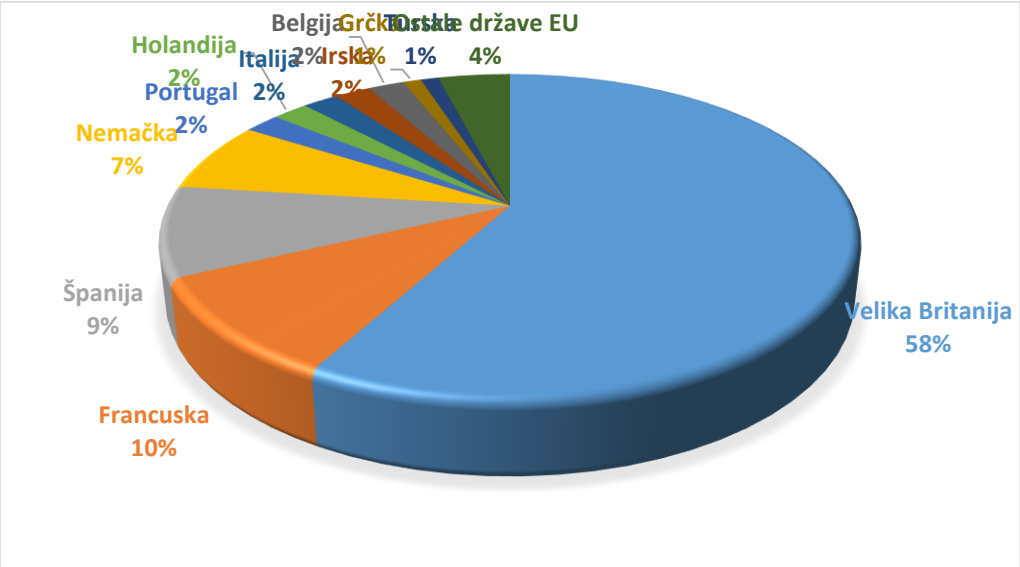
Iz navedenog grafikona (Grafikon br. 1) može se uočiti da je javno-privatno partnerstvo na prostoru Evropske unije kontinuirano raslo do 2007. godine. Nakon toga uslijedio je pad kao posledica globalne finansijske i ekonomske krize. To je, uz ostalo, uticalo i na nedostatak likvidnosti, što je značajno povećalo troškove privatnih finansija. Sa aspekta javno-privatnog partnerstva Velika Britanija ima najrazvijenije tržište u Evropi, nakon čega slijede Francuska, Španija, Portugal, Nemačkoj i Grčka. Transportni sektor, a posebno putevi, obuhvataju najveći dio projekata evropskog javno-privatnog partnerstva. U državama sa značajnim nedostacima u infrastrukturi, kao što su bile Grčka, Portugal ili Španija početkom devedesetih godina prošlog vijeka, javno-privatno partnerstvo je korišćeno za finansiranje velikih projekata. Nakon finansijske krize 2008. godine, pooštreni limiti i kontrole javnih troškova smanjili su apetit za megaprojektima, koji se i sada sprovode, ali uglavnom sporadično.

Pod mješovitim projektom javno-privatnog partnerstva se podrazumijeva aranžman gdje dio ili cjelokupno javno finansiranje za projekat obezbjeđuje Evropski fond za regionalni razvoj (ERDF) ili Zajednički fond (CF). Očekivanja koja se odnose na dodanu vrijednost JPP-a zasnivaju se na efikasnijoj i efektivnijoj upotrebi resursa i na potrebi da se poboljša orijentacija na rezultat kohezione politike.

Prema podacima EPEC-a, na evropskom tržištu između 1990. i 2016. godine realizovano je 1.766 transakcija javno-privatnog partnerstva u ukupnoj vrijednosti od 356 milijardi EUR. Kao što je prikazano na Grafikonu br.3, broj projekata počeo je značajnije da se povećava od 1995. godine, da bi dostigao svoj maksimalni nivo u 2006. godini sa 138 transakcija ukupne tržišne vrijednosti od 26,7 milijardi EUR. Ekonomska i finansijska kriza koja je započela u periodu 2007-2008. godina uticala

[229] Projekti finansirani od strane Evropske investicione banke

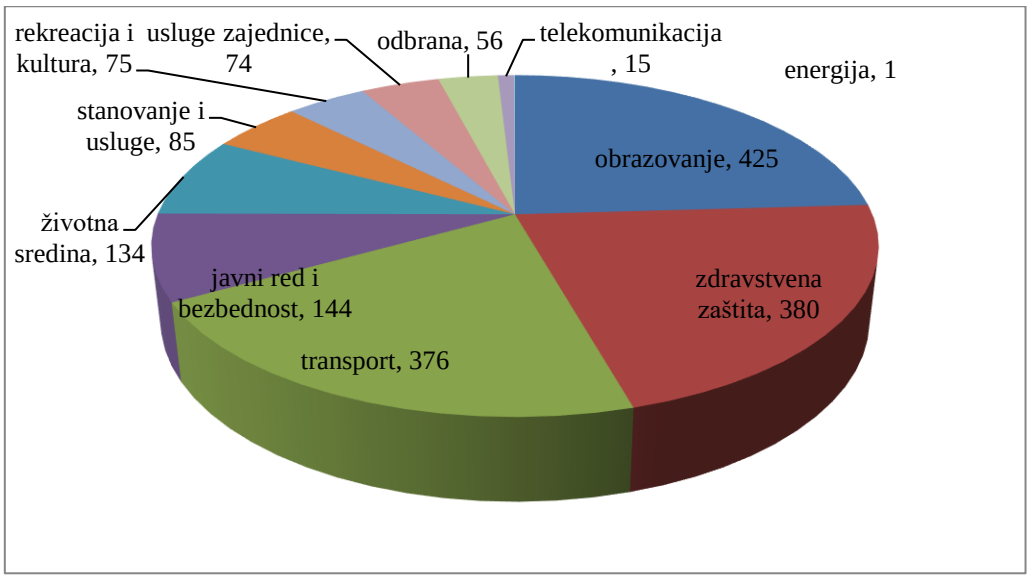
je na trend pada projekata javno-privatnog partnerstva, koji se konstantno smanjivao i dostigao najniže vrijednosti u 2015. godini (49 transakcija). To se može objasniti izazovima sa kojima su privatne kompanije u tom periodu bile suočene, prije svega sa nedostatkom novca i samim tim smanjenom mogućnošću pridruživanja projektima javno-privatnog partnerstva. Vrijednost transakcija u ovoj oblasti se mijenjala tokom godina, a prosječna vrijednost transakcije se značajno smanjila u 2016. godini (174 miliona eura u odnosu na 319 miliona zabilježenih u 2015. godini).



Grafikon br.2.: Evropske države sa najvećim brojem projekata javno-privatnog partnerstva u periodu 1990-2016

Kada su u pitanju nacionalna tržišta (Grafikon br.2) Velika Britanija je tradicionalno najveće tržište u Evropi, i po vrijednosti od 158,2 milijarde eura, i po broju projekata, sa 1.021 ugovorom zaključenim između 1990. i 2016. godine. Francuska i Španija su sledeća najveća tržišta, sa 175, odnosno 160 završenih projekata javno-privatnog partnerstva u ukupnoj vrijednosti od 36 (35) milijardi EUR. Holandija, Portugal i Italija su relativno manja tržišta, jer je u njima završeno oko 40 transakcija od 1990. godine. Belgija i Grčka su nova tržišta u nastajanju, na kojima su se ovi projekti počeli razvijati od 2006. godine. Zanimljivo je da su evidentirana ukupno 72 projekta u 16 ostalih država članica EU, među kojima najveći udio imaju Danska (15) Poljska (11) i Mađarska (10 JPP-a). U toj grupi su i države poput Bugarske, Letonije, Luksemburga i Slovenije koje su zaključile samo po jednu transakciju javno-privatnog partnerstva od 1999. godine.

Kao što je navedeno, finansijska i ekonomska kriza je negativno uticala na sve države članice EU, čak i na vodećim tržištima javno-privatnog partnerstva. U Velikoj Britaniji, na primjer, transakcije iz ove oblasti od 2007. godine opadale su u proseku od 11% godišnje, spuštivši se na 28 u 2016. godini, što predstavlja smanjenje za 64% u odnosu na godinu prije krize (77 transakcija u 2006. godini). U Španiji je pad bio značajniji nego u drugim zemljama, jer se broj završenih projekata smanjio za 70% (10 projekata u 2007. godini u odnosu na 2006. godinu kada ih je bilo 33). Ovaj trend se nastavio sve do 2016. godine kada nije ni bilo zabilježenih projekata javno-privatnog partnerstva.



Grafikon br. 3.: Struktura projekata javno-privatnog partnerstva prema sektorima za period 1990-2016. godine

Ukoliko projekte javno-privatnog partnerstva posmatramo iz ugla određenih sektora (Grafikon br. 3), onda su sektori obrazovanja, zdravstva i saobraćaja predstavljali većinu realizovanih projekata sa 1181 ugovora zaključenih u periodu između 1990-2016. godine. Ipak, sektor transporta je najveći po vrijednosti, sa preko 199,8 milijardi eura transakcija, što je pet puta više od finansiranja javno-privatnog partnerstva u sektoru obrazovanja i zdravstva (46, odnosno 34 milijarde EUR u proseku). To su ujedno i tradicionalni sektori u kojima je javno-privatno partnerstvo najviše dolazilo do izražaja u poslednjih nekoliko godina.

U sektoru saobraćaja je u 2016. godini završeno 11 transakcija, što predstavlja najnižu vrijednost u proteklih 10 godina. U sektoru zdravstva, je broj projekata koji su se finansijski zatvorili u 2016. godini porastao je na 15, dok se ukupna vrijednost značajno smanjila - na 2,3 milijarde eura. Posmatrajući druge relativno manje sektore, može se primijetiti nagli porast vrijednosti u sektoru životne sredine (sa 374 miliona eura u 2015. na 1,2 milijarde eura u 2016. godini). Razlog navedenom je povećanje poslova u vezi sa tretmanom otpada u Velikoj Britaniji. Čak 75 predmetnih projekata zatvoreno je u sektoru rekreacije i kulture, pri čemu je najveći broj zabilježen u 2011. godini (11 transakcija u ukupnoj vrijednosti od 565 miliona eura), nakon čega je došlo do smanjenja (u 2015. godini je zaključen samo jedan ugovor u ukupnoj vrijednosti od 12 miliona EUR). Telekomunikacije predstavljaju novo tržište u pogledu javno-privatnog partnerstva sa četiri transakcije u 2016. godini (sve se tiču širokopojasnih mreža u Francuskoj) u ukupnom iznosu od 1,2 milijarde EUR.

3.5. Nacionalni nivo javno-privatnog partnerstva u pojedinim evropskim državama

U cilju podsticanja nacionalnih ekonomija kao i bržeg razvoja infrastrukture i javnih usluga, države članice Evropske unije su početkom poslednje decenije XX vijeka u značajnoj mjeri prihvatile modele javno-privatnog partnerstva. U tome je prednjačila Francuska, a ostale članice EU su je sledile. Uopšteno posmatrano, zakonodavstvo država članica u toj oblasti usklađeno je regulativom

EU i preporukama relevantnih institucija. Posebnosti zakonodavnog i institucionalnog okvira pojedinih država koje se tiču zastupljenosti pojedinih oblika javno-privatnog partnerstva, njihovih modaliteta, sektorske strukture izabranih projekata i slično, zavise od više faktora, ali prevashodno od različitosti sistema javne uprave i pravnog nasleđa, a takođe i od relativno kratke istorije primjene i još uvijek dinamičnog prilagođavanja samih oblika javno-privatnog partnerstva.

Pravni okvir za javno-privatno partnerstvo u državama članicama EU može sadržavati mješavinu primarnog (krovnog) zakona i sekundarnog ili razrađujućeg zakonodavstva koji se bavi detaljnijim pitanjima kao što su zahjtevi administrativne pripreme i odobrenja za javno-privatno partnerstvo. Kako se sekundarno zakonodavstvo može lakše usklađivati, ono omogućava izmjene u konkretnim oblastima kao odgovor na promjene politike i tržišta. U državama, gdje postoji istorijsko iskustvo o javno-privatnom partnerstvu obično nije ni potrebno posebno zakonodavstvo, jer postoji veća fleksibilnost za unošenje promjena u program i praksu javno-privatnog partnerstva u svijetlu uvida stečenih prethodnim iskustvima. Pored navedenog, mnoge države članice posebnu pažnju posvećuju komunikaciji i koordinaciji u procesu realizacije projekata javno-privatnog partnerstva. U tom smislu, veoma je značajno postojanje posebnog organizacionog okvira za javno-privatno partnerstvo, sačinjenog od specijalizovanog osoblja koje je najčešće sistematizovano u sastavu nadležnog ministarstva. Osnovni zadaci tih organizacionih cjelina su razvijanje politika u području javno-privatnog partnerstva, davanje informacija o projektima i njihovom napretku, promocija dobrih praksi i saradnja sa medijima u cilju blagovremenog i potpunog izveštavanja o stanju i perspektivama u toj oblasti[230]. S druge strane, ne treba zaboraviti, jedna od glavnih poteškoća za javni sektor u realizaciji predmetnog partnerstva je nedostatak ekspertiza u pojedinim oblastima specijalizacije kao što su finansije, pravo, upravljanje projektima, inženjering, planiranje, javna politika i drugo. Zato je važan segment u programima javno-privatnog partnerstva stvaranje posebne organizacione cjeline zadužene za javno privatno-partnerstvo. To je ujedno i razlog što je većina evropskih država uspostavila odgovarajući organizacioni oblik, obično u okviru centralne banke ili ministarstva finansija/ekonomije, kao centar koji pruža ekspertize i tehničke podrške vladinim ministarstvima i drugim ugovornim organima koji razvijaju javno-privatno partnerstvo[231].

3.5.1. Javno-privatno partnerstvo u Belgiji

Iako razvoj infrastrukturnih projekata i pružanje javnih usluga u Belgiji u obliku javno-privatnog partnerstva nisu novost, njihov značaj u vladinoj politici je naglo porastao u poslednje dvije decenije. Međutim, kultura JPP zasnovana na „alternativnom finansiranju“, za razliku od tradicionalnog finansiranja javnim novcem, još uvijek nije čvrsto uspostavljena. Belgija ipak polako postaje svjesna prednosti koje donosi javno-privatno partnerstvo zasnovano na modernoj privatnoj finansijskoj inicijativi, odnosno koristi koje stanovništvo ima od smanjenja trošenja javnog novca i poboljšanja kvaliteta isporučenih usluga. U Belgiji, kao decentralizovanoj državi, ne postoji opšta zakonska definicija za ugovore o javno-privatnom partnerstvu. Dekret koji je 2003. godine usvojila skupština regije Flandrije definiše ih kao „projekte koje zajedno sprovode javna i privatna tijela ili

[230] Yescombe E. R.: *Public-Private Partnerships: Principles of Policy & Finance*, Butterworth-Heinemann Oxford, 2007, pp. 41-42
[231] Ibidem, pp. 44-45

subjekti, u obliku partnerstva, a u cilju stvaranja dodate vrijednosti za ove organe ili entitete". Ova definicija se donekle razlikuje od uobičajenih u evropskim državama, kao i određenja u Zelenoj knjizi Evropske komisije[232].

S druge strane, treba napomenuti da je unutrašnje belgijsko tržište relativno malo, fragmentiranog karaktera, kao posledica složenosti političko-administrativnog uređenja. Naime, na ovom prostoru brojni nivoi administrativne organizacije su doveli i do fragmentacije vještina, resursa i prakse. Štaviše, veličina lokalnih i regionalnih javnih resursa je relativno mala, kao i veličina privatnog tržišta. Ove okolnosti su uticale na belgijsku praksu javno-privatnog partnerstva. Posledica takvog stanja je nepostojanje belgijskog modela javno-privatnog partnerstva, te odsustvo zajedničke politike u tom domenu. U praksi, tri belgijske regije različito pristupaju javno-privatnom partnerstvu, pri čemu Flamanska (Flandrijska) regija ima najviše iskustva u tom pogledu, dok je to znatno manje izraženo u Valonskoj regiji i regionu Brisela[233] (Tabela br.12).

INVESTICIJE JPP			**GODIŠNJI IZNOS**			
REGION	SEKTOR	Iznos	2012	2013	2014	2015
Federalna vlada	zatvori i željezničke pruge	1,687	9	50	113	113
Flamanija	sport, prevoz, javna infrastruktura, stanovanje	2,480	25	53	77	114
Brisel	otpadne vode	360	50	50	50	50
Valonija	putevi i vodovod	1,014	135	213	162	130
Nemačka zajednica	škole	146	-	-	-	-

Tabela br. 12.: Najvažniji projekti javno-privatnog partnerstva u Belgiji (u milionima eura)[234]

S druge strane, evidentna su nedovoljna ulaganja u kvalitativnu infrastrukturu, uz pojačanu potražnju za kvalitetnijim projektima koji se brže realizuju po istoj cijeni i, što je još važnije, manjak raspoloživih sredstava javnog finansiranja, što zahtijeva usklađivanje potreba za investiranjem u datom vremenu. Takvo stanje je doprinijelo naglom oživljavanju projekata javno-privatnog partnerstva poslednjih godina. To se u značajnoj mjeri manifestovalo na saveznom nivou, ali je još izraženije u Flamanskoj regiji, gdje je javno-privatno partnerstvo predstavljalo jedan od stubova državne investicione politike u mandatu vlade 2009–2014. godine[235].

Na saveznom nivou, reprezentativni primjeri velikih projekata javno-privatnog partnerstva uključuju razvoj nove željezničke veze između grada Brisela i nacionalnog aerodroma (projekat Diabolo, završen 2012. godine), izgradnja tunela ispod rijeke Šelde i proširenje autoputa R2 (završena 1991. godine), izgradnja zatvorskog kompleksa u Harenu (Brisel), koji će postati najveći zatvorski kompleks u Belgiji. U Flamanskoj regiji su investirana velika sredstva u uspostavljanje Flamanskog

[232] Gillet E.: Belgium, In: *PPP in Europe*, CMS Legal Services -European Economic Interest Grouping, 2009, pp. 11-12, dostupno na: https://cms.law/en/CHE/Publication/PPP-in-Europe
[233] Blaton A., Vliegher De D.: *An update on the use of public private partnerships (PPPs) in Belgium*, dostupno na: https://www.lexology.com/library/detail.aspx?g=917445f5-4c66-42f2-a55a-c9b29425e418
[234] Van Den Hurk M., Van Garsse S., Verhoest K.: *Ten years of PPP in Belgium: an overview*, Federale Overheidsdienst Financiën – België, 2013, p.164
[235] Ibidem, p.168

centra o javno-privatnom partnerstvu radi daljeg podsticanja uvođenja ovog oblika saradnje. Rezultat navedenog je veliki broj raspisanih projekata javno-privatnog partnerstva u različitim sektorima, uključujući transport, obnovljivu energiju, socijalnu infrastrukturu, kao i druge povezane infrastrukturne projekte. S druge strane, regioni Brisela i Valonije nisu razvijali značajnije projekte javno-privatnog partnerstva, što je promijenjeno nakon novijih značajnih ulaganja u projekte koji uključuju prevoz, socijalnu infrastrukturu i u skorije vrijeme, tržne centre koji sadrže objekte za odmor i stanovanje.

U Belgiji se koncept javno-privatnog partnerstva pojavljuje u više različitih oblika, kao posledica složenosti političkog i administrativnog konteksta, kao i nedostatka jedinstvene politike i nepostojanja belgijskog modela javno-privatnog partnerstva. Osnovna razlika je ona između „ugovornih" i „participativnih" javno-privatnih partnerstva. Iako ugovorna varijanta još uvijek liči na odnos poslodavac-izvođač, participativna varijanta podrazumijeva projekte posebne namjene i od strane vlasti i privatnog partnera, uz prisutni pritisak od strane EU. U tom kontekstu, koriste se različite ugovorne strukture, uključujući tradicionalni (osnovni) ugovor koji utvrđuje posebne kriterijume izvršenja sa ograničenim karakteristikama javno-privatnog partnerstva, kao i novije forme integrisanih ugovora o projektovanju i izgradnji (DB), ugovora o projektovanju, izgradnji i finansiranju (DBF) ili ugovora o projektovanju, izgradnji, finansiranju i održavanju (DBFM), eventualno u kombinaciji sa operativnim ugovorom (DBFM/O). Drugi model koji je uveden u Belgiji je DBM + F, u kome se DBM i finansijski tenderi dijele u fazi nadmetanja i spajaju nakon toga. Pored toga, koriste se i dugoročni ugovori o zakupu, ugovori o građevinskim pravima, ugovori o koncesiji, drugi *sui generis* ugovori ili kombinacija istih.[236].

Belgijsko zakonodavstvo o javnim nabavkama je izmijenjeno u 2016. i 2017. godini u skladu s primjenom Direktiva o javnim nabavkama 2014/24 i 2014/25 i Direktive o ugovoru za koncesije 2014/23. Zakon o koncesiji je usvojen 17. juna 2016. Ova nova pravila stupila su na snagu 2017. godine i primjenjuju se na sve ugovore o javnim nabavkama. Odgovornost za strukturiranje, dodjelu i sprovođenje javno-privatnih partnerstava ostaje zadatak odgovarajućeg nivoa administracije. Nadležni organi (na relevantnom regionalnom, zajedničkom ili nacionalnom nivou, prema potrebi) uvijek mogu da ponište ili izmijene odluke nižih javnih tijela.

Institut za nacionalne izvještaje (račune) daje savjetodavna mišljenja o projektima javno-privatnog partnerstva. To je vladino tijelo na saveznom nivou, zaduženo za pregled dužničkog opterećenja javnog sektora, koje procjenjuje uticaj projekta na budžet države i stanje duga, posebno u odnosu na postojeću regulativu, kao i usklađenost sa propisima na nivou EU. U 2018. godini Institut je izdao mišljenja o pet projekata javno-privatnog partnerstva (dva na saveznom nivou, jedan na nivou Flamanske regije i dva na nivou Briselskog regiona). U Flandriji je osnovan i Flamanski centar o javno-privatnom partnerstvu[237] koji savjetuje i vodi politiku svih javnih tijela i podržava projekte u Flamanskoj regiji. On preuzima savjetodavnu ulogu (uopšte i u pogledu određenog projekta), prikuplja i razmjenjuje znanja, iskustva i modele predmetnog partnerstva sa zainteresovanim stranama. Institut je posebno doprinio uvođenju standardizacije ugovornog pristupa javno-privatnog partnerstva u Flamanskoj regiji. Nasuprot tome ne postoji ekvivalentno javno tijelo na saveznom

[236] Willems Tom, Verhoest K., at all: Ten Lessons from Ten Years PPP Experiencein Belgium, *Australian Journal of Public Administration*, Vol. 76, No. 3, Institute of Public Administration Australia, 2016, pp. 316-329
[237] Article 4 of the Decree of the Flemish Region of 18 July 2003 on public-private cooperation.

nivou, niti u regionu Brisela. U Valonskoj regiji vlada je osnovala ogranak za finansijsko izvještavanje Valonske administracije koji pruža savjete o javno-privatnom partnerstvu za Valonsku regiju i frankofonsku zajednicu, ali i za povezivanje javnih tijela prije usvajanja odluke o sprovođenju projekata predmetnog partnerstva. Pored toga, ovaj ogranak ima ulogu u praćenju i pružanju pomoći u realizaciji projekata javno-privatnog partnerstva. Revizorski sud vrši spoljni nadzor budžetskog, računovodstvenog i finansijskog poslovanja savezne države, zajednica, regiona i institucija nadležnih za javne usluge. Kao dio svoje revizije, Sud razmatra i projekte javno-privatnog partnerstva koji uključuju bilo koju od navedenih institucija kao što je, na primjer, održavanje zatvora putem javno-privatnog partnerstva[238]

Kada je riječ o zakonodavstvu, uopšteno posmatrano u Belgiji ne postoje posebna zakonska ograničenja ili posebni zahtjevi koji se odnose na javno privatno partnerstvo, pa se zbog toga primenjuju opšta pravila o javnim nabavkama ili pravila o koncesijskim ugovorima. Flamanska i Valonska regija su usvojile dodatne propise u cilju olakšavanja realizacije ovog partnerstva u svojim regionima. Pravila koja važe u Flamanskoj regiji odnose se na različite projekte javno-privatnog partnerstva, dok su pravila koja se primjenjuju u Valonskoj regiji i francuskoj zajednici specifična za određene sektore. Na primjer: Uredba Flamanske regije od 18. jula 2003. godine o javno-privatnim partnerstvima, kojom se razmatraju određena ograničenja u pravilima o javnim nabavkama, kao što su učešće javnih tijela u projektima javno-privatnog partnerstva pod određenim uslovima, ili Uredba Vlade Valonije koja se odnosi na uspostavljanje posebnog ogranka za alternativno finansiranje i finansijske izveštaje javnih vlasti i slično[239].

Javni ugovori, uključujući ugovore o javno-privatnom partnerstvu, i dalje podležu opštem Upravnom zakonu i Građanskom zakoniku, kao i specifičnim zakonodavstvima, kao što su Kodeks privrednih društava, poresko zakonodavstvo i zakonodavstvo o osiguranju, osim u mjeri koja je izričito drugačije određena. Sa ugovornog stanovišta, nadležni organ je slobodan da organizuje svoje projekte onako kako smatra prikladnim, bez posebnih ograničenja koja postoje za tradicionalne službe države, kao što su policija i vojska. Pored toga, sve vrste javnih radova, snabdijevanja i usluga mogu se ugovoriti kroz strukturu javno-privatnog partnerstva.

Dvije važne izmjene sadržane u Zakonu o javnim tenderima iz 2016. posebno utiču na opšte zahtjeve koje javni autoritet za ugovaranje mora da poštuje prilikom zaključivanja ugovora o javno-privatnom partnerstvu. Prvo, ugovorni organi moraju primjenjivati, pored principa jednakosti i nediskriminacije, i princip proporcionalnosti. To podrazumijeva da manje nepravilnosti koje je počinio kandidat u vezi sa fakultativnim razlozima za isključenje mogu opravdati njegovo eliminisanje samo u posebnim okolnostima. Drugo, ekološki standardi igraju značajnu ulogu, pri čemu se nepoštovanje ekoloških obaveza od strane izvođača ili jednog od njegovih podizvođača tokom izvršenja ugovora može smatrati kršenjem ugovora i samim tim dovesti do raskida ugovora. U mjeri u kojoj ugovor o javno-privatnom partnerstvu spada u belgijska pravila o javnim nabavkama, primjenjuju se opšta pravila o javnim nabavkama. U skladu sa EU direktivama o javnim nabavkama, belgijska pravila o javnim nabavkama pokrivaju sve ugovore zaključene u pisanom obliku radi

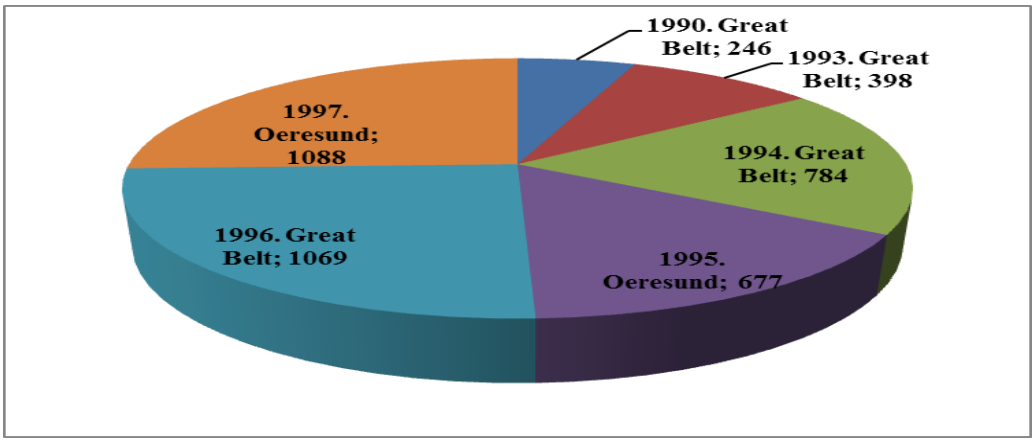
[238] Report: *Maintenance of Prison Facilities in Public-Private Partnership* - Monitoring by the Public Building Authority (Régie des bâtiments) and the Ministry of Justice' (21 November, 2018), dostupno na: https://www.ccrek.be/EN/Publications/Fiche.html?id=2847611e-cb6b-4b04-b897-136cfe1baf48 .

[239] Van Den Hurk M., Van Garsse S., Verhoest K.:*Ten years of PPP in Belgium: an overview*, Federale Overheidsdienst Financiën – België, 2013, pp. 162-163

razmatranja između izvođača, dobavljača ili pružaoca usluga i javnog kupca za preduzimanje radova i usluga. Pravila o koncesijskim ugovorima primjenjuju se ako ekonomski operator dobije pravo na izvođenje radova ili pružanje usluga koji su predmet ugovora, a koji postanu predmet spora. S druge strane, dodjeljivanje koncesije za radove ili usluge podrazumijeva prenos operativnog rizika u eksploataciji na koncesionara [240].

3.5.2. Javno-privatno partnerstvo u Danskoj

Uopšteno posmatrano, Danska se uobičajeno karakteriše kao društvo orijentisano na konsenzus koje stavlja naglasak an pregovaranje, umrežavanje i saradnju između aktera, posebno na tržištu rada. To je ujedno i jedan od razloga što se danska ekonomija naziva i „pregovaračka ekonomija“, čime se apostrofira uska povezanost između javnog i privatnog sektora. Moderna verzija vizije politike javno-privatnog partnerstva prvi put je predstavljena krajem 1990-ih godina, kada je danska vlada počela da obraća pažnju na tokove politike u ovoj oblasti koje su tada bile u toku u Velikoj Britaniji i drugim državama[241]. Danska ima dugu tradiciju javnog pružanja usluga socijalnog davanja, ali se tradicionalno koleba oko nametanja korisničkih naknada za usluge i infrastrukturu. Često se kao primjer navode dva glavna infrastrukturna projekta u toku devedesetih godina - Great Belt i Oeresund. U pitanju su mostovi koje su gradile državne kompanije, a finansirani su iz javnih izvora (Grafikon br. 4). Iako se na tim mostovima naplaćuje putarina, oni se ne mogu smatrati projektima javno-privatnog partnerstva zbog elementa javnih finansija. Takođe je i metro u Kopenhagenu, koji je počeo s radom 2002. godine finansiran iz javnih zajmova i od prodaje zemljišta[242].



Grafikon br. 4.: Podaci o finansijskim iznosima (u milionima eura) za mostove u Danskoj[243]

[240] Judo F., Maeyaert S., Goethals K.: *Belgium*, *The Government Procurement Review*, Law Business Research, London, 2016, pp. 26–37, dostupno na: https://thelawreviews.co.uk//digital_assets/c9be8045-55f1-4902-b275-d2871ba8f8cc/The-Government-Procurement-Review---Edition-7.pdf

[241] Greve C., Mörth U.: Public–private partnerships: the Scandinavian experience, In Graeme A. H., Greve C., Boardman E. A.: *International Handbook on Public–Private Partnerships*, Edward Elgar Publishing, 2010, p. 440

[242] Petersen H.O.: Regulation of public–private, partnerships: the Danish case, *Public Money & Management*, Vol. 30, Issue. 3 2010, p. 175

[243] Iako Danska stručna javnost navedene mostove ne tretira kao javno privatno partnerstvo, Evropski stručni centar za JPP ih prikazuje suprotno. Videti: *PPPs financed by the European Investment Bank from 1990 to 2018*, European PPP expertise centre, 2019, pp. 21-22

Danska je koncept javno-privatnog partnerstva pokrenula 1999. godine. Predmetni kocept je u narednih nekoliko godina u vladinim izveštajima pominjan kao način na koji se može ulagati u infrastrukturne projekte bez formulisane konkretne politike, podzakonskog akta, pa i novca namijenjenog za projekte. To je uticalo da danska vlada 2004. godine pokrene Akcioni plan za javno-privatna partnerstva, u kome je navedeno deset konkretnih inicijativa za podršku ovom konceptu. Među brojnim inicijativama koje su tada pokrenute, isticani su zahtjevi za testiranje predmetnog koncepta i za uspostavljanje organizacione komponente za javno-privatno partnerstvo pri Ministarstvu ekonomskih poslova. Takođe, je došlo i do pokretanja sedam pilot projekata javno-privatnog partnerstva. Akcioni plan je, pored ostalog, uključio i izmjene dijela nacionalnog zakonodavstva, a opredijeljeno je i 13 miliona eura kojim će biti testirana relevantnost javno-privatnog partnerstva. Pored toga, lokalni sektor je dobio finansijsku podršku za testiranje projekata javno-privatnog partnerstva, a formiran je i poseban fond za oslobađanje lokalnih samouprava od komplikovanog skupa budžetskih ograničenja za projekte građevinskog tipa.[244] Akcioni plan je takođe uspostavio finansijsku konstrukciju za podršku lokalnim i regionalnim vlastima u testiranju projekata koji su relevantni za javno-privatno partnerstvo[245].

Iz razvoja koncepta javno-privatnog partnerstva u Danskoj možemo uočiti da se isti razvijao dosta sporo. Naime, prva investicija te vrste bila je 2005. godine kada je raspisan tender za izgradnju škole u Heringu, nakon čega se projekat javno-privatnog partnerstva razvijao samo u ograničenom obimu. Prema zvaničnim podacima, do sredine 2016. godine u Danskoj su raspisani tenderi za oko 35 projekata JPP.[246] U međuvremenu je danska vlada donijela odluku o univerzalnom testiranju javno-privatnog partnerstva za projekte iz javnog sektora (Velika Britanija je imala obavezu takvog testiranja, ali je odlučila da ukine nakon samo nekoliko godina). Testiranje se odnosi samo na projekte na državnom nivou, a ne na lokalne ili regionalne projekte, i obavezno je samo za građevinske projekte, dok su infrastrukturni projekti za koje je nadležno Ministarstvo saobraćaja bili isključeni. Međutim, od 2008. godine fokus se sve više preusmjeravao na inovativna rešenja u sektorima socijalne zaštite, a naročito u zdravstvu. Ipak, danska vlada je postepeno razvila institucionalni i regulatorni okvir za podršku inovacijama i za javno-privatno inovativno partnerstvo.[247]

Pojam javno-privatno inovativno partnerstvo predstavlja vrstu javno-privatnog partnerstva u kome javni i privatni akteri u Danskoj sarađuju kako bi razvili nova i inovativna rešenja. To je ujedno sporazum o zajedničkoj saradnji između javnih i privatnih organizacija sa zajedničkim ciljem inoviranja i razvoja rešenja za javno dobro. Glavne inicijative uključuju poboljšanje okvirnih uslova i povećanje kvaliteta javnih usluga, kao i stvaranje novih poslovnih prilika za uključivanje preduzeća. Ključni elementi javno-privatnog inovativnog partnerstva su kontinuirani prenos ideja i znanja između zainteresovanih strana i uključivanje korisnika u razvoj novih rešenja. U javno-privatnom

[244] Petersen H.O.: Public-private partnerships as converging or diverging trends in public management? a comparative analysis of PPP policy and regulation in Denmark andIreland, *International Public Management Review*, Vol. 12, Issue 2, 2011, p. 10

[245] Petersen H. O.: Regulation of public–private, partnerships: the Danish case, *Public Money & Management* Vol. 30, Issue 3, 2010, p. 176

[246] Brøgger T., Kristiansen F.Ø.: Denmark, In: Çakmak Z., Çağdaş E. E.: *Global Public-Private partnership (PPP) guide*, Çakmak Yayınevi ve Medya Limited Şirketi, Ankara, 2016, p. 36

[247] Weihe G., at all: *Strategic use of public-private cooperation in the Nordic region*, Nordic Council of Ministers, Copenhagen 2011, p. 27

inovativnom partnerstvu, javne i privatne organizacije su razvojni partneri, a samo partnerstvo se može organizovati na različite načine i često uključuje učešće korisnika (na primjer, uključivanje krajnjih korisnika, kao što su pacijenti zdravstvene zaštite ili stručno osoblje koje pruža takve usluge). Zbog toga, organizaciona struktura javno-privatnog inovativnog partnerstva može varirati[248].

U Danskoj se koristi više različitih modela javno-privatnog partnerstva, uključujući model sa privatnim finansiranjem (*build-operate-transfer*), pojedinačne tenderske procedure u kojima se prenosi pravo na eksploataciju imovine (prenos operativnih prava), model sa javnim finansiranjem (*build-operate*), uključujući razne varijacije u kojima odgovornosti ostaje privatnom subjektu, kao i modele kod kojih se javno finansiranje obezbjeđuje putem finansijskog lizinga (prenos-zakup-operativni prenos). Pored toga, sprovedene su pojedinačne tenderske procedure u kojima su raspisani tenderi za odgovornu javnu službu, kao dio projekata javno-privatnog partnerstva. Kada se radi o modelu javno-privatnog partnerstva u tenderskim procedurama, on se koristi za izgradnju škola, administrativnih zgrada, sudnica, parking garaža, bolnica, policijskih stanica, postrojenja za čišćenje, bazena, održavanje objekata i jednog dijela javnih puteva. Tenderske procedure su sprovodile državne institucije (Danska agencija za imovinu), te regije i opštine u manjem obimu.[249].

Danska vlada je izdvojila značajna sredstava za podršku pokretanju projekata javno-privatnog partnerstva i javno-privatnog inovativnog partnerstva na regionalnom i lokalnom nivou vlasti. Tako je fondacija Investicije u tehnologiju javne dobrobiti pokrenula inicijativu usmjerenu na razvoj novih i poboljšanje postojećih rešenja za dobrobit u javnom sektoru, sa fokusom na tehnologijama za uštede u radu i unapređenje radnih procesa u javnom sektoru. Fond za poslovnu inovaciju je kao cilj postavio promovisanje rasta, zapošljavanja i izvoza kroz podršku unapređenju poslovnih mogućnosti i socijalne održivosti, kao i iskorišćavanju novih poslovnih prilika i mogućnosti rasta u manje razvijenim područjima države. Pored toga, pokrenuta je inicijativa Ministarstva nauke i tehnologije za promociju javno-privatnih inovacija sa ciljem obezbjeđenja instrumenata finansiranja namijenjenih podršci istraživačkoj saradnji između javnih istraživačkih institucija i privatnih kompanija. Pomenutim sredstvima upravlja više tijela, Danski istraživački savjet za nezavisna istraživanja, Danski istraživački savjet za strateška istraživanja i Danska nacionalna fondacija za naprednu tehnologiju. Danska vlada je objavila i izvještaj u kome je ocijenila inicijative za finansiranje, uz zaključak da su oni uspješni u smislu povećane javno-privatne saradnje i poboljšanja ekonomskih performansi danskih kompanija koje učestvuju u zajedničkim istraživačkim programima[250].

U Danskoj inače ne postoji eksplicitni pravni okvir za projekte javno-privatnog i javno-privatnog inovativnog partnerstva. Projekti se uglavnom sprovode u okviru postojećeg pravnog okvira, kao što je direktiva Evropske unije o nabavkama, Zakon o opštinskom upravljanju i opšti propisi u vezi sa porezom i porezom na dodatu vrijednost. Pored toga, Vlada je pokrenula dvije zakonske izmjene s ciljem podrške prihvatanju infrastrukturnih projekata javno-privatnog partnerstva. Prva zakonska izmjena, koja je izvršena 2004. godine, postavila je uslov da svi vladini projekti izgradnje moraju biti ispitani u kontekstu relevantnosti primjene koncepta javno-privatnog

[248] Ibidem, p. 14
[249] Brøgger T., Kristiansen F.Ø.: Denmark, In: Çakmak Z., Çağdaş E. E.: *Global Public-Private partnership (PPP) guide*, Çakmak Yayınevi ve Medya Limited Şirketi, Ankara, 2016, p. 36
[250] Weihe G., at all: *Strategic use of public-private cooperation in the Nordic region*, Nordic Council of Ministers, Copenhagen 2011, p. 29

partnerstva. Kao rezultat toga, mnogi vladini projekti su testirani na relevantnost, a započeto je i nekoliko novih projekata. Drugi zakonski amandman, koji je stupio na snagu 1. januara 2007. godine bio je vezan za novi Zakon o javno-privatnim preduzećima (Zakon 548) i uključivao je uvođenje zajedničke kontrole vlasništva u projektima JPP. Ovo rešenje je na tragu onog što Evropska komisija naziva institucionalnim javno-privatnim partnerstvom[251].

Dansko zakonodavstvo u oblasti javno-privatnog partnerstva je ostalo specifično. Naime, projekti javno-privatnog partnerstva sklapaju se kao ugovorna saradnja i regulišu se ugovorima. Međutim, ne postoji centralizovano tijelo za javno-privatno partnerstvo. S druge strane, Danska uprava za zaštitu konkurencije i potrošača daje opšta uputstva o javno-privatnim partnerstvima i objavljuje smjernice, među kojima i one koji se odnose na standardne ugovore za tenderske postupke u vezi s projektima javno-privatnog partnerstva (partnerstvo sa privatnim finansiranjem i partnerstvo sa javnim finansiranjem novih građevina i projektima obnove)[252].

Projekti javno-privatnog partnerstva u Danskoj i ostalim državama članicama EU podležu i nizu zajedničkih propisa o nabavkama. Takozvani „postupak konkurentnog dijaloga“ pokrenut je 2004. godine kao novi princip nabavki koji bi trebao da olakša nabavke kod ugovora koji su „posebno složeni“, a gdje ugovorni organi objektivno nisu u stanju da definišu tehnička sredstva ili nisu u mogućnosti da odrede pravni ili finansijski okvir projekta[253].

Posebna specifičnost se odnosi na posebnu organizacionu cjelinu zaduženu za javno-privatna partnerstva - Dansku upravu za zaštitu konkurencije i potrošača, koja predstavlja vladinu agenciju u okviru danskog Ministarstva industrije, poslovanja i finansijskih poslova. Zadatak Uprave je razvijanje konkurentnog, tržišnog okruženje i podsticanja privrednog rasta, što treba ostvarivati u saradnji sa korporativnim sektorom, poslovnim udruženjima i drugim akterima iz javnog sektora. Primarna uloga Danske uprave za zaštitu konkurencije i potrošača je ipak konsultantska, a ne menadžerska. Njeni zadaci su prvenstveno usmjereni na konsultacije sa opštinama i regionima uključenim u projekte javno-privatnog partnerstva. Uprava donosi i određene smjernice i djeluje kao ključni partner u razmjeni relevantnih znanja i iskustava u ovoj oblasti. Takođe, u njenoj nadležnosti je i sufinansiranje dijela troškova vladinih organizacija u postupku početnih istraživanja i raspisivanja tendera[254].

Danska uprava za zaštitu konkurencije i potrošača je u 2013. godini ostvarila uvid u 20 projekata ugovora o javnim radovima. Pored toga, razmatrala je i pet projekata na tenderu, kao i nekoliko projekata u preliminarnim fazama. Uprava se u 2012. godini bavila sa 13 ugovora iz te oblasti, što ukazuje na rast interesovanja za tu vrstu projekata, što je dijelom bilo posledica pozitivnih iskustava Danske sa modelom javno-privatnog partnerstva. Pozitivno dansko iskustvo je, između ostalog, rezultat i studije o prvih 13 projekata javno-privatnog partnerstva, koje su svi ugovorni subjekati ocijenili kao uspješne. Pored toga, od devet već realizovanih projekata svi su završeni na vrijeme, a osam od devet u okviru opredijeljenih budžetskih sredstava. Ovo se, među raznim drugim

[251] Ibidem, p. 28
[252] Brøgger T., Kristiansen F.Ø.: Denmark, In: Çakmak Z., Çağdaş E. E.: *Global Public-Private partnership (PPP) guide*, Çakmak Yayınevi ve Medya Limited Şirketi, Ankara, 2016, p. 37
[253] Petersen H. O.: Regulation of public–private, partnerships: the Danish case, *Public Money & Management* Vol. 30, Issue 3, 2010, p. 177
[254] *Dedicated Public-Private Partnership Units A Survey of Institutional and Governance Structures*, OECD Publishing, 2010, p. 98

faktorima, može pripisati i modelu javno-privatnog partnerstva, koji ohrabruje opštine i regione da se usredsrede na troškove ostvarivanja vitalnih funkcija na svojim područjima i da dijele rizike sa svojim privatnim partnerima[255].

Javno-privatno partnerstvo u Danskoj nije precizno definisano zakonskim aktima, danska vlada ne koristi finansijske instrumente za podršku uspostavljanju predmetnih projekata, niti je uspostavila centralno tijelo za koordinaciju javno-privatnog partnerstva. Pojam javno-privatnog partnerstva se pominje u odeljku 2 vladine Uredbe o javnim objektima, po kojoj vlasnik javne zgrade mora da se brine o objektu koji je predmet Zakona o državnoj gradnji, u smislu da je dužan da razmotri da li izgradnja može donositi korist iz perspektive javno-privatnog partnerstva. Prema zakonski neobavezujućim Smjernicama o javno-privatnom partnerstvu, Uredba o javnim objektima, javno-privatno partnerstvo se definiše kao saradnja koja podrazumijeva visok nivo privatne uključenosti u javnu izgradnju i funkcionisanje tih zgrada. U uslovima postojanja veoma malog broja, i to parcijalno usmjerenih, propisa i normativa koji se odnose na tu oblast, učinjeni su i pokušaji donošenja odgovarajućih strategija (usvojene su dvije), koje takođe nijesu imale značajniji efekat u smislu regulisanja koncepta danskih javno-privatnih partnerstava. Ni prva ni druga predmetna strategija nisu imala značajnog efekta na uspostavljanje koncepta javno-privatnog partnerstva u Danskoj. U suštini, propisima je obuhvaćen samo mali dio projekata JPP, koji su vezani za projektovanje, izgradnju, korišćenje i održavanje zgrada, u smislu utvrđivanja obaveza javnih i privatnih subjekata u određenom broju godina[256].

3.5.3. Javno-privatno partnerstvo u Austriji

Istorija javno-privatnog partnerstva Austrije počinje u XIX vijeku, tačnije 1874. godine kada je dodijeljena prva koncesija privatnom konzorcijumu za izgradnju, finansiranje i rad železničke pruge između Steinaha i Rida (poznata pod nazivom Kronprinz Rudolphsbahn). U vezi sa realizacijom ovog projekta značajno je da je njegovo finasisaranje bilo moguće tek nakon što je država dala finansijsku garanciju, kao i to da je projekat realizovan prije planiranog vremena i da je u kasnijem periodu ta pruga nacionalizovana. Kao i u ostalim evropskim državama tokom XX vijeka, i u Austriji se obezbjeđenje usluga vezanih za infrastrukturu (putevi, željeznice, električna energija, telekomunikacije, voda, gradski prevoz i druge javne usluge) smatralo odgovornošću javnog sektora[257].

Austrija je sporo prihvatila javno-privatno partnerstvo kao sredstvo za pružanje javnih usluga, iako je od sredine 1990-ih godina eksperimentisala sa ovim modelom, što je za posledicu imalo samo nekoliko projekata u kojima je privatni sektor uključen u finansiranje javne infrastrukture i usluga. U

[255] *Executive summary of barriers to PPP in municipal and regional public works contracts*, Danish Competition and Consumer Authority, 2013, r. 1, dostupno na: https://www.en.kfst.dk/media/3304/20131209-executive-summary-of-barriers-to-ppp-in-municipal-and-regional-public-works-contracts.pdf

[256] Tvarnø D. C.: Legal, Financial and Governmental PPP Initiatives, *Fifth International PPP conference in Antwerpen*, 2016, pp. 12-13, dostupno na: https://openarchive.cbs.dk/bitstream/handle/10398/9387/2016%20tvarno%20legal%20finansiel%20and%20governmental%20PPP%20initiatives.pdf?sequence=1

[257] Bastin J.: Public-Private Partnerships: *A Review of International and Austrian Experience, Public Private Partnership*, Studiengesellschaft für Wirtschaft und Recht, Wirtschaftsuniversität Wien, Vienna, 2003, p. 6

stvaranju nacionalnog koncepta javno-privatnog partnerstva Austrija je koristila iskustva država u srednjoj i istočnoj Evropi i Velikoj Britaniji, te u manjoj mjeri Njemačke. U početnom periodu je zabilježena povećana motivacija za implementaciju projekata javno-privatnog partnerstva usled uticaja međunarodnih iskustva, nakon čega je zabilježen pad interesovanja, s obzirom da je došlo do ograničavanja projekata iz javnog budžeta u skladu s Mastrihtskim kriterijumima EU koji se odnose na deficit državnog budžeta[258].

U odnosu na države Srednje i Istočne Evrope, broj projekata javno-privatnog partnerstva u Austriji bio je znatno niži, iako su ograničenja u javnom budžetu porasla, posebno na nivou regiona i opština. S druge strane, zahtjevi za predmetnim partnerstvom ostali su nepomijenjeni. Karakteristično je da se nakon finansijske krize 2009. godine austrijska vlada nije vratila na uobičajeni nivo javnih ulaganja u infrastrukturu i javne usluge, zbog čega je potreba za obnavljanjem, proširivanjem ili održavanjem infrastrukture postajala sve veća. Pored toga, Austrija drži svoje javne dugove pod strožijom kontrolom od ostalih evropskih država, tako da ima više sredstava u rezervi. Međutim, na pokrajinskom i opštinskom nivou, aspekt zadržavanja projekata izvan javnog budžeta će i dalje imati nesumnjivo važnu ulogu[259].

Transportni sektor (prije svega putevi, tuneli i žjeleznica) je najznačajnije tržište za velike projekte javno-privatnog partnerstva u Austriji, ne samo zahvaljujući austrijskoj topografiji, već i kao rezultat procesa pridruživanja istočnoevropskih zemalja Evropskoj uniji (Tabela br. 13). Ovo je povećalo geografski značaj Austrije zbog intenziviranja tranzitnog saobraćaja prema Istočnoj Evropi i iz nje . Pored transporta, zaštita okoline i zdravstveni sektori potencijalna su područja rasta za programe malih i srednjih privatnih kompanija. Međutim, imajući u vidu dosadašnji broj projekata javno-privatnog partnerstva u ovim domenima, evidentno je da Austriji još uvijek nedostaje dugoročni pristup za sprovođenje javno-privatnog partnerstva. Uspostavljanje nadležnog centra za javno-privatno partnerstvo, kao što to preporučuje privatni sektor, ne samo da bi obezbijediilo zakonske smjernice za javni i privatni sektor, već bi služilo i kao centar za stručno znanje koje je neophodno za pripremu i primjenu programa javno-privatnog partnerstva.[260].

godina	NAZIV PROJEKTA	SEKTOR	IZNOS (mil. eura)
2003.	Graz Intermodal Freight Centre	transport	40
2004.	Europpass LKW Maut	transport	48
2006.	Ostregion	transport	350
2014.	Zwettl Road Bypass	transport	29
2017.	Campus Berresgasse	obrazovanje	21
		UKUPNO	488

Tabela br. 13.: Pregled projekata javno privatnog partnerstva Austrije finasiranih od strane EIB za period 1990-2018[261]

[258] Schaffhauser-Linzatti M.: Risk menagement in an Austrian standardised public-private partnership model, In: Akintoye A., Beck M., Hardcastle C.: *Public-private partnerships, managing risk and opportunities*, Blackwell Science, 2003, p. 245

[259] Hamerl T.: Austria, In: Ivan Mattei E. I., Rivera J. A.: *Public-Private Partnerships 2015*, Law Business Research Ltd, London, 2015, p. 16

[260] *Global Guide toPublic-PrivatePartnerships*, Allen & Overy LLP, UK, 2010, p. 145

[261] *PPPs financed by the European Investment Bank from 1990 to 2018*, European Investment Bank, 2019, pp. 6-15

Većina dosadašnjih projekata javno-privatnog partnerstva u Austriji ostvarena je na pokrajinskom ili opštinskom nivou. Na nacionalnom nivou postojalo je samo nekoliko velikih projekata saradnje javnog i privatnog sektora. Najpoznatiji projekti javno-privatnog partnerstva bili su *Vienna Climatic Wind Tunnel* kao najveće svetsko postrojenje za testiranje šinskih vozila, i kargo centar u Gracu. U izgradnji kargo centra učestvovao je konzorcijum privatnih transportnih i špediterskih kompanija, tri najveće štajerske banke, štajerska pokrajinska vlada i savezna vlada Austrije. U junu 2003. godine, kargo centar Grac počeo je sa radom kao jedan od najefikasnijih evropskih teretnih saobraćajnih centara, a u 2008. godini ovaj centar je zabilježio promet robe od 800.000 tona. I u austrijskom zdravstvenom sektoru država tradicionalno igra snažnu ulogu u funkcionisanju zadravstvenih ustanova. Međutim, na tržištu su u novije vrijeme registrovani brojni primjeri partnerstva privatnog sektora i opštinskog nivoa vlasti malog i srednjeg obima. Tako je znatan broj bolnica kojima upravljaju opštine donio odluku da sarađuje sa privatnim sektorom kako bi se podmirili sve veći troškovi. Vodeća privatna austrijska kompanija iz ovog sektora, VAMED AG bavi se kako generalnim planiranjem i izvođenjem radova (po principu ključ u ruke) tako i organizovanjem rada raznih bolnica i domova zdravlja. Primjeri za to su Centar za majku i dijete u Lincu, koji je finansirala austrijska banka, izgradnja bolnice u Voklabruku, rekonstrukcija bolnice u Steiru, kao i planiranje, izgradnja, finansiranje i rad urgentne bolnice u Lincu[262].

Jedan od pozitivnih primjera javno-privatnog partnerstva u području zdravstva je i ugovor o obezbjeđenju podrške za sterilizaciju za tri bolnice u Vorarlbergu, sa ciljem poboljšanja nivoa usluga, postizanja ušteda kroz efikasniju strukturu i organizaciju rada, te ostvarivanje ekonomične i konkurentne cijene usluga. Partner za taj projekat je izabran u skladu sa EU modelom tendera na dva nivoa, pri čemu je osnovana nova kompanija sa mješovitim učešćem javnog sektora (51% udijela) i privatnog partnera (49% udijela) odgovorna za sterilizaciju medicinske opreme za tri pomenute regionalne bolnice. Urgentna bolnica u Donjoj Austriji bila je prije toga na ivici zatvaranja, a kroz javno-privatno partnerstvo je uspješno transformisana u savremeni holistički (psihosomatski) centar za njegu Valdviertel (PSCV). Licenca za rad koja uključuje razvoj, planiranje, implementaciju projekata, cjelokupno finansiranje i opšte upravljanje i pružanje usluga, dodijeljena je projektnoj kompaniji osnovanoj za projekat u skladu sa austrijskim bolničkim planom i smjernicama o njezi. Osnovana kompanija obuhvata tri kompanije KAV (51% udela), ROMED (39% udela) i VAMED (10% udela)[263].

Primjer uspješnog javno-privatnog partnerstva u obrazovanju je projekat osnovne škole „Bednar park“ u Beču. Grad Beč dodijelio je ugovor za izgradnju, rad i održavanje zgrade osnovne škole i vrtića, za period od 25 godina nakon završetka izgradnje, kompaniji Porr Solutions Immobilien- und Infrastrukturprojekte GmbH. Ukupni troškovi projekta su iznosili oko 38 miliona eura[264].

Kada se radi o zakonodavnom okviru javno-privatnog partnerstva, u Austriji ne postoji poseban zakon, već su ta pitanja regulisana opštim pravilima javnih nabavki. Drugim riječima, austrijski propisi javno-privatno partnerstvo obično klasifikuju kao koncesiju za usluge ili radove.

[262] *Global Guide to Public-Private Partnerships*, Allen & Overy LLP, UK, 2010, pp. 146-147
[263] Nikolic A. I., Maikisch H.: *Public-Private Partnerships and Collaboration in the Health Sector, An Overview with Case Studies from Recent European Experience*, World Bank Publications, Washington, 2006, pp. 15-17
[264] *Global Guide to Public-Private Partnerships*, Allen & Overy LLP, UK, 2010, pp. 148

Kada je riječ o regulisanju javnih nabavki, najvažniji zakonski akt je Savezni zakon o javnim nabavkama i Savezni zakon o dodjeli ugovora u oblastima odbrane i bezbjednosti. Zbog federalne strukture države (savezna država, pokrajine i opštine), na regionalnom nivou postoji devet zasebnih akata o javnim nabavkama. Savezni zakon o javnim nabavkama se primjenjuje na sve javne tendere koje raspisuju devet austrijskih pokrajina, odnosno zajednice i javna tijela koja njima upravljaju. Nasuprot tome, postupci revizije na regionalnom nivou ne podležu odredbama predmetnog zakona, već su uređeni sa devet različitih regionalnih zakona. Sadržinski, ovi regionalni zakoni ne odstupaju značajno od postupaka revizije predviđenih u Saveznom zakonu. Klasični ugovorni organi obuhvaćeni Saveznim zakonom o javnim nabavkama su savezna država, pokrajine (regionalne države) i opštine, udruženja formirana od ranije pomenutih tijela i „tijelo koje upravlja javnim zakonom“ kao subjekt koji kontroliše, finansira ili nadgleda ugovaranje. To tijelo se osniva radi služenja potrebama u opštem interesu i kao takvo nema industrijski ili komercijalni karakter[265].

Uopšteno uzevši, ugovori o snabdijevanju, ugovori o uslugama i ugovori o radovima koje dodjeljuju gore navedeni ugovorni autoriteti podležu propisima o nabavkama. U sektoru komunalnih usluga primjenjuje se manje strog režim. Autoritet za ugovaranje ima veću slobodu u izvršavanju postupka nabavke (na primjer, širi izbor prihvatljivih tenderskih postupaka). Pored toga, Savezni zakon o javnim nabavkama utvrđuje posebna pravila i odredbe koje se primjenjuju na dodjelu ugovora o pružanju usluga i koncesija za radove. Ugovori o koncesiji za usluge ili radove su ugovori iste vrste kao i ugovori o uslugama ili radovima, osim činjenice da se naknada za usluge ili radove koje treba izvesti sastoji isključivo od prava na eksploataciju usluga ili izgradnje, ili od takvog prava zajedno sa određenim iznosom plaćanja. Koncesije za usluge i radove reguliše Savezni zakon, ali se fleksibilniji režim primjenjuje na klasične ugovore o radovima i uslugama. Što se tiče davanja koncesija za usluge, moraju se poštovati osnovni evropski principi (jednak tretman i transparentnost) i princip nediskriminacije. Pored toga, u Zakonu se navodi da se u zavisnosti od predmeta i vrijednosti ugovora - koncesija za usluge u principu dodjeljuje putem konkursne procedure. Postupci za dodjelu koncesija za usluge ne spadaju u sudsku praksu upravnih sudova, već ih je moguće osporiti pred građanskim sudovima. Što se tiče koncesija za radove, primjenjuju se samo neke odredbe zakona (minimalni rokovi, sadržaj tenderske dokumentacije, pravila o dodjeli ugovora, dio o pravnim ljekovima). I pored toga, moraju se poštovati opšti principi transparentnosti i jednakog postupanja[266].

Pored navedenog, u Austriji se široko koriste okvirni sporazumi, posebno u tržišnim sektorima koje karakteriše značajna dinamika cijena (npr. informacione tehnologije ili tržišta električne energije i gasa). Međutim, okvirni sporazumi su dostupni samo u otvorenim, ograničenim ili pregovaračkim procedurama. U principu, rok okvirnog sporazuma ne smije biti duži od trogodišnjeg perioda. Okvirni sporazumi mogu se zaključiti između jednog ili više subjekata za ugovaranje na jednoj strani i jednog ili više subjekata sa druge strane. Na taj način su ostvareni pojačana konkurencija i fleksibilnost, a obije prednosti su široko poštovane od strane ugovornih organa. Ugovorni organi imaju pravo da zajedno sprovode tenderske postupke. Štaviše, Zakon omogućava osnivanje centralnih subjekata za nabavke, a jedan od njih je i Austrijska federalna agencija za nabavke. Njen glavni zadatak je pružanje

[265] Marboe J P., Lassner N.: Austria, In: Davey J., Gatenby A.: *The Government Procurement Review*, Law Business Research Ltd, London, 2015, pp. 14-15
[266] Ibidem, p. 16

usluga nabavke saveznoj državi, pokrajinama i opštinama, kao i udruženjima koja su formirana od strane određenih zakonom predviđenih tijela[267].

Zakon predviđa da ugovorni organi moraju koristiti jedan od sledećih tenderskih postupaka: otvorene, ograničene ili pregovaračke procedure, direktnu dodjelu (sa ili bez prethodnog ispitivanja javnog tržišta), konkurentski dijalog, dinamički sistem nabavke, elektronsku aukciju, konkurs za projekat i realizaciju ili okvirni ugovor. U principu, pregovarački postupak može biti izabran, osim ako je otvoren ili ograničen postupak uz prethodnu najavu doveo do bilo koje ponude pogodne za kupovinu. Međutim, originalni uslovi ugovora ne smiju se bitno mijenjati i dopunjavati. Dakle, pregovarački postupak može biti izabran ako posebne karakteristike ugovora ne dozvoljavaju otvoren ili ograničen postupak, ili se usluge ugovora ne mogu odrediti u ugovornim specifikacijama. Takmičarski dijalog je najprikladniji ako se traže rešenja posebno složenih projekata. To je slučaj kada se ne mogu utvrditi tehničke specifikacije ili pravni ili finansijski uslovi projekta. U strogom smislu, elektronska aukcija treba da bude kvalifikovana kao dio tenderskog postupka.

3.6. Javno-privatno partnerstvo u zakonodavstvu Crne Gore

Početak razvoja javno-privatnog partnerstva u Crnoj Gori vezuje se za početak XX vijeka, odnosno za potpisivanje dva velika ugovora o koncesiji sa stranim kompanijama privatnog sektora za izgradnju i održavanje pruge između Bara i Virpazara i pomorskog saobraćaja između Bara, Ulcinja i Skadara. Kada je riječ o savremenom dobu, razvoj javno-privatnog partnerstva u Crnoj Gori započinje 2002. godine, nakon usvajanja Zakona o učešću privatnog sektora u vršenju javnih usluga, koji je imao za cilj poboljšanje saradnje između javnog i privatnog sektora u toj oblasti[268]. Iako zakon uređuje različite forme javno-privatnog partnerstva (koncesije, lizing, ugovor o upravljanju i drugo), svaki od navedenih oblika je regulisan posebno, a u pojedinim slučajevima pozivanjem na proceduru javnih nabavki.

Prema odredbama Zakona o učešću privatnog sektora u vršenju javnih usluga, koncesije je moguće dodijeliti samo za prirodne resurse, dok je aranžmane izgradnja- funkcionisanje-transfer moguće primijeniti u oblastima saobraćaja, vodosnadbijevanja, elektroenergetike. U zakonski postupak su bila uključena brojna tijela javnog sektora, poput Savjeta za privatizaciju, što cio proces čini zamršenim. Postupak izbora projekata je nejasno formulisan, a pojedini članovi ovog zakona (na primjer odredbe koje stimulišu predkvalifikaciju i pozive za dostavljanje ponuda nijesu jasno razgraničene) komplikovani su za praktičnu primjenu. Odredbe koje se bave projektnim ugovorima su dovoljno fleksibilne, ali su trebale biti bolje formulisane. Nesumnjivo je da su pomenutim zakonom regulisana brojna značajna pitanja, ali na nedovoljno koherentan način. Uz to, u zakonskom tekstu se koriste i termini koji nisu definisani. Takođe, dio odredbi nije dovoljno preciziran, a neke su i u međusobnoj koliziji. Zbog svega toga predmetni zakon nije obezbijedio stabilnost i pouzdanost zakonskog okvira[269].

Iako u dosadašnjem periodu u Crnoj Gori nije bilo posebne organizacione cjeline zadužene za javno-privatno partnerstvo, dvije institucije, i to Kancelarija premijera i Komisija za koncesije, imale

[267] Ibidem, p. 17
[268] *Montenegro-PPP Units and Related Institutional Framework*, European PPP Expertise Centre, 2014, p. 4
[269] Sredojević G.S.: *Javno-privatno partnerstvo*, Arhipelag i Institut ekonomskih nauka, Beograd, 2010, str. 156-159

su značajnu ulogu u promociji ovog koncepta. Pored toga, korišćena je praksa formiranja jedinice na projektnoj osnovi. Prva takva jedinica uspostavljena je za projekat autoputa Luka Bar-Boljare. U praksi, predmetne organizacione cjeline okupljale su predstavnike različitih ministarstava, kao i pojedine eksperte i specijaliste[270].

Aktivnosti na unapređenju zakonodavnog okvira su rezultirale usvajanjem novog Zakona o koncesijama kojim su izmijenjene odredbe Zakona o učešću privatnog sektora u vršenju javnih usluga u pogledu koncesija i aranžmana BOT, kao i procedure prema kojima ugovorne strane mogu da koriste predmetni oblik javno-privatnog partnerstva. Zvanični podaci ukazuju da su u Crnoj Gori u periodu od 1999. do 2013. godine zaključena 183 ugovora o koncesiji[271].

S druge strane javno-privatna partnerstva su uglavnom primjenjivana za realizaciju projekata na lokalnom nivou, prije svega na planu unapređenja turističkih usluga. O tome svedoče projekti „NTC Marina“ i „Bigovo“ u Kotoru, „Dobra luka“ u Herceg Novom, „Ostrvo cvijeća“ u Tivtu, kulturno-istorijski objekat „Virpazar“ u Baru, „Cmiljača“ u Bijelom Polju, „Valdanos”, „Velika Plaža”i „Ada Bojana” u Ulcinju i „Kraljičina Plaža” u Baru i Budvi. Pored navedenih, realizovani su i određeni projekti javno-privatnog partnerstva na nacionalnom nivou, kao što je projekat besplatnog bežičnog pristupa internetu za građane Crne Gore u informaciono-komunikacionom sektoru, projekat izgradnje novog studentskog doma u Podgorici, te registracija nacionalnog domena „me“ koji je obezbijeđen preko privatne kompanije. Kada se radi o novom studentskom domu, sam projekat je realizovalo Ministarstvo obrazovanja. Privatni partner je bio odgovoran za projektovanje, finansiranje, izgradnju i rad studentskog smještaja koji će biti prenesen Ministarstvu nakon isteka ugovora (30 godina). Pored navedenih projekata, i Ministarstvo zdravlja je realizovalo dvije koncesije. Naime, u 2010. godini potpisan je 25-godišnji ugovor za finansiranje, izgradnju i rad opreme računarske tomografije, kao i 15-godišnji ugovor za finansiranje, izgradnju i rad postrojenja za medicinski otpad. Ministarstvo ekonomije je ostvarilo 13 koncesija za izgradnju i rad malih hidroelektrana u okviru dva procesa tendera koji su sprovedeni u 2008. i 2010. godini. Četiri procesa su prevremeno prekinuta zbog neispunjavanja ugovornih obaveza od strane privatnih partnera[272].

Na lokalnom nivou realizovano je nekoliko projekata, kao što je izgradnja dva tržna centra („Bazar“ i „Mall of Montenegro”) i projekat socijalnog stanovanja u Podgorici, tržni centar u Budvi („Plaza“), mali projekat ulične rasvete prema ugovoru za komercijalni i turistički razvoj „Lipske pećine“ na Cetinju (25 godina) i putni projekti u Herceg Novom (koncesija na 22 godine).[273]

Kao i za države u okruženju, i za Crnu Goru je politička i pravna sigurnost od posebnog značaja za ostvarivanje javno-privatnog partnerstva, naročito ukoliko se radi o stranom ulagaču (partneru). Činjenica je da je crnogorska privreda nedovoljno razvijena i da u mnogome, kao i ostale države u okruženju, zavisi od stranih investicija, zato je veoma važno što odredbe posebnog Zakona o stranim investicijama otvaraju širi prostor i daju garancije stranim ulaganjima da se njihova imovina ne može eksproprisati, osim kada je u pitanju javni interes koji je određen zakonom ili na osnovu zakona, ali uz adekvatnu nadoknadu. Zakon o učešću privatnog sektora u vršenju javnih usluga

[270] *Montenegro-PPP Units and Related Institutional Framework*, European PPP Expertise Centre, 2014, p. 4
[271] Vujačić S.: Montenegro, In Çakmak Z., Ergün E. C.: *Global public-private partnership (PPP) guide*, Çakmak Yayınevi ve Medya Limited Şirketi, 2016, p. 156
[272] *Montenegro - PPP Units and Related Institutional Framework*, European PPP Expertise Centre, 2014, pp. 5-6
[273] *Public-private partnership analysis*, Network for Affirmation of NGO Sector, Balkan monitoring public finances, 2017, p. 2

predviđa da pravila i propisi donijeti na osnovu ovog zakona, koji mogu uticati ili štetiti dodijeljenim ili stečenim pravima u skladu sa poništenim zakonodavstvom, neće imati retroaktivni efekat[274].

Kao i druge države bivše SFRJ i Crna Gora je dograđivala nacionalno zakonodavstvo u području javno-privatnog partnerstva u potrazi za adekvatnim normativnim okvirom. U ovoj oblasti je pravni okvir činilo nekoliko sektorskih zakona[275]. Međutim, nijedan od njih nije u potpunosti odražavao suštinu javno-privatnog partnerstva, zbog čega je bilo potrebno upotpuniti ovu pravnu prazninu. U toku je postupak donošenja Zakona o javnom privatnom partnerstvu u cilju stvaranja novog zakonodavnog okvira za adekvatno ostvarivanje javno-privatnog partnerstva. Ovaj novi zakon treba da zamijeni Zakon o koncesijama i druge sektorske zakone.

U cilju aktuelnosti rada ukratko ćemo analizirati aktuelni Predlog Zakona o javno-privatnom partnerstvu. Vlada Crne Gore je sa Predlogom Zakona napravila značajan iskorak u smjeru adekvatnije normativne regulative ove oblasti, s obzirom na prethodna iskustva i činjenice da je u postupku usvajanja jedinstveni akt kojim su definisana sva pitanja od značaja za realizaciju projekta javno-privatnog partnerstva. Analizom sadržaja predmetnog Predloga zakona, evidentno je da je zakonodavac posebno vodio računa o usklađenosti zakona sa relevantnom regulativom Evropske unije.

Na osnovu analize Predloga uočava se cjelovit pristup problematici javno-privatnog partnerstva, ali postoji neusklađenost pojedinih odredbi kojima se konkretnije uređuje oblast primjene budućeg zakona. Otklanjanje nedorečenosti u zakonskom tekstu je veoma značajno, jer je potrebno precizno utvrditi područja u kojima investitor može ostvariti partnerstvo sa državom ili lokalnom zajednicom. S druge strane, načinjen je kvalitativan pomak u određivanju vrsta projekata koji se mogu ostvarivati kroz javno-privatno partnerstvo. Naime, u ovom slučaju uži ili širi pristup prvenstveno zavisi od države i njene zainteresovanosti, pri čemu u ovom trenutku ne postoje opšteprihvaćene smjernice. Zato je važno da se zakonodavac odlučio za šire određenje, pri čemu nije isključena ni jedna relevantna oblast za javno-privatno partnerstvo[276].

Predlog zakona obuhvata i razradu procedure pripremanja projekata. Prema predloženim zakonskim rešenjima, naručilac pripremljen projekat dostavlja nadležnoj Agenciji koja na predloženi projekat daje svoje mišljenje i kao takvo dostavlja Ministarstvu finansija, koje u okviru svojih nadležnosti ocjenjuje finansijske efekte. Nakon realizovane javne rasprave izrađuje se godišnji plan odobrenih projekata javno-privatnog partnerstva, a konačnu odluku o njihovom prihvatanju donosi Vlada[277].

Jedno od pozitivnih rešenja u Predlogu zakona je osnivanje posebne agencije (Agencija za investicije) za koju su predviđene nadležnosti u oblasti promocije investicionog potencijala i praćenja realizacije investicija javno privatnog partnerstva i zaključenih ugovora o koncesijama. Pored

---

[274] Vujačić S.: Montenegro, In Çakmak Z., Ergün E. C.: *Global public-private partnership (PPP) guide*, Çakmak Yayınevi ve Medya Limited Şirketi, 2016, p. 154

[275] To su Zakon o koncesijama („*Službeni list Crne Gore*“, 08/09); Zakon o učešću privatnog sektora u obavljanju javnih usluga („*Službeni list Crne Gore*, br. 30/02 i73/10); Zakon o stranim investicijama („*Službeni list Crne Gore*“, br. 8/11), Zakon o javnim nabavkama („*Službeni list Crne Gore*“, br. 42/11, 45/14); Zakon o prostornom razvoju i izgradnja objekata („*Službeni list Crne Gore*“, br. 51/08 i 33/14); Zakon o državnoj upravi („*Službeni list Crne Gore*“, br. 38/03 i 42/11).

[276] *Predlog Zakona o javno-privatnom partnerstvu*, čl. 5-6, dostupno na: https://www.paragraf.me/nacrti_i_predlozi/predlog-zakona-o-javno-privatnom-partnerstvu.pdf

[277] *Predlog Zakona o javno-privatnom partnerstvu*, čl. 37-45

navedenih opštih nadležnosti, Agencija ima značajnu ulogu jer odobrava sve projekte javno-privatnog partnerstva. Drugim riječima, Agencija ima zadatak da utvrdi usaglašenost predloga ugovora o predmetnom partnerstvu sa relevantnim propisima, ali i opravdanost projekta iz ugla prioriteta razvoja države i lokalne zajednice. Na taj način Agencija je ujedno i krovni organ koji ima nadzornu ulogu nad svim javnim naručiocima projekata. S obzirom da je zakonodavac predvidio veliki broj javnih naručilaca, nesumnjivo je da Agencija mora imati adekvatne kapacitete u cilju ostvarivanja efikasnosti institucionalnog okvira u oblasti javno-privatnog partnerstva Crne Gore. Pri tome treba uzeti u obzir da Agencija nema zakonsku mogućnost angažovanja spoljnih stručnih saradnika[278].

Takođe su značajne i odredbe koje propisuju da javni naručilac ima obavezu utvrđivanja potencijala određenog projekta javno-privatnog partnerstva na osnovu koga priprema predlog čiji je sadržaj zakonom određen. U vezi sa tim, pažnju zaslužuje rešenje kojim se javnom naručiocu daje mogućnost angažovanja stručnih savjetnika u skladu sa potrebama[279].

Predlog zakona uključuje i potrebne mjere zaštite od korupcije i osiguranja integriteta procesa nabavki potrebnih za realizaciju projekata javno-privatnog partnerstva. To se posebno odnosi na odredbe koje ukazuju na obavezu javnog naručioca da u procesu dodjeljivanja ugovora preduzme sve neophodne radnje u cilju sprečavanja prevare, korupcije i favorizovanja ponuđača i da efikasno spriječi sukob interesa, u cilju sprečavanja pojava narušavanja konkurencije na tržištu, kao i obezbjeđenja transparentnosti postupka.

Može se ocijeniti da su u Predlog zakona: uključene adekvatne mjere koje sprečavaju koruptivne radnje u postupku dodjele ugovora[280]; autori uvažavali relevantnu međunarodnu praksu, ostavljajući mogućnost osnivanja projektne kompanije (*special purpose vehicle*) koja je u funkciji realizacije određenog projekta javno-privatnog partnerstva. Na taj način data je mogućnost potencijalnim investitorima da ostvare različite pogodnosti, posebno u domenu projektnog finansiranja[281].

[278] *Predlog Zakona o javno-privatnom partnerstvu,* čl. 13-25
[279] *Predlog Zakona o javno-privatnom partnerstvu,* čl. 37 i 38
[280] *Predlog Zakona o javno-privatnom partnerstvu,* čl. 64
[281] *Predlog Zakona o javno-privatnom partnerstvu,* čl. 33

ČETVRTI DIO

JAVNO-PRIVATNO PARTNERSTVO U ZAŠTITI KRITIČNE INFRASTRUKTURE

Nastanak i razvoj javno-privatnog partnerstva u bezbjednosnoj sferi predstavlja novu koncepciju unutar bezbjednosti, koja je po svojoj prirodi promjenljivog karaktera jer je uslovljena suštinskim promjenama u savremenim društvima, političkim i ekonomskim nestabilnostima u pojedinim državama, pojavom novih oblika svojine, uspostavljanjem širokog spektra aktera na tržištu bezbjednosti, kao i brzim razvojem privatnog poslovanja. Ipak, do sada se nije došlo do jedinstvene definicije javno-privatnog partnerstva u bezbjednosti. Primjera radi, pojedini autori na predmetni koncept gledaju kao na odnose izgrađene na potrebama, mogućnostima i dvosmjernoj komunikaciji među bezbjednosnim partnerima[282], dok je za druge taj koncept zasnovan na ugovornim aranžmanima u kojima se dijele resursi i mogućnosti[283]. Pored navednih definicija, javno-privatna partnerstva se nerijetko određuju kao organizovani napori sa institucionalnom podrškom i pismenim sporazumima, ili kao oblici neformalne saradnje[284].

Nezavisno od preciznosti definicija, za javno-privatno partnerstvo u bezbjednosti je karakteristično da mora biti javno dostupno, posvećeno, angažovano i zakonski održivo. To partnerstvo je ujedno aranžman između javnog (vladinog) sektora i subjekta privatnog sektora bezbjednosti, uspostavljen u svrhu pružanja bezbjednosne usluge, zadovoljavanja bezbjednosnih potreba zajednice i srodnih bezbjednosnih usluga. Takva partnerstva karakterišu dijeljenje kompetencija, rizika, odgovornosti, rezultata i nagrada između partnera. Važno je napomenuti da u javno-privatna partnerstva u ovoj oblasti ne moraju spadati svi ugovori koje javne agencije sklapaju sa privatnim sektorom za obavljanje poslova bezbjednosti, niti svi slučajevi finansiranja ili odobravanja mogućnosti privatnim subjektima, pošto se dio tih aranžmana može na različite načine klasifikovati i odrediti, poput međuvladinog bezbjednosnog menadžmenta ili međuvladinih bezbjednosnih odnosa[285].

Obično postoji tendencija da se javno-privatno partnerstvo u bezbjednosti uspostavlja u hijerarhijskoj strukturi koja odražava hijerarhiju javne uprave. S druge strane, države sa dugom tradicijom raspodjele moći između javnog i privatnog sektora obično imaju manje izraženu hijerarhijsku strukturu u javnoj administraciji. U tim okolnostima, država (vlada) ima po, pravilu pragmatičan pristup i nema potrebe za detaljnom pravnom regulativom, budući da sporazume i

[282] Prenzler T., Sarre, R. Public-private crime prevention partnerships. In: Prenzler T.: *Policing and security in practice: challenges and achievements*, Palgrave Macmillan UK,2012, pp. 149–197

[283] Nemeth C..P. *Private Security and the Law*, Elsevier, USA, 2012, pp. 139–140

[284] Sparrow M.K.: Managing the boundary between public and private policing, New Perspectives in Policing Bulletin,U.S. Department of Justice, National Institute of Justice, Washington,DC, 2014, dostupno na: https://www.ncjrs.gov/pdffiles1/nij/247182.pdf

[285] Schaeffer P. V., Loveridge S.: Toward an understanding of types of public-private cooperation, *Journal Public Performance & Management Review*,Vol. 26 (2), 2002, pp. 169–189, dostupno na: https://www.researchgate.net/publication/247885699_Toward_An_Understanding_Of_Types_Of_Public-Private_Cooperation

protokole o objavljivanju podataka smatra dovoljnim za uspostavljanje i unapređenje saradnje između privatne i javne bezbjednosti[286].

Kada se govori o javno-privatnom partnerstvu u zaštiti kritične infrastrukture, treba napomenuti da se izraz zaštita kritične infrastrukture prvenstveno odnosi na one aktivnosti koje su usmjerene na njenu zaštitu od fizičkih napada ili opasnosti. Ove aktivnosti mogu biti usmjerene i na odvraćanje od napada (ili ublažavanje njihovih efekata) koji su posledica djelovanja čovjeka ili prirodnih nepogoda. Primarna odgovornost za zaštitu kritične infrastrukture i za odgovor ukoliko je šteta već nanijeta leži na vlasnicima i operatorima. Međutim, kada postoji javno-privatno partnerstvo u zaštiti kritične infrastrukture vlada i vlasnici - operatori zajedno rade na identifikaciji te infrastrukture, a zatim i na procjeni stepena rizika povezanog sa tom imovinom i resursima. Ako vlasnici i operatori ne žele ili nijesu u mogućnosti da učestvuju u ovom procesu, vlada može intervenisati, procijeniti i propisati nivo zaštite i osmisliti odgovore na potencijalne prijetnje[287]. Povezanost države i operatora je poseban element koji razlikuje zaštitu kritične infrastrukture od ostalih područja unutrašnje bezbjednosti države. S obzirom na trend da sve veći dio kritičnih infrastruktura prelazi u privatne ruke, ova oblast politike zahtijeva značajnu i obimnu koordinaciju između države (vlade) i privatnog sektora[288]. Sve to ukazuje na kompleksnost zaštite kritične infrastrukture i upućuje na potrebu iznalaženja sveobuhvatnog rešenja u toj oblasti. Izvjesno je da opšteprihvaćeno rešenje ne postoji, jer svaka država u skladu sa svojim interesima, mogućnostima i definisanim obimom i sadržajem kritične infrastrukture razvija sopstveni sistem zaštite. S druge strane, evidentno je proširivanje sadržaja kritične infrastrukture na nacionalnom nivou, od toga da se ona ranije prvenstveno odnosila na oružane snage i sistem odbrane i bezbjednosti države, do savremenih određenja kritične infrastrukture po kojima je ona okrenuta funkcionisanju ne samo države, već i društva u cjelini. To su, između ostalog, razlozi koji zahtijevaju definisanje i uspostavljanje dodatnih kapaciteta vezanih za njenu zaštitu.

4.1. Uloga države (javnog sektora) u zaštiti kritične infrastrukture

Izraz „javni sektor“ odnosi se na agencije koje su u vlasništvu ili kojima upravlja država. Primjeri prve opcije su federalne, državne ili lokalne službe i ustanove, a druge postrojenja za prečišćavanje vode, elektrane i slično. Ti subjekti često dobijaju finansijsku podršku vlade, najvećim dijelom iz sredstava koja se prikupljaju od poreskih obveznika. Akteri javnog sektora su, u okviru svojih kompetencija, odgovorni za zaštitu ljudi i imovine. U praksi, država i lokalne samouprave sve češće ne uspijevaju da idu u korak sa razvojem i promjenama u području kritične infrastrukture. Najizraženiji problemi su vezani za obezbjeđenje finansijskih sredstava i potrebnog nivoa stručnosti kako bi bili ravnopravni sa privatnim sektorom[289].

---

[286] Prenzler T., Sarre R.: Public-private crime prevention partnerships. In: Prenzler T.: *Policing and security in practice: challenges and achievements*, Palgrave Macmillan UK, 2012, pp. 149–197

[287] Pesch-Cronin A. K., Marion E. N.: *Critical infrastructure protection, risk management, and resilience a policy perspective*, Taylor & Francis Group, 2016, pp. 8-9

[288] Nadav M.: *Comparative homeland security : global lessons*, John Wiley & Sons, 2011, pp. 261-262

[289] Cordesman A. H., Cordesman J. G.:*Cyber-Threats, Information Warfare, and Critical Infrastructure Protection*: Defending the U.S. Homeland. Westport, CT: Praeger, 2002, p. 18

S obzirom na značaj koji ima kritična infrastruktura za funkcionisanje društvene zajednice u cjelini, uloga države u toj oblasti je primarna. Ako se ta uloga hronološki posmatra i raščlani, ona je na samom početku vezana za definisanje pojma i identifikaciju nacionalne kritične infrastrukture. Primjeri mnogih država ukazuju da postoje značajne međusobne razlike, kako na nivou definisanja, tako i na nivou utvrđivanja kritične infrastrukture. U radu smo naveli primjer Njemačke, gdje je nacionalna infrastruktura razvrstana na vitalne tehničke i ključne socio-ekonomske uslužne infrastrukture, kao i primjer Velike Britanije, u kojoj je infrastruktura podijeljena na kritičnu nacionalnu infrastrukturu i ostale kritične infrastrukture[290].

Na osnovu relevantne literature i preovlađujuće međunarodne prakse, formalni postupak identifikacije i imenovanja nacionalnih kritičnih infrastruktura se ostvaruje kroz četiri faze[291]:

- identifikacija kritičnih sektora (podsektora), gdje se identifikuju sektori i (ili) podsektori koji se smatraju značajnim za nacionalne interese;
- identifikacija kritičnih usluga, koje se imenuju za svaki kritični sektor;
- imenovanje kritične infrastrukture za svaku kritičnu uslugu, pri čemu se identifikuju i imenuju i kritična sredstva - komponente koje sadrže kritičnu infrastrukturu;
- zaštita kritične infrastrukture, koja obuhvata postupke zaštite i bezbjednosti koji se implementiraju za svaki sektor kritične infrastrukture.

U fazi identifikacije kritičnih sektora, svaka država sastavlja početnu listu svojih kritičnih nacionalnih sektora, odnosno sektora koji postoje unutar geografskih granica njene teritorije i koji uključuju potencijalne kritične infrastrukture. Proces odabira kritičnih nacionalnih sektora i podsektora nije uvijek jednostavan, budući da svi nacionalni sektori nisu podjednako vitalni za svaku državu. Naime, neki sektori se mogu klasifikovati kao kritični, a neki kao manje kritični ili manje značajni. Štaviše, nisu ni sve službe sektora - podsektora jednako kritične, što otežava identifikaciju inicijalne liste kritičnih sektora na strateškom nivou.

U literaturi se mogu naći dva glavna pristupa za identifikaciju nacionalnih kritičnih službi po sektorima, u zavisnosti da li je vođen od države (odozgo na dolje) ili od operatora (odozdo na gore)[292]. U pristupu odozgo na dolje, vlada ima vodeću ulogu u definisanju i određivanju prioriteta kritičnih službi preko odgovarajućeg koordinacionog tijela ili nadležnog organa za zaštitu kritične infrastrukture. U tom slučaju, na centralnom nivou se sastavlja lista indikativnih usluga kritičnih nacionalnih sektora. Alternativno, lista nacionalnih kritičnih službi se sačinjava na međusektorskom (ili poprečnom) nivou. Zatim se vrednuju kritične službe, sa specifičnim kriterijumima, i postavljaju prioriteti da bi se dobila konačna lista nacionalnih kritičnih službi. Za svaku kritičnu službu sastavlja se lista zainteresovanih strana-operatora, iz koje se (ili u saradnji sa) izvlači lista najkritičnijih roba, proizvoda i sistema koji podržavaju određenu uslugu.U pristupu upravljanja odozdo na gore, vodeću ulogu imaju operatori kritičnih infrastruktura. Konkretno, nakon što su na centralnom nivou

---

[290] *National Security Strategy and Strategic Defence and Security Review*, UK Government, 2015, dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

[291] Gritzalis D., Stergiopoulos G., Kotzanikolaou P., Magos E., Lykou G.: Critical infrastructure protection: a holistic methodology for Greece,*Conference on security of industrial control and cyber physical systems (CyberICPS)*, Springer, 2016, pp.22–34

[292] Rossella M., Cédric L-B.: *Methodologies for the identification of critical information infrastructure assets and services. Guidelines for charting electronic data communication networks*, European union agency for network and information security. ENISA, Heraklion, 2014, pp.15-16, 21

identifikovani nacionalni kritični sektori - podsektori (postupak zasnovan na javno-privatnom partnerstvu), sastavlja se lista zainteresovanih strana-operatora kritične infrastrukture, poznatih i kao vitalni operatori, od kojih se zahtijeva da identifikuju i procijene kritične usluge i najkritičnija sredstva (sisteme) koje sadrže. U nekim od evropskih zemalja ova odgovornost je dodijeljena odgovarajućem vitalnom operatoru od strane tijela nadležnog za relevantni kritični sektor (uglavnom nadležno ministarstvo). U primjeni ovog pristupa vitalni operator izlazi u prvi plan, za razliku od koncepta kritične službe, dominantnog u pristupu koji vodi država. Na neki način, vitalni operator je istovremeno i sama najvažnija imovina kojoj je potrebna zaštita[293] Ovaj pristup je korišćen u Francuskoj i Velikoj Britanija. Svaki od ovih pristupa zahtijeva primjenu metoda za procjenu i određivanje prioriteta kritičnosti svakog sredstva (usluga, roba, sistema i slično) kritičnog sektora. Ovaj proces, uprkos svojoj važnosti, nije uvijek očigledan, pogotovu jer se kriterijumi za kritičnost uključenih podataka razlikuju od države do države. S druge strane, infrastruktura može biti kritična i zbog međuzavisnosti između usluge koju data infrastruktura podržava i drugih usluga unutar istog ili različitog sektora.

Treba napomeniti i da usluga ili podsektor mogu biti kritični ne samo zbog neposrednog uticaja koji može nastati zbog njihovog neispravnog rada ili gubitka (tzv. efekat prvog reda), već i zbog uticaja na druge kritične usluge ili podsektore (efekti drugog reda). U tom kontekstu, efekti prvog reda odražavaju direktnu vitalnost kritičnog dobra za društvo[294], dok se efekti drugog reda posmatraju kao zavisnost u kojoj kritični element zavisi od drugog elementa, ili kao međuzavisnost gdje su dva kritična elementa uzajamno pogođena na nacionalnom ili čak međudržavnom nivou[295]. Iz navedenog se može zaključiti da zavisnosti ili međuzavisnosti mogu postojati kako u sektoru (podsektoru) u kojem se usluga obezjbeđuje, tako i između dva ili više sektora (podsektora) na nacionalnom nivou, pa i između dva sektora (podsektora) koji egzistiraju u različitim državama.

U literaturi se mogu pronaći dvije grupe kriterijuma koji se koristite za procjenu kritičnosti (a zatim i prioriteta) potencijalne kritične usluge ili infrastrukture. Prvu grupu čine sektorski kriterijumi koji obuhvataju tehničke ili funkcionalne kriterijume pomoću kojih se mogu identifikovati i prioritetno odrediti potencijalna kritična infrastruktura. Na primjer, sektorski kriterijumi se mogu odnositi na (obično kvantitativno izražena) specifična svojstva ili karakteristike infrastrukture koja podržava sektorsku uslugu. Predmetne karakteristike mogu biti tehničke prirode (npr. minimalni prečnik naftovoda ili gasovoda, minimalni kapacitet električne snage u megavatima i slično.), a koje variraju u zavisnosti od sektora. Na primjer, u slučaju informacionog indeksa informacija, sektorski kriterijumi su između ostalog: brzina tranzita podataka, vrijeme oporavka informacionog sistema, broj evidencija ličnih podataka koji se održavaju ili obrađuju od strane sistema i slično. Unakrsni kriterijumi procjenjuju težinu uticaja koji mogu nastati zbog kvara, poremećaja ili uništenja potencijalne kritične infrastrukture. Predmetno određenje odražava uticaj neočekivanog incidenta na nacionalnom nivou koji utiče na tu infrastrukturu u najgorem scenariju u kritičnoj službi (sektoru-

[293] Klaver M.:*Good practices manual for CIP policies, for policy makers in Europe*, Brussels, 2011, dostupno na: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/FINAL_RECIPE_manual.pdf

[294] Luiijf E., Burger H., Klaver M., Marieke H.:*Critical infrastructure protection in the Netherlands: a Quick-scan*, EICAR Denmark, Copenhagen, 2003, p. 9

[295] Rossella M, Cédric L-B: *Methodologies for the identification of critical information infrastructure assets and services. Guidelines for charting electronic data communication networks, European union agency for network and information security*, ENISA, Heraklion, 2014, pp. 25, 27

podsektoru ili na međusektorskom nivou), a koji se manifestuje preko pogođene infrastrukture[296]. Kada je riječ o kriterijumu kritičnosti isti se određuju na osnovu:

- *obima geografskog područja*, u kome se infrastruktura definiše za najmanji obim geografskog područja na koji bi mogao uticati incident u funkcionisanju infrastrukture,
- *potencijalnih žrtava,* gdje je kriterijum minimalan broj žrtava i (ili) povreda koje može izazvati incident koji utiče na infrastrukturu,
- *ekonomskih efekata*, pri čemu je kriterijum makroekonomski uticaj (npr. gubitak bruto nacionalnog proizvoda, gubici zbog zavisnosti, gubitak zemljišta, troškovi preseljenja stanovništva i troškovi eventualnog zagađenja) i (ili) makrosocijalni uticaj, uključujući potencijalne uticaje na životnu sredinu.
- *javnih efekata*, gdje se ocjenjuje kako (potencijalni) uticaj na infrastrukturu može uticati na veliki dio ljudi koji koriste kritične usluge[297].

S obzirom na činjenicu da je zaštita kritične infrastrukture stalan proces koji se mora redovno analizirati u cilju nadogradnje postojećeg sistema i iznalaženja novih rešenja, a to je veoma otežano zbog glomaznosti i složenosti svakog pojedinog sektora kritične infrastrukture, kao i njihove povezanosti, mnoge države su odabrale strategijski pristup ovom problemu. Strategija je važna jer pruža mapu puta za rešavanje složenih problema koji uključuju organizaciju, tehnologiju i raspodjelu resursa u izazovnom okruženju[298].

Analizom brojnih nacionalnih strategija zaštite, pored uočljive različitosti, možemo naći i pojedina ključna područja koja doprinose potpunijem strategijskom pristupu zaštiti kritične infrastrukture. Najvažniji elementi strategijskog pristupa, između ostalog, uključuju:

- *viziju ili ciljeve*, odnosno formulisanje strateških ciljeva (vizija) koji su podijeljeni u pojedinačne mjerljive ciljeve,
- *bezbjednosnu administraciju kritične infrastrukture*, koja se odnosi na strukturu upravljanja, imenovanje nadležnih i ovlašćenih tijela za zaštitu kritične infrastrukture, definisanje uloga i odgovornosti po tijelima, kao i okvir za saradnju između javnog i privatnog sektora,
- *javno-privatno partnerstvo*, u kome svaki nacionalni program zaštite uključuje saradnju zainteresovanih strana, posebno putem javno-privatnog partnerstva, uključujući javna tijela i vlasnike - operatore kritične infarstrukture,
- *razmjenu informacija*, koja se odnosi na svijest o prijetnjama i ranjivostima kritične infrastrukture, obezbjeđivanje ranog upozorenja zainteresovanim stranama, te uopšteno na razmjenu informacija i odgovarajućeg znanja o rizicima i prijetnjama,
- *zakonodavni (regulatorni okvir)*, koji je posebno značajan jer je donošenje zakona važno sredstvo kojim se osigurava da javni i privatni organi reaguju u skladu sa dodijeljenim ulogama i odgovornostima, kao i u skladu sa posebnim bezbjednosnim standardima,

---

[296] Petrakos N., Kotzanikolaour P.:Methodologies and Strategies for Critical Infrastructure Protection In: Gritzalis D., Theocharidou M., StergiopoulosG. (ed): *Critical Infrastructure Security and Resilience, Theories, Methods, Tools and Technologies*, Springer, Switzerland, 2019, p. 25

[297] COUNCIL DIRECTIVE 2008/114/EC,The identification and designation of European critical infrastructures and the assessment of the need to improve their protection, art. 3, dostupno na: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[298] Lewis T. G. : *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons, Inc, Canada, 2006, pp. 4-5

- *identifikaciju i procjenu nacionalne kritične infrastrukture* (sektora, podsektora, usluga i specifičnih podsistema), što je preduslov za sprovođenje nacionalnih politika zaštite, pri čemu je važan kriterijum za razvrstavanje, obim i značaj međusobnih veza i međuzavisnosti između sektora kritične infrastrukture,
- *projcenu rizika* kao ključni element strategije zaštite kritične infrastrukture koja se zasniva na metodičkoj i metodološkoj procjeni prijetnji i procjeni rezultirajućih bezbjednosnih rizika za nacionalnu kritičnu infrastrukturu, i
- *rizike i upravljanje krizama*, što se odnosi na mjere i aktivnosti na prevazilaženju vanredne situacije u cilju osiguranja nastavka rada ili brzog oporavka kritične infrastrukture[299].

Evidentno je da su mnoge države u dosadašnjem periodu uspostavile odgovarajuće politike za zaštitu kritične infrastrukture kao i kritične informacione infrastrukture. Uočljivo je i pomjeranje težišta sa zaštite kritične infrastrukture prema otpornosti infrastrukture, premda se ova dva koncepta ne mogu lako razlikovati. Pri tom nije utvrđena ni adekvatna definicija otpornosti, mada se mogu naći neka određenja koja su primjenljiva za kritičnu infrastrukturu, kao što je „sposobnost sistema, zajednice ili društva izloženih opasnostima da se pravovremeno odupru, apsorbuju, prilagode i povrate od posledica opasnosti na efikasan način, uključujući očuvanje i obnavljanje njegovih osnovnih struktura i funkcija ”[300]

S druge strane, „slika“ nacionalnih politika u ovoj oblasti je veoma fragmentirana. Štaviše, nacionalne vlade i međunarodne institucije su prepoznale da je za upravljanje složenošću problema potrebno razvijati nove metodologije, paradigme i alate. U tu svrhu je pokrenuto nekoliko naučnih programa i uspostavljene su neke nove institucije u cilju zaštite i jačanja kritične infrastrukture[301].

Ove inicijative uključuju, između ostalog, Nacionalni centar za simulaciju i analizu infrastrukture SAD-a (*National Infrastructure Simulation and Analysis Center - NISAC*), Evropsku referentnu mrežu za zaštitu kritične infrastrukture (*European Reference Network for Critical Infrastructure Protection-ERNCIP*), Program za modeliranje i analizu kritične infrastrukture u Australiji (*Critical Infrastructure Program for Modeling and Analysis-CIPMA*), Nacionalni program osiguranja kritične infrastrukture (*National Critical Infrastructure Assurance Program -NCIAP*) u Kanadi, Holandski pristup zaštiti kritične infrastrukture, Program otpornosti kritične infrastrukture u Velikoj Britaniji i Plan implementacija zaštite kritične infrastrukture u Njemačkoj. Ove inicijative omogućavaju napredak u razumijevanju postojećih problema kao i iznalaženju mogućih rešenja. Prisustvo takvih programa istraživanja i razvoja je dovelo do novih metodoloških postupaka i do razvoja tehnoloških instrumenata za upravljanje složenošću u domenu kritične infrastrukture, a što omogućava pružanje određenih operativnih alata zainteresovanim stranama, donosiocima odluka i kreatorima politike[302].

---

[299] Petrakos N., Kotzanikolaour P.: Methodologies and Strategies for Critical Infrastructure Protection In: Gritzalis D., Theocharidou M., Stergiopoulos G. (ed): *Critical Infrastructure Security and Resilience, Theories, Methods, Tools and Technologies*, Springer, Switzerland, 2019, pp. 31-32

[300] Terminology on Disaster Risk Reduction, United Nations International Strategy forDisaster Reduction (UNISDR), Geneva, Switzerland, 2009, p. 24, dostupno na: https://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf

[301] Ouyang M.: Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering & System Safety*, Volume 121, 2014, pp. 44-48

[302] Setola R., Luiijf E., Theocharidou M.: Critical Infrastructures, Protection and Resilience In: Setola R., Rosato V., Kyriakides E., Rome E. (ed): *Managing the Complexity of Critical Infrastructures, A Modelling and Simulation Approach*, Springer, Switzerland, 2016, p.7

U ovom kontekstu treba posmatrati i mogućnost uspostavljanja efikasnog odnosa uključenih subjekata na planu zaštite kritične infrastrukture, kako same države, tako i javnih i privatnih aktera, u kome su jasno definisani ciljevi i obaveze, te uspostavljene šeme podsticaja i mehanizmi sankcija u slučaju da neke od uključenih strana odstupaju od sporazuma, odnosno ugovora. Privatizacija usluga u ovoj oblasti je realnost koju nijedan razuman posmatrač ne može poreći. Naime, privatizovati znači transformirati jednom isporučenu i izvršenu javnu uslugu koju će preuzeti privatno tijelo. To se, uz ostalo, može odnositi na prikupljanje smeća, funkcionisanje službe hitne pomoći, bezbjednost u postrojenjima, vojnim bazama, fakultetima i univerzitetima, kulturnim institucijama i slično. U prošlosti su gotovo sve ove usluge obavljali službenici zaposleni u javnom sektoru. Međutim, došlo se do spoznaje da su privatizovane usluge ekonomski povoljnije za nacionalni ili lokalni nivo, pri čemu je opšti trend da javni sektor želi da smanji troškove. S druge strane, ove usluge nisu kontrolisane pravilima sindikata i državne službe, a mogu se prilagoditi i fleksibilno isporučivati bez kršenja propisa koji je utvrdila država. Pored toga, javni sektor bezbjednosti je vezan mnogim internim pravilima rada i ograničenjima, koja utiču da njihove usluge u ovoj oblasti i ne mogu biti uvijek efikasno i produktivno pružane[303].

4.2. Uloga privatnog sektora bezbjednosti u zaštiti kritične infrastrukture

O konceptu privatizacije državnih usluga raspravlja se već nekoliko decenija. Privatizacija u najširem značenju predstvalja prenošenje državnih funkcija koje su u potpunosti ili djelimično povezane, privatnom sektoru. Zagovornici koncepta privatizacije u bezbjednosnom sektoru napominju da budžeti policije širom svijeta rastu oko 3% godišnje, ali da se potrebe za njihovim uslugama povećavaju mnogo brže. Kao odgovor, policijske službe se okreću procesu privatizacije. Neke od metoda koje se u tom procesu koriste su međuvladine organizacije (npr. Odjeljenje šerifa okruga Los Angeles sklopilo je ugovore pružanja usluga policije u drugim državnim nadležnostima). Neki od primjera su i korišćenje volontera za izvršenje manje značajnih obaveza, kao i outsourcing administrativnih, pomoćnih i drugih dužnosti u cilju oslobađanja policije od pojedinih zadataka i usmjeravanje na primarnu misiju zaštite života i imovine. Nalazi nekih istraživanja pokazuju da outsourcing pojedinih policijskih aktivnosti kao što su usmjeravanje saobraćaja, reagovanje na antiprovalne alarme, slanje policijskih vozila, prevoz i nadgledanje zatvorenika, regulisanje parkinga na pojedinim lokacijama, nadgledanje pojedinih objekata kao i obavljanje drugih poslova izvan policijskih prioriteta, mogu smanjiti troškove do 30 %.[304]

Neke od uočenih prednosti u saradnji javnog i privatnog sektora u ovoj oblasti su vezane i za razmjenu informacija o bezbjednosnoj problematici, unapređenje prevencije kriminala i javne bezbjednosti, upotrebu različitih tehnika u sprečavanju kriminala koje se odnose na dizajn životnog okruženja, rad u zajednici i upotrebu savremene tehnologije, saradnju na određenim projektima kao što su visokotehnološki kriminal i slično. Suština navedenog partnerstva je u upotrebi resursa i njihovom međusobnom dopunjavanju (umnožavanju) kao i njihovoj racionalnoj upotrebi (dijeljenju) u dostizanju zajedničkih ciljeva. Javni sektor sa svojim resursima, a u skladu sa zakonskim odredbama ima mogućnost da pomogne zaposlenima u privatnom obezbjeđenju da ostvare određene

[303] Nemeth P. C.: *Private Security An Introduction to Principles and Practice*, Boca Raton, 2017, pp. 680-681
[304] Dempsey S. J.:*Introduction to Private Security*, Second Edition, Wadsworth, Cengage Learning, 2011. p. 358

ciljeve. S druge strane, privatni sektor je u mogućnosti da efikasnije pomogne policiji da smanji broj krivičnih djela na štetu objekata kritične infrastrukture. Pored toga ne treba zaboraviti ni pojavu novih krivičnih djela kao što je sajber kriminal, pri čemu se samo zajedničkim naporima javnog i privatnog sektora može doprinijeti njihovom efikasnom sprečavanju i suzbijanju.

Ideja o kritičnoj infrastrukturi i njenoj zaštiti ne može biti odvojena od učešća javnog i privatnog sektora, jer u savremenom svijetu značajan dio te infrastrukture štite privatne kompanije, pri čemu su se pojedine specijalizovale za ovu oblast[305]. To je ujedno posledica činjenice da su vladine službe brojnih zemalja procijenile da nijesu u mogućnosti da same štite nacionalnu kritičnu infrastrukturu, pa su pristupile podsticanju partnerstva s privatnim sektorom na gotovo svim nivoima i u svim kategorijama kritične infrastrukture[306]. Navedeno ukazuje da bezbjednost kritične infrastrukture na nivou države zahtijeva efikasan i inovativan partnerski okvir između javnog i privatnog sektora.

4.2.1. Funkcije privatnog sektora bezbjednosti

Pored različite uloge koju ostvaruje u svakom konkretnom slučaju, generalno uzev funkcije privatnog sektora bezbjednosti u zaštiti kritične infrastrukture obuhvataju: administrativnu bezbjednost, fizičku i tehničku bezbjednost postrojenja i objekata, bezbjednost od požara, postupanje u vanrednim situacijama, informacionu bezbjednost, podizanje nivoa bezbjednosne svijesti i programe obuke[307].

4.2.1.1. Administrativna bezbjednost

Jedna od funkcija privatnog sektora bezbjednosti bez obzira o kakvoj se prirodi kritične infrastrukture radi, jeste administrativna bezbjednost. Da bi privatni sektor bezbjednosti i zaposleni u objektima kritične infrastrukture uspješno obavljali svoje dužnosti i ispunili svoje odgovornosti, moraju postojati odgovarajuće smjernice i uputstva. U takvim okolnostima logično je uspostaviti potrebne pisane politike, postupke i formalne procese. Ako bi se drugačije postupilo, zaposleni bi štitili imovinu u obimu koji smatraju odgovarajućim, ili je uopšte ne bi štitili, a akteri privatnog sektora bezbjednosti bi mogli obavljati svoje dužnosti na način koji drže prikladnim. U tom kontekstu, očigledno je da planovi, politike, procedure i procesi dovode do reda i usklađenog djelovanja u neizvjesnom okruženju. Naime, svi planovi, politike, procedure i procesi dokumentovani su na papiru i čine ono što se naziva administrativnom bezbjednošću. Postoje različiti načini gledanja na planove, politike i postupke koji se realizuju, ali je zajedničko da postoji uzajamni odnos i podrška između istih u cilju njihove usklađenosti. Zbog toga je između ostalog značajan i njihov redosled – planovi, politike i postupci[308]. Treba napomenuti i da se planovi bezbjednosti i zaštite ne razvijaju odvojeno

[305]Videti:, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, U.S. Government Accountability Office, 2015, dostupno na: http://www.gao.gov/assets/680/673779.pdf

[306] Busch E. N., Givens D. A.: Public-Private Partnerships in Homeland Security: Opportunities and Challenges, *Homeland Security Affairs*, Vol.8, Article 18, 2012, pp.3-4, dostupno na: https://www.hsaj.org/articles/233

[307] Trivan D., Radović V.: Corporate security role in protecting critical infrastructure, In: Keković Z., at all (ed.): *National critical infrastructure protection, regional perspective*,Faculty of Security Studies, Belgrade, 2013, p. 245

[308] Kovacich G.L., Halibozek E. R.: *The manager's handbook for corporate security: establishing and managing a successful assets protection program*, Elsevier Science,USA, 2003, r. 163

od planova kritične infrastrukture, već ih moraju podržavati nakon čega dolazi do preduzimanja određenih radnji i mjera na zaštiti štićene vrijednosti. To dovodi do politike koja između ostalog postavlja opšti smjer za bezbjednost i zaštitu. Na osnovu ukupnih politika, razvijaju se procedure na određenom nivou kako bi se pružile smjernice, između ostalog, i o tome kako zaposleni da se pridržavaju definisane politike. Na taj način dokumentovani postupak dovodi do razvoja procesa koji će dati još više detalja o tome kako da se politike i procedure ispoštuju. Zato postoji sinergija od vrha prema dolje i odozdo nagore koja osigurava potpunu integraciju svih aspekata programa bezbjednosti u zaštiti kritične infrastrukture.

Sa aspekta bezbjednosti, navedeni planovi su posebno značajni jer je potrebno razumijevanje vizije i misije štićenog objekta kritične infrastrukture. Ukoliko se to postigne obezbjeđuje se da sektor bezbjednosti postane značajan resurs koji podržava napredak štićene organizacije. U suprotnom bezbjednosni sektor biće isključivo fokusiran na bezbjednost kao cilj sam po sebi, ne razumijevajući kako ona služi širim ciljevima štićenog objekta[309].

Privatni sektor bezbjednosti zadužen je za dokumentovanje zaštite kritične infrastrukture u planovima, politikama, procedurama i postupcima neophodnim da bi se pružile smjernice svim zaposlenima u pogledu njihove odgovornosti za zaštitu objekata, imovine i drugih vrijednosti. Pored toga, privatno obezbjeđenje bavi se i načinom kako različitu imovinu treba zaštititi. Najbolji način za ostvarivanje funkcije administrativne bezbjednosti je upotreba pristupa odozdo nagore, jer bezbjednosni upravljački programi dolaze s vrha. S druge strane, subjekt koji je odgovoran za bezbjednost i zaštitu imovine u objektima kritične infrastrukture daje potrebne smjernice o tome kako zaštititi različitu imovinu na osnovu procjena o tome koji djelovi te imovine imaju poseban značaj sa aspekta dodatnih mjera zaštite.[310]

4.2.1.2. Fizička i tehnička bezbjednost

Fizička bezbjednost, odnosno upotreba fizičke kontrole radi zaštite prostorija, lokacije, objekta, zgrade ili druge fizičke imovine, predstavlja najvažniji aspekt zaštite kritične infrastrukture. Primjena fizičke bezbjednosti, čiji je najvažniji dio postupak upotrebe fizičkih zaštitnih mjera za sprečavanje neovlašćenog pristupa i oštećenja, otuđenja ili uništavanja imovine, od suštinskog je značaja za profil zaštite objekata i resursa te infrastrukture. U suštini, mjere fizičke zaštite štite imovinu, postrojenje, objekat, zgradu ili bilo koji njen sadržaj od gubitka ili štete. Mjere fizičke bezbjednosti takođe doprinose zaštiti ljudi i informacija. Uopšteno posmatrano, za zaštitu informacija i informacionih sistema koriste se sofisticirane mjere zaštite koje nijesu fizičke kontrole. Međutim, mjere fizičke bezbjednosti dio su ukupnog zaštitnog paketa. One su osnovne bezbjednosne mjere na kojima se zasnivaju sve ostale mjere bezbjednosti. Mjere fizičke bezbjednosti pomažu osiguranju da samo ovlašćene osobe imaju pristup objektima i imovini koja se štiti. Primijenjene mjere moraju biti

[309] Smith F. C., Schmalleger F.,Siegel J. L.: *Private Security Today,* Pearson Education, 2017, r. 43
[310] Kovacich G.L., Halibozek E. R.: *The manager's handbook for corporate security: establishing and managing a successful assets protection program*, Elsevier Science, USA, 2003, p. 182

odgovarajuće za svako posebno radno okruženje[311]. Zbog svega navedenog fizička bezbjednost se često opisuje i kao „prva linija odbrane od potencijalne prijetnje“.[312]

U literaturi se podjela fizičke bezbjednosti najčešće vrši na njena dva glavna dijela - spoljašnju i unutrašnju bezbjednost, prvenstveno zbog nedostatka boljeg načina opisivanja spoljašnjeg, fizičkog svijeta. Istorijski posmatrano, fizička bezbjednost definisana je kao sistem prepreka, kontrole ulaska i pretrage, otkrivanja upada, procjene alarma, te njihovog testiranja i održavanja. Ukupno uzev, ovaj sistem sa praksama i procedurama specifičnim za svaku lokaciju, predviđen je za odvraćanje, otkrivanje, procjenu i odgovarajuće reagovanje na neovlašćene aktivnosti[313]. Efikasan plan fizičke bezbjednosti započinje globalnom analizom lokacije koja se štiti i nastavlja sve do mikronivoa pojedinih objekata i instalacija i donošenja odluka gdje i kako odrediti potrebne aktivnosti kako bi se osiguralo bezbjedno okruženje.

Međutim, za efikasnu fizičku zaštitu potrebna je i procjena fizičke bezbjednosti koja umnogome zavisi od svrhe samog objekta. Naime, pojedini objekti kao što su bolnice, podzemne željeznice, javni željeznički centri, sistemi javnog prevoza i slično, imaju posebne zahtjeve koji se tiču bezbjednosti. S druge strane, fizička bezbjednost se mora uklopiti sa životom zajednice i objektom koji se štiti, stvarajući istovremeno osjećaj bezbjednosti i povjerenje u subjekte zadužene za bezbjednost štićene vrijednosti. Na tom planu, perimetarska zaštita je prva linija odbrane u pružanju fizičke bezbjednosti objekta. Perimetar je spoljna zona, dovoljno udaljena da omogući vrijeme reakcije od strane službenika obezbjeđenja koji su zaduženi za stvaranje sigurnog okruženja. To se najčešće postiže postavljanjem ograde ili drugih fizičkih barijera, prirodnih dobara pretvorenih u odbrambene svrhe, rasveta, kapija koje se mogu zaključati, detektora provale ili zaštitne snage. Perimetri se takođe mogu podijeliti na različite sektore, ili djelovi objekta koji treba da se obezbijede, a mogu obuhvatati određene zidove, vrata i prozore, i protivpožarne sektore. Pored toga što kontroliše pristup objektu, perimetrska barijera stvara fizičko i psihičko odvraćanje od namjere za neovlašćeni ulazak, pomaže u otkrivanju i neutralisanju, hapšenju i kontroli protoka lica. Obim obodnih kontrola u velikoj mjeri određuje sam objekat, a sredstva i metode zaštite perimetra su prilično raznolike, pri čemu je privatni sektor bezbjednosti lider u razvoju efikasne linije proizvoda za zaštitu obodne linije[314].

Kada se osigura obodna zona, pažnja se usmjerava na bezbjednost i integritet konkretnog objekta ili druge građevine. Ovi objekti mogu ali ne moraju imati sva sredstva fizičke bezbjednosti, već mogu imati samo pojedine od njih. To u značajnoj mjeri zavisi od dizajna i arhitektonskih karakteristika objekta, jer će, na primjer, zgrada sa malo prozora i pristupnih tačaka zahtijevati manje mjere bezbjednosti od otvorenije i znatno preglednije.

Strategija kontrole pristupa zavisi od mnoštva faktora, uključujući vlasničke interese, osjetljivost informacija ili proizvoda, specifične opasnosti koje su povezane sa proizvodnjom ili kretanjem proizvoda, kao i druga pitanja. Potreban stepen bezbjednosti unutrašnjosti u velikoj mjeri

---

[311] Halibozek E., Jones A., Kovacich L. G.: *The corporate security professional's handbook on terrorism*, ElsevierIn, 2008, pp. 84-85

[312] Ortmeier J. P.:*Introduction to Security, 3rd ed*., Prentice Hall, 2009, p. 94

[313] Nemeth P. C.: *Private Security, An Introduction to Principles and Practice*, CRC Press, Taylor & Francis Group, 2018, p. 232

[314] Khairallah M.: Identifying Control Perimeters, *Security Magazin*, 2007, dostupno na: https://www.securitymagazine.com/articles/78267-identifying-control-perimeters-1

zavisi od funkcionalnosti i svrhe objekta, pri čemu bezbjednosne potrebe diktiraju bezbjednosni zahtjevi. Politika koja se odnosi na pristup bilo kojoj zgradi ili objektu počinje na njenom obodu. Kapije i rampe, bilo sa ili bez izvršioca, imaju funkciju kontrole protoka saobraćaja i sprečavaju nesmetani pristup onima koji namjeravaju da čine štetu ili ugroze objekat i lica. Zbog toga su često neke od tehnologije pristupa već ugrađene u spoljni obod koji kontroliše pristup. Nakon ulaska u unutrašnjost zgrade ili objekta, mogu se ponovo primijeniti isti protokoli. Imajući u vidu iznijeto, politika pristupa je istovremeno i tradicionalna i tehnološki inovativna zaštita objekata kritične infrastrukture[315].

Postoji mnoštvo metoda za pružanje fizičke bezbjednosti na kontrolno-pristupnim tačkama, uključujući i upotrebu elektronskih brava, mehanizama za zaključavanje sa karticama i slično, ali se od svih alternativnih načina pouzdane identifikacije za kontrolu pristupa, biometrija (podaci koji sadrže osnovne tačke na licu ili dlanu, otisak prstiju, obrazac glasa i mrežnjače oka) čini najpouzdanijom i najsigurnijom.[316]

Drugi ključni oblik kontrole pristupa i opšte bezbjednosne provjere za zaposlene i posjetioce, odnosno za sprečavanje ulaska uljeza u unutrašnjost štićene zgrade ili objekta jeste video nadzor. Kao i kod drugih oblika kontrole pristupa i identifikacije, nadzor obično počinje izvan unutrašnjosti na obodu. Treba napomenuti da su oprema za osvetljenje i nadzor po pravilu povezani sa barijerama, čineći zajedno jedinstvenu cjelinu koja sprečava ulazak neželjenih lica. Međutim, proces vizuelnog identifikovanja neovlašćenih ulazaka, a takođe i praćenja svakodnevnih aktivnosti, neprimjerenog, kriminalnog ili drugog neprihvatljivog ponašanja ne može biti u potpunosti moguća bez efikasnog nadzora. U tom smislu, nadzor je sastavna komponenta bezbjednosti bilo kog mjesta, ali njegov predmet, odnosno osobe koja se nadgledaju i aktivnosti pod nadzorom, su nepoznati subjekti. Upotreba nadzora treba da bude spoj agresivnog i opreznog, agresivnog u smislu da je to jedno od najznačajnijih oruđa u paleti alata za bezbjednost, istovremeno uvažavajući implikacije njegove upotrebe na privatnost pojedinca.

4.2.1.3. Informaciona bezbjednost

Informacione i računarske tehnologije se upotrebljavaju za snimanje, čuvanje, analizu i prenos podataka. Informacije koje se bilježe, čuvaju, analiziraju i prenose u okviru ovih tehnologija smatraju se jednim od najvažnijih i najvrednijih bogatstava organizacija javnog i privatnog sektora, a samim tim i objekata kritične infrastrukture. Organizacije javnog sektora (npr. vladine agencije) nastoje da zaštite informacije koje mogu ugroziti nacionalnu bezbjednost i nacionalnu ekonomsku bezbjednost ako dođu u posjed pojedinaca koji nemaju odobren pristup i imaju kriminalne, terorističke i druge nezakonite namjere. Pored toga, i privatni sektor štiti poslovne tajne, jer ove informacije mogu naštetiti privrednim subjektima ako se otkriju trećoj strani (npr. pojedincu, konkurenciji ili stranoj vladi) bez odobrenja. Neovlašteno otkrivanje poslovne tajne može takođe štetiti nacionalnoj

[315] Meyer C.: Compounding Technologies for More Accurate Intruder Detection, *Security Magazin*, February 2015, p. 45, dostupno na: http://digital.bnpmedia.com/publication/?i=244485&article_id=1920048&view=articleBrowser&ver=html5#{%22issue_id%22:244485,%22view%22:%22articleBrowser%22,%22article_id%22:%221920048%22}

[316] Zalud B.: Transition Times for Bank and Financial Services, Security Magazin, June 2015, p. 50, dostupno na:https://www.securitymagazine.com/articles/86405-transition-times-for-bank-and-financial-services-security

ekonomskoj bezbjednosti. Javne i privatne organizacije štite povjerljive informacije (npr. finansijski podaci ili podaci o zaposlenima, klijentima i operacijama).

Bezbjednost informacija obuhvata mjere zaštite informacija od slučajnog ili namjernog neovlašćenog otkrivanja, pristupa, izmjena, brisanja, kopiranja ili druge neodobrene upotrebe. Procjene i analize rizika bezbjednosti informacija pružaju uvid u vjerovatnoću, kritičnost (uticaj) i ranjivost (izloženost) informacija potencijalnoj prijetnji[317].

Ove procjene i analize rizika uzimaju u obzir potencijalne političke, socijalne i finansijske gubitke koji mogu biti pretrpljeni u slučajevima da se informacijama neovlašćeno pristupa, da se iste modifikuju i dobijaju bez odobrenja i na druge načine zloupotrebljavaju. U vezi sa tim, bezbjednost informacija uključuje kombinaciju mjera fizičke bezbjednosti, bezbjednosti radnih mjesta i procesa, bezbjednosti komunikacije i računarske bezbjednosti. Angažovani subjekti sprovode mjere zaštite čiji je cilj da onemoguće kriminalcima i pretpostavljenim protivnicima pristup informacijama. Da bi se zaštitile informacije, potrebna je fizička bezbjednost objekta u kome se podaci čuvaju i bezbjednost sistema koji te podatke čuvaju. Mjere fizičke bezbjednosti treba da uključuju sisteme kontrole pristupa, alarmne sisteme, sisteme nadzora koji omogućavaju nadležnom licu i osoblju obezbjeđenja da kontroliše pojedinačni pristup računarskim sistemima, serverima i oblastima u kojima se nalaze[318].

Pored toga, neophodne su efikasne mjere provjere autentičnosti, u cilju sprečavanja pristupa oblastima u kojima se nalaze računarski sistemi i serveri i podaci unutar njih. Ove mjere treba da uključuju one koje dokazuju „šta znate“ (lozinke), „šta imate“ (token i značke) i „ono što jeste“ (biometrijske podatke). Za efikasno fizičko obezbjeđenje potreban je multifaktor autentičnosti, što uključuje kombinaciju mjera projektovanih da dokažu „šta znate“, „šta vi imate“i „ono što jeste “[319].

Često se zanemaruje činjenica da je suštinski element informacione bezbjednosti operativna bezbjednost, kojom se identifikuju, kontrolišu i štite informacije organizacije kako bi se uskratio pristup konkurentima, kriminalcima i potencijalnim protivnicima (u daljem tekstu počiniocima). Da bi se utvrdilo koji potencijalni počinioci i koje informacije mogu tražiti i dobiti pristup, vrši se procjena rizika. Kod operativne bezbjednosti to se vrši iz perspektive počinioca u cilju identifikacije ranjivosti. Ovaj proces pomaže u predviđanju unutrašnje oblasti zaštite i prakse organizacije iz ugla počiniloca, koju može iskoristiti u svoju korist. Zato moraju postojati politike i procedure kojima se osigurava zaštita informacija od onih koji ne bi trebali imati pristup njima. O tim postupcima se obučava i osoblje, jer je sam proces operativne bezbjednosti osmišljen da pomogne organizacijama u primjeni kontramjera potrebnih da se počiniocima onemogući pristup informacijama[320].

Bezbjednošću komunikacija nastoji se uskratiti otkrivanje informacija konkurentima, kriminalcima i protivnicima koji potiču iz telekomunikacija i da osigura autentičnost komunikacija. Bezbjednost prenosa i bezbjednost emisije dio su napora bezbjednosti komunikacija. Bezjednost prenosa ima za cilj da zaštiti prenose od presretanja ili interferencije, dok bezbjednost emisije sprečava protivnika da koristi kompromitujuće emanacije za dobijanje informacija. Šifrovanje, koje

[317] Johnson B.R., Ortmeier P. J.: *Introduction to security : operations and management*, Pearson, 2018, p. 119
[318] Nemeth P. C: *Private Security An Introduction to Principles and Practice*, Taylor & Francis Group, 2018, p. 664
[319] Lehtinen R., Russell D., Gangemi Sr G.T.: *Computer Security Basics*, 2nd Edition, O'Reilly Media, California, 2006, p. 51
[320] Williams J: Physical Security: Thret after september 11, 2001, In:Tripton F. H., Krause M.: *Information Security Management Handbook*, Taylor &Francis Group, 2007, pp. 1379-1382

fizički blokira pristup komunikacijama treće strane, može se upotrebiti za zaštitu komunikacija i dio je mjera računarske bezbjednosti[321]

Računarska bezbjednost nastoji da zaštiti sisteme od ranjivosti (nešifrovani, pogrešno konfigurisani sistemi i uređaji), prijetnji (potencijalni neovlašćeni pristup sistemima) i napadima (krađa identiteta). Bezbjednost mreže i bezbjednost podataka dio su računarske bezbjednosti koja uključuje proaktivne mjere projektovane za suočavanje sa raznim prijetnjama i napadima i sprečava ih da pristupe, šire, modifikuju, oštete ili na bilo koji drugi način negativno utiču na mrežu. U svom najosnovnijem značenju, mrežna bezbjednost uključuje politike, procedure i prakse koje obezbjeđuju validnost, pouzdanost i upotrebljivost mreže i zaštitu mreže. Svrha mrežne bezbjednosti je da obezbijedi sigurne veze između pošiljalaca i primalaca i da obezbijedi integritet (podaci su ono što namjeravaju da budu i nisu modifikovani ili na drugi način izmijenjeni), povjerljivost (zaštita privatnih, ličnih i osjetljivih podataka) i dostupnost poslatih podataka preko mreže[322].

Mjere bezbjednosti moraju se stalno prilagođavati brzom rastu i razvoju informacionih i računarskih tehnologija. Ove tehnologije omogućavaju snimanje, čuvanje, upotrebu i prenos podataka. Kao takve, organizacije moraju da razviju i primijene mjere bezbjednosti koje mogu zaštititi informacije koje sadrže, koriste i dijele sa ovih uređaja. Bezbjednost informacija uključuje fizičko obezbjeđenje, bezbjednost rada i bezbjednost komunikacija. Mjere bezbjednosti informacija moraju zaštititi računarske sisteme od unutrašnjih (zaposlenih, izvođača radova i dobavljača) i od spoljnih prijetnji (sajber kriminala i drugih oblika nezakonite aktivnosti). Za adekvatnu zaštitu sistema, mreža i podataka potreban je višestruki sloj odbrane koji može da izoluje i zaštiti sredstva organizacije, podatke u sistemima i mrežnim pristupnim tačkama, internet i spoljne prijetnje. Zato je potrebna strategija reagovanja na nezgode kako bi se osiguralo da pripadnici obezbjeđenja i zaposleni u objektima kritične infrastrukture znaju kako da odgovore na incidente u informacionoj sferi.

4.2.1.4. Zaštita od požara

Brojni slučajevi uništenja i oštećenja imovine, povrede i smrtni slučajevi, koji se događaju i u objektima kritične infrastrukture, standardni su rizici povezani sa požarima. Privatne bezbjednosne kompanije sve više preuzimaju vodeću ulogu u zaštiti od požara u poslovanju i institucionalnim operacijama. To je sasvim razumljivo s obzirom da privatna bezbjednosna industrija nastavlja svoju vodeću ulogu u korišćenju tehnologija za potrebe bezbjednosti, a s druge strane iste te firme razvijaju i primjenjuju tehnologiju za protivpožarnu bezbjednost širom svijeta. Međutim, sama tehnologija nije dovoljna za efikasnu zaštitu od požara, posebno kada se uzme u obzir rastuće regulatorno okruženje, kao i nacionalni standardi u oblasti sprečavanja požara. U nastalim okolnosti cjelokupna problematika gašenja požara je u potpunosti regulisana od strane države, i preostaje samo dosledno sprovođenje zakonske regulative. S druge strane, cjelokupna strategija pripadnika sektora bezbjednosti u zaštiti kritične infrastrukture ne mora se primenjivati samo na prijetnje i ugrožavanja vezana za ljudski faktor, jer su u mnogim slučajevima velike štete i gubici bili izazvani neizazvanom vatrom i vremenskim neprilikama[323].

[321] Johnson B.R., Ortmeier P. J.: *Introduction to security : operations and management*, Pearson, 2018, p. 132
[322] Nemeth P. C: *Private Security An Introduction to Principles and Practice*, Taylor & Francis Group, 2018, p. 666-667
[323] Carter Smith F.S., Schmalleger F., Siegel J. L.: *Private Security Today*, Pearson Education, Inc, 2017, p. 127

Uzroci požara i njima izazvanih žrtava, povreda i ekonomskih gubitaka su prilično raznoliki, iako potpuno proučavanje podataka pokazuje da manji incidenti, koje se mogu sprečiti, obično izazovu požare sa težim posledicama od drugih događaja. Primjera radi, mnogo je manja vjerovatnoća da će gromovi i vatrene kugle biti uzročnici požara u odnosu na grejno tijelo ostavljeno u prostoriji bez nadzora.

Privatni sektor bezbjednosti u zaštiti kritične infrastrukture koordinira protivpožarnu bezbjednost i njene zahtjevne protokole u ukupnom planu bezbjednosti za određene objekate i ujedno edukuje zaposlene o mjerama bezbjednosti i putevima evakuacije.

Bezbjednost od požara je značajna za svako radno mjesto, iz čega proizilazi potreba obučavanja svih zaposlenih u objektima kritične infrastrukture o opasnostima od požara na radnom mjestu i o postupcima i procedurama u slučaju požara. U vezi sa tim, od značaja je plan organizacije za zaštitu od požara koji između ostalog sadrži zadatke ključnog osoblja u slučaju požara i plan evakuacije zaposlenih sa prostora u blizini mjesta događaja. Kada se razmatra program zaštite od požara uputno je koristiti identifikovane kritične komponente i to:

- *aparati za gašenje požara*, što uključuje obezbjeđenje funkcionalnih prenosnih aparata za gašenje požara i potrebnu periodičnu kontrolu istih u zavisnosti od rizika okruženja,
- *obuka za gašenje požara*, koja se izvodi periodično u skladu sa procjenom obučenosti ljudstva u korišćenju aparata i gašanja požara,
- *obilježavanje prostora znakovima za izlazak i vizuelnim signalima (lampice)u slučaju opasnosti,* kojima se zaposlenima pokazuje jasan put do najbližeg izlaza u slučaju požara i evakuacije,
- *alarmni sistemi,* kao važan korak za zaštitu od požara uključuju rano otkrivanje i proces koji upozorava prije nego što situacija postane kritična. Kada se otkrije dim, toplota ili plamen, alarmni sistemi treba da obaveštavaju centralnu dispečersku stanicu ili obližnju vatrogasnu službu kako bi započele početne intervencije,
- *sistemi za prskanje*, koji mogu spasiti živote tokom požara, štite objekte 24 sata, smanjuju širenje plamena i ograničavaju štetu na imovini,
- *strategija od zaštite do prevencije* podrazumijeva da proaktivno sprečavanje požara smanjuje rizik od povreda i oštećenja objekta. Organizacija zaštite od požara treba da podstakne zaposlene da temeljno prouče sve opasne hemijske supstance, jer iste mogu biti zapaljive ili se mogu zapaliti ako se pomiješaju. To obuhvata i mašine za sprečavanje pregrijevanja, kao i sve vidljive električne ili mehaničke opasnosti koje mogu dovesti do požara[324].

Iz navedenog se može zaključiti da efikasan program zaštite od požara u objektima kritične infrastrukture, pored nabavke i održavanja opreme za sprečavanje požara, podrazumijeva i posebne postupke za zaštitu života i imovine u slučaju da dođe do požara. C druge strane, osoblje zaduženo za bezbjednost trebalo bi da poznaje detalje Plana zaštite i spašavanja i njihovo mjesto i obaveze u njemu. Menadžeri bezbjednosti bi trebali da imaju plan postupanja za zaštitu lica i imovine i da redovno sprovode kontrole pripremljenosti u slučaju požara[325].

[324] Rudy J.: Fire Protection: A Complete Approach, *Occupational Healt & Safety*, December 2012, dostupno na: http://ohsonline.com/Articles/2012/12/01/Fire-Protection-A-Complete-Approach.aspx

[325] Hess M. K.: *Introduction to Private Security, Fifth Edition*, Wadsworth, Cengage Learning, 2009, pp. 232-234

4.2.1.5. Djelovanje u kriznim situacijama

Iako je sektoru bezbjednosti primaran zadatak upravljanje rizicima, često se događa da isti prerastu u kriznu situaciju koja utiče na funkcionisanje organizacije koja pripada kritičnoj infrastrukturi. To ukazuje da nije dovoljno samo definisati široki spektar vanrednih i kriznih situacija već je neophodno planirati i razne protokole i postupke za rešavanje katastrofa, prijetnji i vanrednih situacija. Sve to je u nadležnosti i odgovornosti sektora bezbjednosti“[326]. Neadekvatni planovi za vanredne situacije i krize mogu se opisati samo kao ozbiljno kršenje dužnosti od strane stručnjaka za bezbjednost. Naime, kako se ističe, „rizik nikada ne spava, a sigurno ni oni koji su odgovorni za vanredne situacije i krizno upravljanje ne mogu da spavaju“[327].

Planiranje mora biti integrisano na svakom koraku procesa kada se radi o različitim vrstama katastrofa i opasnosti, jer ignorisanje stvarnosti i ne previđanje opasnosti od realnih prijetnji i potencijalnih katastrofa, može biti pogubno po objekte i resurse kritične infrastrukture . U vezi sa tim, bezbjednosni sektor mora da ostane u povišenom stanju pripravnosti kako bi se lakše došlo do oporavka[328].

Iako postoje različiti pristupi planiranju u kriznim situacijama i krizama, četiri faze su od presudnog značaja:

- *pripremljenost*, što podrazumijeva da su planiranje i pripreme neophodni za postupanje u vanrednim situacijama ili katastrofama. Spremnost podrazumijeva izrađene planove i procedure kojima se obezbjeđuje kontinuitet u radu. Pripremljenost identifikuje najvažnije zalihe i radnje, kritične pozicije, posebne uloge, odgovornosti, naredbe o delegiranju određenih ovlašćenja i komunikacija, te predviđa plan evakuacije i alternativnu bezbjednost za osoblje i zaposlene. U fazi pripremljenosti svi subjekti se obučavaju i pripremaju za ono što se može dogoditi[329].
- *ublažavanje*, koje obuhvata radnje i aktivnosti vezane za sprečavanje budućih vanrednih situacija ili smanjenje njihovih efekata. Kada se problem predvidi i pripremi za njega, ublažavanje se fokusira na načine smanjenja šteta ili povreda od prijetnji ili katastrofa. Suštinsko pitanje u ovoj fazi je kako se pravilnim planiranjem može umanjiti količina štete. Navedeno zavisi od konkretnog slučaja, ali uopšteno se mogu navesti primjeri održavanja električne energije upotrebom generatora i druge opreme za napajanje, sigurnog skladištenja hrane i vode, sprovođenja sajber-zaštite za osjetljive podatke i slično. Pored toga, i analiza troškova i koristi može biti efikasna da bi se procijenila izvodljivost i isplativost sprovođenja radnje koja sprečava neželjene posledice[330].

---

[326] Rendiero J.: Threat Analysis and Ratings for Overseas Security, *Security Magazin, January 2013*, dostupno na:https://www.securitymagazine.com/articles/83892-threat-analysis-and-ratings-for-overseas-security

[327] Mitchell B.: Protecting Your People, Property and Posterior: The Top 11 Errors in Emergency Planning, *Security Magazin, May 2013*, dostupno na: https://www.securitymagazine.com/articles/84368-protecting-your-people-property-and-posterior-the-top-11-errors-in-emergency-planning

[328] Pekich J.:What How to Plan for Post-Incident “Golden Minutes”, *Security Magazin, November 2013*, dostupno na:https://www.securitymagazine.com/articles/84887-how-to-plan-for-post-incident-golden-minutes

[329] Halibozek E., Jones A., Kovacich L. G.: *The Corporate Security Professional’s Handbook on Terrorism*, Elsevier Inc, 2008, p. 138

[330] Kovacich G.L., Halibozek E. R.: *The manager’s handbook for corporate security: establishing and managing a successful assets protection program*, Elsevier Science, USA, 2003, p. 304

- *odgovor,* koji podrazumijeva aktiviranje plana za vanredne situacije. Pojam odgovor u ovom slučaju sadrži različite radnje i postupke, uključujući neposredne radnje za spašavanje života, zaštitu imovine i životne sredine i ispunjavanje osnovnih ljudskih potreba. Odgovor takođe uključuje izvršenje planova za vanredne situacije i radnji za podršku kratkoročnom oporavku. Stepen reakcije zavisiće od okolnosti i uslova na određenim lokacijama. U fazi pripreme i ublažavanja, planeri su na osnovu akcionog plana za vanredne situacije obavili različite procjene rizika i ranjivosti. U okolnostima kada dođe do katastrofa i realizacije prijetnji, tim za hitne slučajeve i bezbjednost pokreće i sprovodi planirane radnje za osiguranje objekta i osoblja. Međutim, reagovanje na prirodnu katastrofu kao što je požar ili zemljotres zahtijeva drugačije vještine od reagovanja na primjer hemijskih akcidenata. Štaviše, katastrofe nastale djelovanjem čovjeka mogu dovesti do situacija koji se obično ne pojavljuju tokom prirodne katastrofe[331].
- *oporavak,* koji sadrži neophodne radnje za obnavljanje normalnog poslovanja (često se označava i kao kontinuitet poslovanja). Planovi za oporavak fokusirani su na pokretanje posla i treba da daju odgovor šta treba uraditi u prvih 30 do 60 dana kako bi se obnovili kritični procesi i nastavilo sa radom. Nakon događaja slijede medicinske intervencije, procjena štete, hitne popravke, rešavanje opasnosti koje su u toku, kao i kontakt sa izvođačima, osiguranjem i potrebnim dobavljačima[332].

S obzirom da svaku krizu, između ostalog, karakterišu složenost i neizvjesnost, postavlja se problem i efikasnog načina upravljanja krizom u cilju smanjenja posledica. Kao jedan od načina koji je našao potpunu primjenu su timovi za upravljanje krizama. Zadatak timova za upravljanje krizama, je da donose odluke za planiranje i pripremu (prije događaja) za krizu, a kada se dogodi kriza za upravljanje tom krizom kako bi se ublažila šteta i uticaj na imovinu objekta kritične infrastrukture. Timovi za upravljanje krizama po pravilu treba da budu sastavljeni od predstavnika sektora bezbjednosti, ljudskih resursa, ekološke bezbjednosti, upravljanje poslovanjem i komunikacija[333].

Pored navedenog, treba imati u vidu da će tokom krize i mediji biti zainteresovani za ovaj događaj. Primjer za to su veliki industrijski požari i krize koje su uvijek privlačile pažnju, uglavnom lokalnih i nacionalnih, a u pojedinim slučajevima i globalnih medija. Prirodne katastrofe takođe privlače veliku pažnju medija, a čak i izolovani događaji, poput incidenata sa nasiljem na radnom mjestu, mogu privući medijsku pažnju. Zato je važno imati odgovarajući plan odnosa sa medijima. S obzirom da tokom krize uvijek postoji određeni stepen nepredvidljivosti, najbolje je da svi članovi tima za upravljanje krizama razumiju kako se moraju odnositi sa medijima i moraju biti spremni na to ukoliko dođu u takvu situaciju.[334]

---

[331] Halibozek E., Jones A., Kovacich L. G.: *The Corporate Security Professional's Handbook on Terrorism*, Elsevier Inc, 2008, p. 136

[332] Johnson R. B., Ortmeier J. P. : *Introduction to security:operations and management, fifth edition*, Pearson Education, New York, 2018, pp. 271-273

[333] Halibozek E., Jones A., Kovacich L. G.: *The Corporate Security Professional's Handbook on Terrorism*, Elsevier Inc, 2008, p. 136

[334] O odnosu sa medijima i komunikacijama u toku krize videti šire u: Kešetović Ž.: *Krizni menadžment,* Fakultet bezbednosti, Beograd, 2008, str. 165-218

4.2.1.6. Program edukacije i unapređenje bezbjednosne kulture zaposlenih

Permanentna edukacija zaposlenih radi podizanja bezbjednosne kulture i svijesti je jedan od činilaca koji utiču na smanjenje prijetnji kojima je kritična infrastruktura izložena. Zato je posebno važno da se edukacija zaposlenih redovno realizuje ne samo u fazi zapošljavanja već i tokom rada. Sam proces edukacije zaposlenih mora biti u funkciji definisanih procesa i procedura koje su implementirane u objektu kritične infrastrukture. To ukazuje da se ovaj proces može ostvariti nakon uspostavljenih planova, smjernica, procedura i procesa, budući da zaposleni moraju da poznaju i primenjuju iste. Štaviše, može se pojaviti i dilema - ako bi svi poštovali važeće smjernice o zaštiti imovine, možda i ne bi bilo potrebe za fizičkim obezbjeđenjem, jer nijedna imovina nikada ne bi bila nezaštićena, a svaki zaposleni bi bio pripadnik obezbjeđenja.[335]

Pored navedenog, kod zaposlenih treba razvijati i zainteresovanost za eventualne izmjene procesa i procedura, naročito u okolnostima kada postojeća praksa ukazuje na potrebu takvih izmjena. U cilju adekvatnog reagovanja u raznim situacijama neophodno je da zaposleni budu edukovani i stimulisani, kao i da o određenim nepravilnostima i eventualnim propustima izvještavaju nadležne organe. Kada se govori o edukaciji zaposlenih, pod tim se uobičajeno podrazumijeva sticanje informacija i znanja putem nekog oblika učenja kroz iskustvo. Drugim riječima, sticanje znanja se ostvaruje kroz usmenu komunikaciju i sticanjem sopstvenih iskustava, kao i kroz prenošenje znanja zaposlenima u vezi eksplicitnih politika i procedura zaštite imovine i obaveze njihovog poštovanja. U krajnjoj liniji cilj sticanja znanja je da svi u procesu zaštite imovine vezane za kritičnu infrastrukturu imaju jasno razumijevanje kako to pravilno ostvariti. U okolnostima uočenih propusta i nepravilnosti odgovorna lica moraju naložiti provjeru odvijanja poslovnih procesa i identifikaciju istih ili sličnih ugrožavajućih situacija na drugim objektima ili prostorima kritične infrastrukture. Nakon završetka postupka provjere i utvrđivanja svih relevantnih činilaca potrebno je donijeti odluku da li je bezbjednosni događaj uzrokovan sporadičnim propustom ili uobičajenim modelom ponašanja, kao i da li je njegov uzrok subjektivni odnos pojedinca ili objektivna činjenica, koja je nastala zbog nepredvidivih okolnosti i situacija, odnosno da li su važeća pravila rada i druge bezbjednosne procedure u neskladu sa stvarnošću, te samim tim neprimenljivi.[336]

Evidentno je da će u budućnosti osoblje u objektima kritične infrastrukture morati da posjeduje veće vještine tzv. kulturne kompetencije da bi uspješno djelovali i udovoljili zadacima koji se pred kritičnu infrastrukturu postavljaju. Određene definicije kulturu posmatraju kao obrasce razmišljanja, osećanja i djelovanja koji su ukorenjeni u zajedničke vrijednosti i društvene konvencije. Kultura se takođe može vezivati za nasleđene i kolektivne pretpostavke, osnovne vrijednosti, običaje, vjerovanja, norme ponašanja i društvena očekivanja. Kulturna ili interkulturalna kompetencija u širem značenju obuhvata znanje, vještine i sposobnosti da se kulturno radi i živi u raznolikom svijetu. Interkulturalna kompetencija je takođe i organizaciona odgovornost. Zbog toga organizacije moraju cijeniti i promovisati raznolikost i inkluziju, stvarajući temeljni skup vrijednosti i principa, uz

[335] Kovacich G. L., Halibozek E. P.: *The manager's handbook for corporate security: establishing and managing a successful assets protection program*,Elsevier Science,USA, 2003, p. 247
[336] Trivan D.: *Korporativna bezbednost*, Dosije, Beograd, 2012 str.105

modelovanje prokulturnog ponašanja i stavova kako o filozofskom krajnjem cilju, tako i kao sredstvima za poboljšanje profitabilnosti poslovanja[337].

4.3. Javno-privatno partnerstvo u zaštiti kritične infrastrukture u pojedinim državama

Pojam „privatni sektor“ odnosi se na bilo koju jedinicu kojom ne upravlja državna ili savezna vlada. Ovo može da uključi privatne firme i kompanije, korporacije, privatne banke, televizijske ili radio stanice ili nevladine organizacije. Zbog primarnog cilja zarade ili stvaranja bogatstva postupci koje preduzimaja privatni sektor su usmjereni na minimiziranje bilo kojeg finansijskog rizika i maksimiziranje profita. Te organizacije mogu pokušavati da utiču na vladinu politiku kroz zakonodavni postupak, ali nemaju formalno ovlašćenje za utvrđivanje politike. Oni koji rade privatno moraju odgovarati vlastima koje su izvan vlade, poput matičnih kompanija ili poslovnih partnera, ili čak izvan finansijskih institucija[338]. Iz navednog se može postaviti osnovna dilema, gdje se privatni sektor uklapa u zaštitu kritične infrastrukture, s obzirom da su države odgovorne za zaštitu nacionalne kritične infrastrukture, koja se ipak nalazi većinom u privatnom vlasništvu i kojom upravlja privatni sektor. Zbog toga se javno-privatno partnerstvo posmatra i kao problem u zaštiti nacionalne infrastrukture[339].

Iako u privatnom sektoru u Sjedinjenim Američkim Državama tradicionalno pripada većina onoga što je definisano kao nacionalna infrastruktura, pri čemu se njen udio procjenjuje na oko 85%, u mnogim evropskim državama je infrastruktura kao što su voda, energija i željeznički saobraćaj u ranijem periodu bila u nadležnosti vlade. Međutim, od 80-ih godina XX vijeka, ova infrastruktura prolazi kroz procese liberalizacije tržišta i privatizacije. Brzi razvoj sektora informacionih i komunikacionih tehnologija u većinskom privatnom vlasništvu, kojima taj sektor i upravlja, kao i zavisnost drugih sektora od njega, doveo je do usložnjavanja postojeće situacije. To je zajedno sa drugim kritičnim međuzavisnostima infrastrukture, dovelo do prilično nejasne situacije u smislu stvarnih ovlašćenja, jer državni organi mogu, formalno ili neformalno, imati ukupnu odgovornost za pouzdano pružanje usluga, ali im nedostaju resursi i vještine da bi svoju odgovornost zaista i ispunili[340]. Uz navedeno, treba dodati i proces globalizacije, sa tendencijom prebacivanja kapitala i poslovanja na privatne kompanije van nacionalne države, što umnogom usložnjava situaciju iz ugla državne kontrole. Činjenica da i nacionalni potrošački indeksi zavise ne samo od drugih sektora, već i od situacije u drugim zemljama, komplikuje situaciju, jer nijedna država nije imuna na efekte niti je sposobna da predvidi ishode ako zemlje u njenom susjedstvu trpe ozbiljne poremećaje u infrastrukturi[341].

---

[337] Johnson R. B., Ortmeier J. P. : *Introduction to security:operations and management, fifth edition*, Pearson Education, New York, 2018, pp. 309-310

[338] Radvanovsky R., McDougall A.: *Critical Infrastructure*. Boca Raton, FL: CRC Press, 2013, pp. 5-7

[339] Wigert A.I.: Challenges governments face in the field of critical information infrastructure protection (CIIP): stakeholders and perspective, in: Dunn M., Mauer V. (Eds.): *International CIIP Handbook, Vol. II. Analyzing Issues, Challenges, and Prospects*, Zürich Swiss Federal Institute of Technology Zürich, Switzerland, Zürich, 2006, pp. 150–158

[340] Bruijne De M., Eeten Van M.: Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment, *Journal Contingency Crisis Management*, Volume 15, Issue 1 ,2007, pp. 20–26

[341] Mussington D.: *Concepts for Enhancing Critical Infrastructure Protection. Relating Y2K to CIP Research and Development*, Prepared for the Office of Science and Technology Policy, RAND Science and Technology Policy Institute, US, Santa Monica, CA, 2002, pp. 1-5

Ovdje smo suočeni sa dilemom o opštem dobru. Postoji argumentacija po kojoj rešenje leži u konceptu i praksi korporativne društvene odgovornosti, pri čemu je veza između navedenog kocepta i otpornosti kritične infrastrukture ujedno ubjedljiv argument za razumijevanje i unapređivanje društvene uloge korporacija u poslovanju[342]. Međutim, iako korporativna društvena odgovornost i javno-privatno partnerstvo mogu izgledati sami po sebi razumljivi i opšte prihvaćeni, ovaj plitki konsenzus obično se krši kada postane jasno da vlade očekuju da privatni sektor uloži značajna sredstva iznad njihovih proračuna troškova i koristi. Stoga ova dilema ostavlja vladama samo dvije mogućnosti: da same obezbijede neophodna sredstva za kritičnu infrastrukturu, iz javnog budžeta, ili da povećaju regulaciju[343].

Privatni sektor u Sjedinjenim Američkim Državama danas posjeduje veliki dio kritične nacionalne infrastrukture[344]. Ovi vlasnici i operatori imaju najviše informacija i razumiju prijetnje i ranjivosti tog sektora bolje od bilo koje druge osobe ili grupe. Oni će znati najbolje ili najprikladnije akcije koje treba preduzeti ako se nešto dogodi. Koncept javno-privatnog partnerstva se odnosi na sporazum kojim se razrađuje saradnja između javne agencije i aktera iz privatnog sektora. Cilj sporazuma je sticanje vještina i resursa svake odvojene grupe kako bi se zadatak mogao efikasno izvršiti. Razvijanje adekvatnog partnerstva treba da rezultira efikasnim pružanjem usluga. U SAD je pristup toj oblasti očigledno zasnovan na dobrovoljnoj saradnji privatnog sektora sa saveznom vladom. To se u velikoj mjeri odnosi na antiregulacijske tradicije u zemlji i spremnost privatnog sektora da sprovede svoj udio odgovornosti upravo u cilju izbjegavanja regulacije. U poređenju sa SAD-om, pristup Evropske unije, koji se oslanja na nacionalnu regulativu, a ne na zakonodavstvo EU, izgleda da predstavlja korak ka regulatornim naporima, a ne pukom dobrovoljnom poštovanju zakona, iako i SAD i EU stavljaju naglasak na važnost javno-privatnog partnerstva[345].

Opšti trend privatizacije se neminovno odražava i na policijsku službu, koja se danas suočava sa brojnim ograničenjima, uključujući njihovu ograničenu nadležnost, reaktivnu ulogu, različite poglede na sopstvenu misiju, te veliko opterećenje i složene radne zadatke koje je sve teže efikasno obavljati. S druge strane, industrija privatnog obezbjeđenja pruža usluge svojim klijentima, uključujući i zaštitu kritične infrastrukture koje su van opsega policije. Obavljanje ovih usluga je poboljšalo opšti nivo sigurnosti u SAD. Pouke istorije i rezultati različitih istraživanja pokazuju da ni policija ni privatno obezbjeđenje ne mogu sami obavljati svoje poslove, već da su jedni drugima potrebni. Iako privatni i javni sektor nemaju identične interese u borbi protiv kriminala, njihovi interesi se mogu nadopunjavati. Istina je da privatni zaštitari duguju vjernost svojim klijentima i poslodavcima, dok policija radi za državu ili lokalnu zajednicu. Međutim, i policija i privatno obezbjeđenje imaju zajednički cilj - bezbjednost i sigurnost društva. Osoblje privatnog obezbjeđenja u objektima kritične infrastrukture može predstavljati značajnu pomoć policiji kroz pružanje sveobuhvatnih i tačnih izveštaja vezanih za istrage o incidentima. Nedostatak ili nedovoljan nivo

[342] Ridley G.: National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience, *Journal of Business Ethics*, vol. 103, no. 1, 2011, pp. 115–120

[343] Bruijne De M., Eeten Van M.: Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment, *Journal Contingency Crisis Management*, Volume 15, Issue 1 ,2007, pp. 24

[344] Stevens G. M., Tatelman, T. B.:*Protection of Security-Related Information*. Congressional Research Service, September 27, 2006, dostupno na: http://fas.org/sgp/crs/secrecy/RL33670.pdf.

[345] Pursiainen C., Gattinesi P.: *Towards Testing Critical Infrastructure Resilience*, Publications Office of the European Union, JRC Scientific and Policy Reports, Luxembourg, 2014, dostupno na:https://core.ac.uk/download/pdf/38627770.pdf

komunikacije i saradnje u toj oblasti je posebno ozbiljan problem i izazov, s obzirom na traumatična iskustva terorističkih napada na SAD i njenu kritičnu infrastrukturu, koja su se u najdrastičnijem vidu ispoljila terorističkim akcijama 11. septembra 2001. godine, te činjenicu da ne treba isključiti mogućnost da kritična infrastruktura u toj zemlji bude ponovo na taj ili sličan način ugrožena[346].

4.3.1. Javno-privatno partnerstvo u zaštiti kritične infrastrukture SAD

U okviru reforme obavještajno-bezbjednosnog sistema SAD su 2001. godine formirale Ured za unutrašnju bezbjednost Izvršnog Ureda predsjednika (Office of Homeland Security - OHS), a sa zadatkom koordinacije primjene sveobuhvatne nacionalne strategije za zaštitu SAD od terorističkih prijetnji ili napada. Koordinacija podrazumijeva djelovanje Ureda u cilju objedinjavanja djelovanja svih izvršnih agencija, ustanova izvršne vlasti i njihovih kapaciteta radi otkrivanja, prevencije i zaštite od terorističkih akata na teritoriji SAD. Uredom rukovodi Savjetnik predsjednika za nacionalnu bezbjednost, a sve neophodne kadrovske, materijalne i druge potencijale ovo tijelo dobija od Ureda za administraciju Izvršnog ureda predsjednika. Savjet za unutrašnju bezbjednost (Homeland Security Council - HSC) je osnovan oktobra 2001. godine, Izvršnom naredbom predsjednika SAD. Odgovoran je za savjetovanje i pružanje pomoći predsjedniku SAD, o svim aspektima unutrašnje bezbjednosti i služi kao mehanizam za osiguranje koordinacije svih aktivnosti vezanih za unutrašnju bezbjednost izvršnih ustanova i agencija, kao i razvoj i primjenu politike unutrašnje bezbjednosti. Članovi Savjeta za unutrašnju bezbjednost su: predsjednik i potpredsjednik SAD, sekretar Državnog trezora, sekretar odbrane, Vrhovni tužilac, sekretar Službe za zdravlje i socijalnu pomoć, sekretar transporta, direktor Federalne agencije za vanredne situacije(Federal Emergency Management Agency-FEMA), direktori Federalnog istražnog biro (FBI) i Centralne obavještajne agencije (CIA), pomoćnik predsjednika za unutrašnju bezbjednost i drugi rukovodioci izvršnih ureda koje odredi predsjednik SAD. Savjet za unutrašnju bezbjednost je zadužen za sva pitanja koja se tiču terorističkih prijetnji i napada na teritoriji SAD. On je ujedno i osnovno tijelo zaduženo za razmatranje politike vezane za terorističke prijetnje i napade na teritoriji SAD. Ove odgovornosti Savjet za unutrašnju bezbjednost je preuzeo od Savjeta za nacionalnu bezbjednost (National Security Council - NSC)[347].

Sekretarijat unutrašnje bezbjednosti (Department of Homeland Security – DHS) je osnovan Zakonom o osnivanju Sekretarijata unutrašnje bezbjednosti SAD iz 2002. godine, koji je pratio smjernice Strategije nacionalne bezbjednosti (National Security Strategy) i Nacionalne strategije unutrašnje bezbjednosti (The National Strategy for Homeland Security). Konkretan povod donošenja ovih dokumenata bio je teroristički napad Al Khaide od 11. septembra 2001. godine. Zakon je stupio na snagu 01. januara 2003. godine, što ujedno označava početak rada DHS-a koji je objedinio rad 22 agencije i ustanove izvršne vlasti. U vezi sa tim, DHS ima osnovnu namenu zaštita bezbjednosti domovine, odnosno unutrašnja bezbjednost SAD. To je ujedno funkcija, koju do tada nije imala ni jedna ustanova izvršne vlasti.U sprovođenju definisanih zadataka, glavni poslovi su analiza informacija i zaštita infrastrukture sprečavanje hemijskih, bioloških, radioloških, nuklearnih i sličnih opasnosti, bezbjednost na granicama i u transportu, pripremljenost i reagovanje na vanredne situacije i saradnja (uključujući i opremu i obuku) sa drugim izvršnim tijelima, personalom, službama i

[346] Dempsey S J.: *Introduction to Private Security*, Second Edition, Cengage Learning, 2011, p. 356
[347] Milošević M., Srećković Z.:*Obaveštajne službe*,NIO Vojska, Beograd, 2010, str. 364-365

vlastima na državnom i lokalnom nivou, privatnim sektorom, i drugim entitetima. Sekretarijatom rukovodi Sekretar za unutrašnju bezbjednost, koga imenuje Predsjednik uz konsultacije sa Kongresom. Glavne organizacione jedinice DHS su podsekretarijati, za analizu informacija i zaštitu infrastrukture, za mjere sprečavanja hemijske, biološke, radiološke i nuklearne opasnosti, za bezbjednost granica i transporta i za pripremljenost za reagovanje u vanrednim situacijama[348].

Značajne korekcije u promjeni pristupa Sjedinjenih Američkih Država problemima zaštite kritične infrastrukture vezani su za 1997. godinu, kada je održan sastanak američke vlade i privatnog sektora posvećen tim pitanjima. I prije toga je u SAD prepoznata važnost zaštite kritične infrastrukture, ali uglavnom sa aspekta njenog komercijalnog uticaja, a ne i sa stanovišta implikacija za nacionalnu bezbjednost. Naime, tadašnja američka administracija je uočila potrebu da preispita efikasnost dotadašnjeg koncepta zaštite kritične infrastrukture[349]. To je rezultiralo formiranjem Komisije predsjednika SAD za zaštitu kritične infrastrukture (*President's Commission on Critical Infrastructure Protection-PCCIP*). Napori koji su nakon toga preduzimani su dali izvjesne rezultate, a dalje aktivnosti na tom planu su u velikoj mjeri bile podstaknute terorističkim napadima 11. septembra 2001. godine.

Za manje od mjesec dana nakon terorističkog napada u SAD formirano je Odjeljenje za unutrašnju bezbjednost (*Office of Homeland Security-DHS*) koje je pod jednim „kišobranom" okupilo 22 različite agencije za sprovođenje zakona. U okviru dodijeljenih odgovornosti, DHS je postalo vodeća federalna agencija za koordinaciju aktivnosti na planu zaštite kritične infrastrukture[350]. Međutim, kako je vrijeme prolazilo, postajalo je sve jasnije da je i sama ideja zaštite nužno trebala da evoluira. To je dovelo do dvije važne promjene koje i danas utiču na javno-privatna partnerstva u zaštiti kritične infrastrukture u SAD. Prvo, ideja zaštite je transformisana u koncept „otpornosti". U pitanju je široki koncept koji sugeriše integrisanu ulogu privatnog sektora u zaštiti kritične infrastrukture. Drugo, saradnja između javnog i privatnog sektora postala je „nova norma" ove aktivnosti, jer se uvidjelo da su za postizanje otpornosti potrebne zajedničke akcije vlade i kompanija. Za javni i privatni sektor bezbjednosti, svaka od ovih promjena dalje je razvijala spoznaje o načinima kako da se efikasno zaštiti kritična infrastruktura.

Nakon terorističkih napada od 11. septembra 2001. godine, postignut je značajan napredak u unapređenju partnerstava javnog i privatnog sektora za zaštitu kritične infrastrukture u Sjedinjenim Američkim Državama. Javno-privatna partnerstva u toj oblasti koja su odlikovala dobrom saradnjom između javnog sektora (vlade) i privatnog sektora (profitno usmjeren) u naporima za postizanje određenog zajedničkog cilja ili skupa ciljeva sve više su doprinosila realizaciji inicijative za zaštitu kritične infrastrukture od lokalnog nivoa do savezne države. Potreba za tim vidom saradnje nije vezana samo za sigurnost građana koji se bave svojim svakodnevnim poslovima, već i za bezbjednost fizičke i sajber infrastrukture na kojoj počiva ekonomski prosperitet i dobrobit SAD-a. Konkretno, događaji od 11. septembra 2001. godine stavili su u prvi plan potrebu za novim razmišljanjem o ulozi privatnog sektora u novom bezbjednosnom okruženju. Do tada se na bezbjednost uglavnom gledalo

---

[348] Ibidem, str. 370

[349] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, *Report of the President's Commission on Critical Infrastructure Protection*, Washington, DC, 1997, dostupno na: https://fas.org/sgp/library/pccip.pdf

[350]Bush G.: *Homeland Security Presidential Directive 7*: Critical Infrastructure Identification, Prioritization and Protection, Washington, DC 2008, dostupno na: https://www.hsdl.org/?abstract&did=441950

tradicionalno, prije svega kao na vojne napore da se odbrane američki interesi od spoljnih prijetnji, pretežno od pojedinih suparničkih ili neprijateljski nastrojenih država. Međutim, uočena je potreba za novom sveobuhvatnijom paradigmom bezbjednosti dovoljno širokom da obuhvati bezbjednost građana, kao i ključna područja ekonomije koja su ranjiva na napade, uključujući kritičnu infrastrukturu[351]. I prije 11. septembra 2001. godine, nezavisne savjetodavne grupe i vladine agencije upozoravale su na moguće napade na tlo SAD-a i naglašavale potrebu da javni i privatni sektor zajedno rade na rešavanju takvih rizika. Međutim, suštinski napredak u uspostavljanju takvog zajedništva krajem 90-ih godina prošlog vijeka bio je usporen nedostatkom percipirane prijetnje, posebno u privatnom sektoru, ali su pomenuti tragični događaji to promijenili[352]. Stoga je iskustvo 11. septembra ukazalo na važnost zaštite kritične infrastrukture za suočavanje sa prijetnjama javnom i privatnom sektoru, a teroristički napadi su uticali i na značajne promjene u organizaciji i načinu djelovanja američke administracije.

4.3.1.1. Normativni i institucionalni okvir partnerstva

O značaju privatnog sektora za nacionalnu bezbjednost Sjedinjenih Američkih Država najbolje svedoče konceptualne teze Strategije nacionalne bezbjednosti[353] po kojima vlada i nevladin sektor treba da rade zajedno u postizanju bezbjednosnih ciljeva. Inače, opseg privatnog sektora bezbjednosti u SAD prevazilazi lokalni, državni i savezni nivo vlasti. U dvije ključne oblasti kritične infrastrukture, snabdijevanje stanovništva i proizvodnja energije, slučajevi prirodnih katastrofa sa kojima se ova država u više navrata suočila pokazali su neophodnost funkcionisanja koncepta javno-privatnih partnerstava. Posebno je bio upečatljiv primjer uragana Katrin koji je 2005. godine primorao zaposlene u javnom i privatnom sektoru da tijesno sarađuju i koordiniraju svoje akcije[354]. Navedeno ukazuje da su od lokalnog do saveznog nivoa, javno-privatna partnerstva sada neizostavan dio zaštite kritične infrastrukture SAD.

Brojna dokumenta koji se odnose na zaštitu kritične infrastrukture, uključujući Direktivu 63 o predsedničkoj politici i unutrašnjoj bezbjednosti (Presidential Policy Directive-63-PPD-63)[355] i Predsedničku direktivu 21 (Homeland Security Presidential Directive-21-HSPD-21)[356], ukazuju na važnost uključivanja privatnog sektora u proces bezbjednosnog planiranja. Odluka predsjednika br. 63 (PPD-63), je posebno značajna jer se njome zahtijeva da vlada i civilne organizacije, a posebno nacionalni koordinator za bezbjednost, zaštitu infrastrukture i borbu protiv terorizma, unaprijede

---

[351] Bowman S.: *Homeland Security: The Department of Defense's Role*, Congressional Research Service, Library of Congress, 14 May 2003.

[352] Eckert S.: Protecting Critical Infrastructure: The Role of the Private Sector, p.1, dostupno na: https://1pdf.net/protecting-critical-infrastructure-the-role-of-the-_58d0335ff6065d954b511e0a

[353] I u aktuelnoj strategiji se apostrofira saradnja javnog i privatnog sektora. Videti: The White House, National Security Strategy, Washington, DC 2017, pp. 19, 31, dostupno na: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[354] Barbaro M., Gillis J.:Wal-Mart at forefront of hurricane relief, *The Washington Post*, September 6, 2005, https://www.washingtonpost.com/archive/business/2005/09/06/wal-mart-at-forefront-of-hurricane-relief/6cc3a4d2-d4f7-4da4-861f-933eee4d288a/?noredirect=on

[355] White House *The Clinton's Administration's Policy on critical infrastructure protection: presidential decision directive 63/PDD-63*, White paper, 22 May 1998, dostupno na: http://fas.org/irp/offdocs/pdd/pdd-63.htm

[356] White House *Presidential Policy Directive--Critical Infrastructure Security and Resilience*, 12, February, 2013, dostupno na: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

saradnju sa privatnim vlasnicima i operatorima kritičnih infrastruktura i počnu da dijele informacije koje se odnose na kritičnu infrastrukturu. U postupku implementacije Direktive PPD-63, mnogi vlasnici i operatori kritični infrastrukture su formirali Centre za dijeljenje i analizu informacija, s namjerom da razmjenjuju informacije sa federalnim zvaničnicima. I pored toga u praksi je bilo relativno malo razmijenjenih informacija između privatnih agencija i savezne vlade. Razlog tome treba tražiti u zabrinutosti privatnih kompanija da li će informacije koje su podijeljene ostati povjerljive[357].

U julu 1996. godine formirana je predsjednička Komisiju za zaštitu kritične infrastrukture sa osnovnim zadatkom da procijeni ranjivosti kritične infrastrukture u SAD i sačini nove planove zaštite. Komisija je u svom izvještaju navela da je potrebna veća razmjena informacija između svih učesnika u zaštiti kritične infrastrukture kako bi vlada mogla da analizira informacije, odredi ranjivosti, i da na osnovu toga predviđa ili sprečava potencijalne napade. U izvještaju je ukazano da je neophodno razviti metode za dvosmjernu razmjenu informacija unutar svake od kritičnih infrastruktura, ali i unutar i između različitih sektora.

Pored toga, Komisija za zaštitu kritične infrastrukture je predložila i formiranje Centara za dijeljenje i analizu informacija (*Information Sharing and Analysis Centers - ISAC*) koji bi se sastojao od predstavnika vlade i privatnog sektora. Pomenuti centri bi predstavljali forum u kome bi se informacije iz svih izvora mogle jednostavno dijeliti i zatim analizirati u cilju identifikovanja ranjivosti. Sličan postupak bi se sprovodio i nakon incidenata kako bi se utvrdilo zašto se taj događaj dogodio i kako izvršiti promjene da bi se spriječio slični incident u budućnosti. Komisija za zaštitu kritične infrastrukture je ipak ubrzo uvidjela da će ove informacije, iako su u teoriji idealne, uticati na povećanje straha vlasnika kompanija da će se njihove poslovne tajne objaviti u javnosti. Stoga je bilo neophodno da se privatnom sektoru pruže garancije da će sve povjerljive informacije koje su podijelili sa drugima biti zaštićene. U aktuelnoj praksi, centri za dijeljenje i analizu informacija predstavljaju sektorski specifične cjeline koje olakšavaju interakciju i komunikaciju između članova. Ukratko, oni prvenstveno omogućavaju razmjenu informacija između vlade i privatnog sektora. Primjeri ISAC-a uključuju lance snabdijevanja, javni prevoz, sektor vode, sektor električne energije, upravljanje u hitnim situacijama i reakciju, informacione tehnologije, hemijski sektor, zdravstvene usluge, autoputeve, hranu i poljoprivredu i druge[358].

Cilj ovih grupa je unapređivanje fizičke i sajber zaštite kritične infrastrukture širom zemlje. Prema PPD-63, centri za dijeljenje i analizu informacija su odgovorni za prikupljanje, analizu i dijeljenje informacija o incidentima i odgovorima među članovima. Prvobitna ideja je bila da postoji jedan Centar za dijeljenje i analizu informacija, ali to se kasnije promijenilo tako da svaki sektor ima svoj centar. Pored razmjene informacija, Centri su uključeni u zaštitu kritične infrastrukture i na druge načine, jer stalno prate događaje i nadgledaju sistem upozorenja o ranoj prijetnji i detekciji. Oni blisko sarađuju sa Sektorskim koordinacijskim vijećima (*Sector Coordinating Councils - SCCs*) kako bi pružili detaljnu analizu događaja ili prijetnji njenom članstvu. Ako se desi neki događaj, Centri

[357] Hemme K.:Critical Infrastructure Protection: Maintenance is National Security, *Journal of Strategic Security*, Number 5 Volume 8, 2015, pp. 25-26, dostupno na: https://scholarcommons.usf.edu/jss/vol8/iss5/3/?utm_source=scholarcommons.usf.edu%2Fjss%2Fvol8%2Fiss5%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages

[358] Sullivant J.: *Strategies for Protecting National Critical Infrastructure Assets A Focus on Problem-Solving*, John Wiley & Sons, Inc., Publication, New Jersey, 2007, pp. 295,296,420

pomažu u koordinaciji odgovora i dijele relevantne informacije sa drugima u tom i u drugim sektorima, kao i između javnih i privatnih agencija. Takođe pomažu u planiranju, koordinaciji i izvođenju vježbi obuke. Članstvo i obim svakog Centra su različiti, ali oni ipak imaju određene zajedničke karakteristike. Na primjer, svaka od grupa promoviše informacije o određenim sektorima i vrši razmjenu obavještajnih podataka o svim prijetnjama i opasnostima po kritičnu infrastrukturu, kao i o ranjivosti i incidentima koji se mogu dogoditi. Pored toga, Centri sarađuju sa drugim agencijama u naporima na smanjenju rizika od potencijalnih napada. Oni takođe uspostavljaju dijalog između povezanih organizacija i vladinih agencija pomažući im da identifikuju najbolje prakse[359].

Posebno je značajno da Centri obezbjeđuju zaštićenost svih osjetljivih informacija. Neki od materijala koji su dostupni preko ISAC-a uključuju informacije iz američkih i stranih vladinih izvora koje nijesu javno dostupne, kao što su informacije Nacionalnog i međunarodnog računarskog tima za hitne slučajeve (*National and International Computer Emergency Response Team - CERT*), informacije agencija za sprovođenje zakona i javne bezbjednosti, informacije o proizvodnji od dobavljača hardvera i softvera, istraživanja nezavisnih istraživača i sektorskih eksperata i geoprostorne analize prijetnji[360].

Kada se razmatra bezbjednost u sajber prostoru, SAD su 2009. godine osnovale Odbor za preispitivanje politike kibernetskog prostora, sa zadatkom da dostavi preporuke o načinima za poboljšanje sajber-bezbjednosti. Među preporukama koje je to tijelo pripremilo je i potreba imenovanja izvršnog koordinatora za sajber bezbjednost, kao i da izvršna vlast bliže sarađuje sa svim ključnim akterima koji učestvuju u politici sajber bezbjednosti SAD, uključujući državnu i lokalnu upravu i aktere iz privatnog sektora. Na taj način bi se obezbijedio organizovaniji i jedinstveniji odgovor na buduće sajber incidente i ojačalo postojeće javno-privatno partnerstvo u cilju stvaranja adekvatne sajber-bezbjednosti. To ujedno predstavlja i temeljni pristup u stvaranju javno-privatnog partnerstva zasnovanog na okvirima upravljanja rizikom u ovoj oblasti. Naime, za rešavanje rastućih sajber-prijetnji potreban je visok nivo javno-privatne saradnje, a priprema i posvećenost i vrhova vlasti i privrede su posebno značajni. U tom smislu, poslovni sektor bi trebao tešnje sarađivati s vladom kako bi najbolje iskoristio modele upravljanja rizikom i pripremi planova otpornosti. Agenciji za bezbjednost kritične infrastrukture (Critical Infrastructure Security Agency - CISA) namijenjena je usklađujuća uloga u domenu sajber spremnosti, reakcije i otpornosti kritične infrastrukture. Pored toga, predmetna agencija koordinira „napore u vezi sa sigurnošću i otpornošću uz korišćenje pouzdanih partnerstava iz privatnog i javnog sektora, kao i na planu pružanja obuke, tehničke pomoći i davanja procjena zainteresovanim stranama, uključujući vlasnike infrastrukture i operatore širom države.[361]

Fuzioni centri (*Fusion Centers*) predstavljaju važan način da se federalnim, državnim, lokalnim, i teritorijalnim agencijama na prostoru SAD omogući razmjena informacija i obavještajnih podataka. Mnoge američke države i veliki gradovi osnovali su ove centre kao način za međusobnu

---

[359] *Sector Coordinating Councils*, Department of Homeland Security, dostupno na: https://www.dhs.gov/cisa/sector-coordinating-councils

[360] Pesch-Cronin K. A., Marion N. E.: *Critical infrastructure protection, risk management, and resilience :a policy perspective*, Taylor & Francis Group, 2016, pp.104-105

[361] Brooks C: Public Private Partnerships And The Cybersecurity Challenge Of Protecting Critical Infrastructure, *Forbes*, May 6, 2019, dostupno na: https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/#7f93f8fc5a57

komunikaciju i razmjenu informacija i obavještajnih podataka u okviru svojih nadležnosti, kao i sa saveznom vladom. Predmetni centri osiguravaju da se klasifikovane i nerazvrstane informacije mogu dijeliti, uz obezbjeđivanje potrebnog nivoa stručnosti. U praksi, informacije se dijele od strane zainteresovanih aktera i stručnjaka za određenu temu, pri čemu Centri imaju pristup podacima koji su neophodni da bi se izvršila analiza. Oni takođe podržavaju vježbe i obuke vezane za zaštitu koje planiraju savezne, državne i regionalne vlasti. Neke od informacija koje se mogu razmijeniti u Centru uključuju bezbjednosne rizike specifične za lokaciju, međuzavisnosti sa drugim sektorima, različite izveštaje o sumnjivim aktivnostima, tehnike protivnika, najbolje prakse zaštite imovine i otpornosti, standardne operativne procedure za reagovanje na incident i hitne komunikacije [362].

InfraGard *(InfraGard*) predstavlja partnerstvo između Federalnog Istražnog Biroa (*Federal Burea of Investigation - FBI*) i aktera iz privatnog sektora. U tom smislu, program InfraGard je sredstvo za nesmetanu javno-privatnu saradnju s vladom koje ubrzava pravovremenu razmjenu informacija i promoviše mogućnosti međusobne saradnje od značaja za zaštitu kritične infrastrukture. Sa hiljadama provjerenih članova na nacionalnom nivou, u članstvu InfraGarda se nalaze menadžeri kompanija, preduzetnici, vojni i vladini službenici, računarski profesionalci, akademije i državne i lokalne službe za sprovođenje zakona, pri čemu je svako od njih u okviru svojih mogućnosti posvećen doprinosu specifičnom uvidu u funkcionisanje ekonomije i unapređenje nacionalne bezbjednosti[363].

Nacionalni savjetodavni odbor za infrastrukturu (*National Infrastructure Advisory Committee*) je u svojoj studiji pod nazivom „Optimizacija resursa za ublažavanje poremećaja infrastrukture“, ukazao na aktuelnu praksu usklađivanja otpornosti infrastrukture sa otpornošću zajednice, na određivanje programa koji bi se mogli ocijeniti kao uspješni i kao takvi mogli biti primijenjeni u drugim zajednicama, kao i na načine kako zajednice i sektori mogu postići sinergiju. U vezi sa ispitivanjem resursa zajednice, namjera Nacionalnog savjetodavnog odbora za infrastrukturu je bila da se sazna da li se može uspostaviti sinergija u javnom i privatnom sektoru i da li postoje mogućnosti za unapređenje zajedničkog planiranja. U završnom dijelu studije se preporučuje da se uspostavi čvršće partnerstvo između javnih i privatnih agencija kako bi se postigla bolja komunikacija između različitih aktera. Takođe je preporučeno da se Državno, lokalno i teritorijalno vladino koordinaciono vijeće (*State, Local, Tribal, and Territorial Government Coordinating Council - SLTTGCC*) i slične organizacije koje imaju značajnu ulogu u pružanju stručnih savjeta saveznoj vladi, aktivnije uključe u pitanja koja se odnose na zaštitu kritične infrastrukture. Pomenuti izvještaj je ukazao da je od suštinske važnosti da resursi i infrastruktura zajednice budu zaštićeni i otporni, što će bitno doprinijeti da i zajednica u cjelini bude otpornija. Na taj način je Nacionalni savjetodavni odbor za infrastrukturu nedvosmisleno pružio podršku jačanju otpornosti zajednice i naglasio potrebu da se prepoznaju značajne postojeće slabosti u infrastrukturi koje mogu ograničiti sposobnost zajednice da bude otporna[364].

Informaciona mreža unutrašnje bezbjednosti (*The Homeland Security Information Network - HSIN*) je sigurni mrežni sistem koji je Odjeljenje za unutrašnju bezbjednost (Office of Homeland Security - DHS) uspostavilo kako bi povećao napore za razmjenu informacija i saradnju između

[362] *Fusion Centers*, Department of Homeland Security, dostupno na: https://www.dhs.gov/fusion-centers
[363] *InfraGard*, dostupno na: https://www.infragard.org
[364] *Optimization of Resources for Mitigating Infrastructure Disruptions Study*, Final Report and Recommendations by the Council, National Infrastructure Advisory Council, 2010, dostupno na: https://www.dhs.gov/sites/default/files/publications/niac-optimization-resources-final-report-10-19-10-508.pdf

vladinih agencija i privatnog sektora koji su uključeni u zaštitu kritične infrastrukture. Informaciona mreža se sastoji od zajednica interesa (*Communities of Interest - COI*) koja omogućava korisnicima u svih saveznih 50 država da u sigurnom okruženju u realnom vremenu razmjenjuju informacije sa drugima u svojim zajednicama. Takođe omogućava članovima da razgovaraju o problemima ili da traže informacije od drugih zajednica. Putem ove mreže grupe su u mogućnosti da virtuelno održavaju sastanke, upućuju poruke i dijele potrebna dokumenata[365].

Kao još jedan način dijeljenja povećanog broja informacija, Odjeljenje za unutrašnju bezbjednost je formiralo i američki tim za spremnost računara u hitnim situacijama (*US Computer Emergency Readiness Team - US-CERT*). Ova agencija pruža drugim subjektima informacije u vezi sa računarskim ranjivostima i prijetnjama, kao i o odgovorima na incidente. US-CERT prikuplja i izvještaje o incidentima od drugih agencija širom zemlje i analizira te informacije kako bi se otkrili obrasci i trendovi kriminala zasnovanog na računarskoj tehnologiji. Službenici ovog tima upravljaju i Nacionalnim sistemom za upozoravanje na sajber, koji pruža opšte informacije svakoj organizaciji ili pojedincu koji se na to pretplati[366].

Prvobitno uspostavljeni 2004. godine, zaštitni savjetnici za bezbjednost (*Protective Security Advisors - PSAs*) dio su Odjeljenja za unutrašnju bezbjednost (Office of Homeland Security-DHS), kao i programa Uprave za nacionalnu zaštitu i programe (National Protection and Programs Directorate - NPPD) koja se nalazi u okviru Kancelarije za zaštitu infrastrukture (*Office of Infrastructure Protection - OIP*). Ovu grupu čine stručnjaci koji su posebno obučeni za zaštitu kritične infrastrukture. Predmetni program fokusiran je na tri oblasti - unapređenje zaštite infrastrukture, pomoć u upravljanju incidentima i olakšavanje razmjene informacija[367]

U prvoj oblasti (unapređenje infrastrukture), regionalni direktori i savjetnici pomažu vlasnicima i operatorima kritične infrastrukture na način da im pružaju obuku i pomoć i vrše procjene ugroženosti ukoliko se to od njih traži. Oni takođe pomažu u procesu identifikacije mogućih rizika po kritičnu infrastrukturu, kao i načina ublažavanja tih rizika. U njihovoj nadležnosti je i pružanje pomoći agencijama za sprovođenje zakona vezano za planiranje i sprovođenje vježbi i drugih scenarija planiranja, odnosno za posebne događaje koji zahtijevaju mjere bezbjednosti, poput političkih skupova ili sportskih događaja.

Drugo područje obuhvata pomoć u upravljanju incidentima. Regionalni direktori i savjetnici (PSAs) često mogu biti prvi koji će se odazvati nakon vanredne situacije ili drugih katastrofa. Tokom događaja, oni sarađuju sa državnim i lokalnim centrima za vanredne situacije, uključujući i Federalnu agenciju za upravljanje vanrednim situacijama (Federal Emergency Management Agency - FEMA) i druge, kako bi smanjili rizike međuzavisnosti ostalih sektora kritične infrastrukture u kriznim situacijama. Takođe, oni mogu biti od koristi u pružanju savjeta u aktivnostima oporavka nakon krize.

Treće područje je olakšavanje razmjene informacija. Ovdje regionalni direktori i savjetnici pomažu protok informacija između svih nivoa vlasti i privatnog sektora. U slučajevima kada nema vanrednih situacija, oni obavljaju preglede i održavaju sastanke sa partnerima za zaštitu infrastrukture

---

[365] Pesch-Cronin K. A., Marion N. E.: *Critical infrastructure protection, risk management, and resilience : a policy perspective*, Taylor & Francis Group, 2016, pp.232,268, 287,341

[366] Ibidem,pp. 107,260

[367] The Department of Homeland Security, *Protective Security Advisor Program*, dostupno na: https://www.dhs.gov/sites/default/files/publications/PSA-Program-Fact-Sheet-05-15-508.pdf

radi razmjene informacija. U slučaju događaja, ostvaruju saradnju sa drugim subjektima o reakcijama i oporavku kritične infrastrukture. Sopstvene informacije o stanju i događajima pružaju Nacionalnom koordinacionom centru za infrastrukturu i predstavnicima državnog, lokalnog i privatnog sektora. Posebno značajna saradnja se ostvaruje i sa vlasnicima i operatorima kritične infrastrukture u uslovima njenog oštećenja[368].

Nakon što je Kongres SAD 2007. godine usvojio amandman na Zakon o unutrašnjoj bezbjednosti, sekretar za unutrašnju bezbjednost dodijelio je zadatak Federalnoj agenciji za upravljanje u kriznim situacijama (FEMA), da u saradnji sa Odjeljenjem za unutrašnju bezbjednost (DHS), Kancelarijom za zaštitu infrastrukture (OIP), Direkcijom za nauku i tehnologiju Odjeljenja za unutrašnju bezbjednost i drugim, razviju program spremnosti privatnog sektora (*PS - Prep Program*). U skladu sa ovom inicijativom, Federalna agencija za upravljanje u kriznim situacijama je pokrenula dobrovoljni program za aktere u privatnom sektoru s ciljem poboljšanja njihove pripremljenosti za događaje. Program uključuje uspostavljanje smjernica, najboljih praksi, propisa i kodeksa prakse. Uz ovaj program, vlasnici i operatori imovine privatne kritične infrastrukture u privatnom vlasništvu mogu koristiti standarde za poboljšanje svojih planova zaštite[369]. U vezi sa tim je značajno da je Odjeljenje za unutrašnju bezbjednost je izradilo katalog resursa privatnog sektora koji je posebno usmjeren na potrebe vlasnika iz privatnog sektora. Katalog resursa privatnog sektora, koji je prvi put objavljen u maju 2010. godine, centralizuje pristup svim resursima namijenjenim privatnom sektoru, uključujući male i velike kompanije, akademske zajednice, trgovinska udruženja i druge nevladine organizacije. Prepoznajući širinu i raznolikost raspoloživih resursa, kao i kontinuirani rad i promjene u ovoj oblasti, katalog se ažurira dva puta godišnje[370].

Odjeljenje za unutrašnju bezbjednost je sačinilo i priručnik za otpornost i zaštitu kritične infrastrukture (*Critical Infrastructure Protection and Resilience Toolkit*) kao pomoć vlasnicima i operatorima kritičnih infrastrukturnih resursa na lokalnom i regionalnom nivou, kako bi im se pomoglo da se pripreme, zaštite, reaguju, ublaže i oporave od mogućih prijtnji ili opasnosti. Ovaj priručnik sadrži informacije koje opisuju ulogu lokalne i regionalne zajednice i privatnih organizacija u aktivnostima zaštite. Priručnik takođe uključuje resurse za vježbe planiranja i obuke koje mogu pomoći u prepoznavanju ranjivosti i problema sa otpornošću u njihovim zajednicama Odjeljenje za unutrašnju bezbjednost je takođe pripremilo i odgovore na razna često postavljana pitanja koja se tiču uloge privatnih vlasnika u zaštiti kritične infrastrukture. U priručniku su navedeni i linkovi do drugih korisnih referentnih materijala i sredstava za obuku, kao i informacije o mogućim partnerstvima i drugim načinima za dijeljenje kritičnih informacija[371].

Odjeljenje za unutrašnju bezbjednost je uspostavilo i Savjet za savjetodavno partnerstvo kritične infrastrukture (*Critical Infrastructure Partnership Advisory Council - CIPAC*) kao način da se unapredi komunikacija između saveznih programa i državnih, lokalnih, teritorijalnih i agencija

---

[368] Pesch-Cronin K. A., Marion N. E.: *Critical infrastructure protection, risk management, and resilience: a policy perspective,* Taylor & Francis Group, 2016, p.108

[369] Office of Homeland Security, Federal Emergency Management Agency, *Critical Asset Risk Management, Participant Guide*, 2014, pp. 6-12

[370] Department of Homeland Security, *Private Sector Resources Catalog*, dostupno na: https://www.dhs.gov/private-sector-resources-catalog

[371] Pesch-Cronin K. A., Marion N. E.: *Critical infrastructure protection, risk management, and resilience: a policy perspective,* Taylor & Francis Group, 2016, p.109

koje obezbjeđuju zaštitu infrastrukture. Savjet pored ostalog uključuje predstavnike saveznih, državnih, lokalnih vlasti, kao i specijalizovane vladine grupe koje su članovi Koordinacionog savjeta za svaki sektor[372]. Predmetni organ pomaže u koordinaciji programa zaštite savezne kritične infrastrukture sa vlasnicima i operatorima iz privatnog sektora. CIPAC je takođe i forum na kome se razgovara o problemima ili učestvuje u aktivnostima koje doprinose poboljšanju koordinacije u području zaštite kritične infrastrukture. Članovi Savjeta se često sastaju kako bi razgovarali o planiranju, bezbjednosnim problemima, operativnim aktivnostima, reagovanju na incidente ili oporavku. Oni takođe mogu razgovarati i o informacijama o mogućim prijetnjama, ranjivosti ili zaštitnim mjerama. Savjet pruža značajan doprinos saradnji između javnih i privatnih entiteta na saveznom nivou koji se odnose na zaštitu kritične infrastrukture i implikacije na nacionalnu bezbjednost. Postojanje ovakve koordinacione savjetodavne grupe, kao i prisustvo vodećih američkih kompanija u njoj, svjedoči da su javno-privatna partnerstva sastavni dio ostvarivanja ciljeva u zaštiti kritične infrastrukture i podizanju nivoa opšte bezbjednosti u zemlji[373].

Odjeljenje za unutrašnju bezbjednost Federalne agencije za upravljanje u kriznim situacijama ima i ulogu sponzora, na način da pruža finansijsku podršku programima koji žele da unaprijede zaštitu infrastrukture i sigurnost imovine. Te programe prati Direkcija za programe (*Grant Programs Directorate - GPD*). Fokus Direkcije je na uspostavljanju i promovisanju komunikacije sa državnim, lokalnim i drugim zainteresovanim stranama i na povećanju nivoa spremnosti i sposobnosti države da se zaštiti od napada i reaguje na njih. Sve u svemu, pomenuti programi FEMA pomažu u finansiranju mnogih aktivnosti koje se odnose na unutrašnju bezbjednost i spremnost za vanredne situacije. Neki od tih programa se odnose na planiranje, organizaciju, kupovinu opreme, obuku, vježbe i troškove upravljanja i administracije[374].

Odjeljenje za unutrašnju bezbjednost je takođe, preko Nacionalne direkcije za pripremljenost, kreiralo brojne programe s ciljem pomoći lokalnim zajednicama da sprovedu obuke na planu adekvatnog reagovanja na različite događaje. Kroz program obuke Nacionalnog konzorcijuma za domaću spremnost (*National Domestic Preparedness Consortium - NDPC*), Odjeljenje za unutrašnju bezbjednost i Federalna agencija za upravljanje u kriznim situacijama oficijalno pružaju obuku za hitne slučajeve u SAD-u i na njenim prekomorskim teritorijama. U vezi sa tim, obezbijeđena su tri nivoa obuke: obuka na nivou svijesti, obuka na nivou performansi i obuka na nivou menadžmenta. Programi obuke na nivou svijesti dizajnirani su za brojne aktere širom svijeta i cilj im je da predstave osnovne pojmove učesnicima. Namijenjeni su upućivanju u ključne principe i politike vezane za zaštitu i bezbjednost infrastrukture. Ovi kursevi se obično fokusiraju na osnovne teme koje se tiču sprečavanja i pripreme za incidenate (uključujući tehnike ublažavanja). Druga vrsta treninga je obuka na nivou performansi. Na ovaj način, službenici Odjeljenja za unutrašnju bezbjednost pomažu u obuci učesnika kako bi mogli obavljati određene zadatke ili posjedovati određene vještine koje su potrebne prilikom odgovara na događaj ili oporavak od njega. Na primjer, neki od kurseva se fokusiraju na to kako se nositi sa havarijama vezanim za opasne hemijske supstance ili radioaktivne materijale. Treća

[372]Department of Homeland Security, Critical Infrastructure Partnership Advisory Council, dostupno na: https://www.dhs.gov/critical-infrastructure-partnership-advisory-council

[373] Busch E. N., Givens D. A: Public-Private Partnerships in Homeland Security: Opportunities and Challenges, *Homeland Security Affairs*, Volume 8, article 18, 2012, pp. 3-4, dostupno na: https://www.hsaj.org/articles/233

[374] Više o navedenom programu: Federal Emergency Management Agency- *Grant*s, dostupno na:https://www.fema.gov/grants

vrsta obuke koju omogućava Odjeljenje za unutrašnju bezbjednost su časovi obuke na nivou menadžmenta. Njihov osnovni cilj je poboljšanje liderskih vještina za lica na rukovodećim ili drugim nadzornim pozicijama. Ako je potrebno, Odjeljenje za unutrašnju bezbjednost takođe pruža pomoć zajednicama u realizaciji vježbi, s ciljem da se utvrde i otklone eventualni nedostaci. Najzad, program vježbanja i evaluacije za unutrašnju bezbjednost (*Homeland Security Exercise and Evaluation Program - HSEEP*) pruža pomoć u osmišljavanju vježbi, njihovom izvođenju i procjeni. Te vježbe mogu obuhvatati seminare, radionice, funkcionalne vježbe ili vježbe u cijelom obimu i slično[375].

4.3.1.2. Privatni sektor bezbjednosti u zaštiti kritične infrastrukture

Istorijski posmatrano, SAD imaju dugu tradiciju privatnog sektora bezbjednosti. Korijeni savremenog sektora privatne bezbjednosti u toj zemlji vezani su za Alana Pinkertona koji je 1850. godine osnovao prvu privatnu detektivsku agenciju. Pored rada sa lokalnom policijom, Pinkerton je bio angažovan od strane željezničke korporacije za kontrolu vozova i uspostavljanje bezbjednosnih sistema. Po izbijanju građanskog rata 1861. godine, Pinkerton je ponudio svoje usluge saveznoj vladi i dobio je zadatak da štiti predsjednika SAD Abrahama Linkolna. Nakon toga je uslijedilo i formiranje Nove željezničke policije koja je imala puna policijska ovlašćenja vezano za zaštitu opreme kompanije, voznog parka i imovine, kao i za zaštitu željeznica od napada organizovanih grupa i pljačkaša vozova. Sa nastavkom procesa industrijalizacije, američke kompanije su počele da koriste snage privatnog obezbjeđenja da bi zaštitile svoju imovinu koju su ugrožavale aktivnosti štrajkača. Generalno, privatne bezbjednosne snage bile su uspješne u razbijanju radničkih štrajkova, ali je 1892. godine došlo do promjene, kada su iste bile poražene od strane štrajkača u sukobu do koga je došlo u Pensilvaniji. Tokom ovih burnih vremena, Kongres je započeo istrage privatnih kompanija za obezbjeđenje, a mnoge savezne države su donijele zakone kojima je oružanim plaćenicima zabranjeno da ulaze na njihove teritorije. Pored toga, mnoge velike kompanije u područjima brodogradnje, čeličana i drugim industrijskim granama osnovale su privatne bezbjednosne snage radi zaštite imovine i održavanja reda u gradovima i fabrikama u sastavu svojih kompanija[376]. Početkom dvadesetog vijeka u SAD je nastavljen trend porasta potreba za bezbjednosnim uslugama zbog naglo rastuće industrijalizacije i potrebe za rešavanjem problema vezanih za radnu snagu i upravljanje. Na tom planu, fabrike i kompanije su nastavile da uspostavljaju unutrašnje, sopstvene snage obezbjeđenja i da na ugovornoj osnovi angažuju firme za obezbjeđenje kako bi zaštitile kompanijsku robu i imovinu, te rešavale poremećene odnose sa sindikatima[377].

Velika ekspanzija privatnog obezbjeđenja u SAD je započela u godinama prije i tokom Drugog svetskog rata, pošto su američke kompanije postale glavni dobavljači materijala Velikoj Britaniji i Francuskoj u njihovim ratnim naporima. Sredinom XX veka, posebna pažnja je bila fokusirana na zaštitu američkih aviokompanija jer je zabilježen veliki broj pokušaja otimica aviona i prijetnji bombama. Kao odgovor na te prijetnje, Savezna uprava za vazduhoplovstvo započela je od 1972. godine obaveznu kontrolu putnika. Odgovornost za navedene mjere preuzele su vazduhoplovne kompanije, a kontrolu su vršile privatne bezbjednosne kompanije. Slični postupci uspostavljeni su i

[375] Pesch-Cronin K. A., Marion N. E.: *Critical infrastructure protection, risk management, and resilience: a policy perspective*, Taylor & Francis Group, 2016, p.109
[376] Dempsey S. J.: *Introduction to Private Security, Second Edition*, Wadsworth, Cengage Learning, 2011, rr. 10-11
[377] Ibidem, pp. 11-12

u mnogim drugim zemljama. Učinak odabranih firmi u ovoj oblasti je bio veoma loš i i mnogi smatraju da je uspjehu terorista - otmičara vazduhoplova 11. septembra 2001. godine doprinio i njihov neprofesionalni rad[378].

U ovoj kratkoj istorijskoj retrospektivi privatnog sektora bezbjednosti posebno je značajna 2004. godina kada je sekretar Odjeljenja za unutrašnju bezbjednost saopštio da je Američko društvo za industrijsku bezbjednost (*American Society for Industrial Security -ASIS*), imenovano kao partner privatnog sektora u novom nacionalnom programu za razmjenu informacija i obaveštenja o terorizmu, u okviru informativne mreže o unutrašnjoj bezbjednosti i kritičnoj infrastrukturi (*Homeland Security Information Network–Critical Infrastructure (HSIN-CI)*. Ovaj operativni, međuresorni, međusektorski program je omogućio Američkom društvu za industrijsku bezbjednost da učestvuje u razmjeni informacija sa saveznim vlastima u vezi sa upozorenjima o terorizmu i drugim povezanim incidentima i prijetnjama.[379]Američko društvo za industrijsku bezbjednost je 2009. godine uspostavilo i objavilo smjernice o kontinuitetu poslovanja, ulozi glavnog bezbjednosnog službenika, upravljanju fizičkom bezbjednošću objekata, opštoj procjeni rizika bezbjednosti, zaštiti imovine, izboru i obuci privatnih službenika za poslove obezbjeđenja, procjeni rizika, sprečavanju nasilja i intervencijama na radnom mjestu. I druge industrije koje utiču na bezbjednost takođe su počele da definišu minimalne standarde u svojim domenima. I bez dalje analize evidentno je da su posebni pomaci na tom planu načinjeni tek nakon terorističkih napada 2001. godine [380].

Funkcionisanje kritične infrastrukture u SAD i njena zaštita se ne mogu odvojiti od javnog i privatnog učešća u tome, budući da veliki dio američke nacionalne infrastrukture štite privatne kompanije. U vezi sa tim, treba napomenuti da Američko društvo za industrijsku bezbjednost ima posebnu profesionalnu radnu grupu koja je posvećena između ostalog i zaštiti kritične infrastrukture. Privatni sektor je postao nezamjenjiv igrač u procesu zaštite kritične infrastrukture u SAD (Šema br. 3), jer je pripadnicima tog sektora povjeren najveći dio tih poslova. Razlog tome leži i u činjenici da javni sektor u potpunosti priznaje sopstevenu nemoć da bezbjednosno pokrije mnoštvo objekata i resursa nacionalne kritične infrastrukture. Kao rezultat toga, promovišu se partnerstva s privatnim sektorom na gotovo svim nivoima i sektorima američke kritične infrastrukture[381].

---

[378] Ibidem, p. 14

[379] ASIS International, *ASIS International Joins Department of Homeland Security and FBI on Information-Sharing Project*, ASIS International Press Release, June 23, 2004, dostupno na: https://www.businesswire.com/news/home/20040623005739/en/ASIS-International-Joins-Department-Homeland-Security-FBI

[380] U.S. Government Accountability Office, *Critical Infrastructure Protection*: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress 2015, dostupno na:http://www.gao.gov/assets/680/673779.pdf.

[381] Busch E. N., Givens D. A.: Public-Private Partnerships in Homeland Security: Opportunities and Challenges, *Homeland Security Affairs*, Article 18, 2012, p.1, dostupno na: https://www.hsaj.org/articles/233

Šema br. 3.: Preklapanje i odgovornost za zaštitu infrastrukture[382]

Bezbjednost nacionalne kritične infrastrukture zahtijeva efikasan partnerski okvir između javnog i privatnog sektora i to se ostvaruje kroz niz inicijativa, uključujući program partnerstva u sektoru kritične infrastrukture. Pri tome treba napomenuti da svaki pojedinačni sektor kritične infrastrukture u SAD ima razvijen sopstveni sistem javno-privatnog partnerstva u zaštiti kritične infrastrukture[383].

Privatne firme za obezbjeđenje podjednako su angažovane na konsolidaciji sopstvenih resursa u svijetu kritične infrastrukture. Takav razvoj u ovoj oblasti donosi ogromne prihode privatnim firmama za obezbjeđenje i ukazuje na još jednu mogućnost privatizacije u području bezbjednosne zaštite. Tako je na primjer Sekuritas (*Securitas Critical Infrastructure Services*) razvio posebno odjeljenje namenjeno isključivo raznim infrastrukturnim uslugama u oblasti energije, vazduhoplovstva i petrohemijske industrije[384].

Vjerovatno nijedna druga oblast kritične infrastrukture u SAD ne nudi takve perspektive privatnim bezbjednosnim službama kao što je to slučaj sa sektorom saobraćaja i transporta. Jednom riječju, u pitanju je ogroman sektor, koji uključuje ne samo kretanje ljudi, već i isporuku komercijalne robe i usluga na globalnom nivou. U proteklom periodu su akteri privatne bezbjednosti ostavili neizbrisiv trag u zaštiti željeznice, vazduhoplova i aerodroma, luka i skladišta, transportnih centara i čvorišta, pristupnih i izlaznih tačaka. Postoji niz razloga za to. Prvo, pomenuta infrastruktura je po

[382] Nemeth C. P.:*Private security : an introduction to principles and practice*, Taylor & Francis Group, 2018, p. 491

[383] Videti: Review the Sector Coordinating Council for Energy, dostupno na: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

[384] Više o vitalnoj ulozi koju privatni sektor može igrati u obezbeđenju kritične infrastrukture na. https://www.scisusa.com/.

svom obimu prevelika da bi se mogla osloniti samo na vladu po pitanjima svoje zaštite. Drugo, taj sektor po pravilu pokreću privatne kompanije i privatni ekonomski interesi, pri čemu je vlada konceptualno udaljena i nespremna da u dovoljnoj mjeri cijeni, pa i da u potpunosti pojmi finese funkcionisanja tako glomaznog i složenog sistema. Zbog toga je to dugogodišnje područje partnerstva koje zahtijeva koordinisano djelovanje vlasti (savezne, državne i lokalne) i privatnog sektora. Novi oblici javno-privatnog partnerstva su neophodni za suočavanje sa izazovima koje predstavljaju nove tehnologije i netradicionalne prijetnje[385].

Kontrola i nadzor američke trgovine, bez obzira da li se ostvaruje kopnom, morem ili vazduhom predstavlja složen proces u kome se moraju „pomiriti" bezbjednost i sigurnost sa brzim i efikasnim kretanjem robe. To postaje sve veći izazov u globalnoj ekonomiji u kojoj potrošači, pravovremeni procesi i integrisani lanci snabdijevanja zahtijevaju pouzdanost, tačnost i brzinu. Pored toga, taj izazov je u direktnoj vezi i sa ogromnom količinom robe koji se kreće u luke SAD-a i izvan njih. Neke procjene ukazuju da čak tri biliona dolara robe u SAD uđe morskim putem godišnje, a otprilike 90% robe koja se konzumira u SAD dolazi brodovima[386]. Prije nego što ta roba stigne, bezbjednosni izazovi su različiti i brojni – od somalijskih pirata do međunarodnih terorista. Iz tih razloga, vlasnici brodova su počeli da se oslanjaju na obezbjeđenje od strane privatno ugovorenog naoružanog osoblja (privately contracted armed security personnel - PCASP) kako bi na taj način osigurali bezbjedan prolazak svoje robe. Osnivanje navedenih bezbjednosnih kompanija je predstavljalo iskorak naprijed u odbrani od narasle piraterije.

Globalna razmjena i trgovina zahtijevaju partnerski mentalitet gdje pomorski prevoznici, njihove bezbjednosne snage i osoblje usko sarađuju sa Obalskom stražom, Carinskom i graničnom zaštitom i Odjeljenjem za unutrašnju bezbjednost. U stvari, najveći dio morske trgovine SAD oslanja se na samoosveštavanje i integritet špeditera i pomorskih operatora. Kako bi podstakla integritet ovog partnerstva, Carinska i granična zaštita je usvojila program Carinsko-trgovinsko partnerstvo protiv terorizma (*Customs Trade Partnership against Terrorism - C-TPAT*). Predmetni program prepoznaje suštinsku ulogu koju privatni teretni prevoznici imaju na planu sigurnosti i bezbjednosti robe koja se odvija kroz luke. Privatne firme za obezbjeđenje su dio programa S-TRAT u smislu pružanja usluga obuke, usavršavanja, softverskih paketa i dizajna i regulatorne ekspertize firmama širom svijeta. Kompanije poput Pinkerton's i Allied Barton promovišu svoj poslovni model zaštitite imovine kompanija i poboljšanja upravljanja rizikom lanaca snabdijevanja, naročito za uvoznike (izvoznike), kompanije za transport, dostavljače, špeditere, kao i za pokretanje globalnih logističkih firmi[387]

Sektor u kome se ispoljio nejednako uspješan uticaj privatnog sektora bezbjednosti je aviosaobraćaj. Prije 11. septembra 2001. godine, ovo je bila industrija najvećeg rasta privatnog sektora. Nakon ovog događaja, privatne bezbjednosne kompanije gotovo su nestale sa liste operatora Agencije za bezbjednost transporta, kojoj je i data nadležnost za konrolu putnika i bezbjednost vazduhoplova[388]. Međutim, i u funkcionisanju ove Agencije uočeno je dosta problema. Tako je na

---

[385] Eckert S.: *Protecting Critical Infrastructure: The Role of the Private Sector*, p. 1, dostupno na: https://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf.

[386] Videti šire u: Christopher K.: *Port Security Management, Second Edition*, Taylor & Francis Group, 2015, pp. 6-7,

[387] Izvor: https://www.pinkerton.com/our-services/Global-Supply-Chain-Security-Risk-Management

[388] Taylor A.B.: *The Evolution of Airline Security Since 9/11*, (December 2003), dostupno na: http://www.ifpo.org/resource-links/articles-and-reports/protection-of-specific-environments/the-evolution-of-airline-security-since-911/.

primjer Uprava za masovni tranzit grada Njujorka uputila upozorenje da će usluge Agencije za bezbjednost transporta biti zamijenjene uslugama koje pruža privatni sektor bezbjednosti, što umnogom svjedoči da ni ta agencija ne funkcioniše na optimalan način, te da ima problem sa nedostatkom javne podrške[389].

Nesumnjivo je da će u svijetu tranzitne bezbjednosti privatni sektor u SAD i dalje ostvarivati kontakte i saradnju sa Agencijom za bezbjednost transporta, imajući u vidu da pregled putnika i prtljaga, uz širok spektar drugih aktivnosti, ostaje glavni zadatak ove Agencije. Inače, Agencija za bezbjednost transporta je sastavni dio Odjeljenja za unutrašnju bezbjednost i ne samo da je odgovorna za bezbjednost sistema vazdušnog prevoza u zemlji, već je u njenoj nadležnosti da, u saradnji sa državnim, lokalnim i regionalnim partnerima, nadgleda sigurnost autoputeva, željeznica, autobusa, sistema za masovni tranzit, luka, te 450 aerodroma širom SAD-a. Najveći dio poslova Agencije za bezbjednost transporta odnosi se na bezbjednost aviokompanija, a osnovna misija je transport od aerodroma do autobuskih stanica i željezničkih terminala (svi oblici i sve lokacije). Agenciji je povjerena izuzetna odgovornosti, ali je ista u proteklom periodu ispoljila određenu suzdržanost u širenju svog djelovanja na sve vidove transporta[390].

Zadatak obezbjeđenja željezničkog i masovnog tranzitnog sistema u SAD je jednako važan kao i zaštita vazdušnog saobraćaja. Treba imati u vidu da sistemi za masovni tranzit u toj zemlji prevoze gotovo 10 milijardi putnika godišnje, dok vozni park masovnog prevoza iznosi gotovo 150.000 vozila. Jedan od primjera je željeznički operator Amtrak, koji u nacionalnoj mreži prevozi gotovo 31 milion putnika. Postojeći trend prema masovnom tranzitu je i kratkoročan, a dugoročno će biti sve izraženiji. Državni željeznički sistem sa nizom linija za teretni i putnički saobraćaj, predstavlja glavni dio ekonomskog života Sjedinjenih Američkih Država. Inače, u svijetu trgovine vozovi isporučuju teretne robe, po kilometru, više i efikasnije nego što je za to sposobna bilo koja kompanija za prevoz robe na kopnu. Svakodnevno se preko nacionalne infrastrukture SAD prevozi više od milion pošiljki opasnih hemikalija, veliki procenat ovih hemikalija prevozi se željeznicom, pri čemu postoje rizici akcidenata[391].

Trenutni naglasak Agencije za bezbjednost transporta i drugih vladinih agencija u SAD je angažovanje privatnih partnera koji pomažu u praćenju bezbjednosti robe. Jačanje bezbjednosti teretnih i putničkih željezničkih sistema u zemlji i smanjenje rizika povezanog sa prevozom bezbjednosno osjetljivih materijala, kao što su otrovni materijali opasni za udisanja, određeni eksplozivni materijali i isporuke radioaktivnog materijala visokog nivoa, su stalni izazov. U tom smislu, Odjeljenje za unutrašnju bezbjednost nastoji da ostvari efikasnu saradnju sa brojnim teretnim prevozncima u zemlji kako bi se osigurala bezbjednost, posebno na železnici. U vezi sa tim, Odjeljenje za unutrašnju bezbjednost je osnovalo i Komitet za javno i privatno partnerstvo javnih i privatnih subjekata radi sprovođenja konsultacija o politici u toj oblasti.

---

[389] Port Authority Warns TSA It Will Be Replaced By Private Security Force Over Long Lines At Airports, *New York CBS*, dostupno na: http://newyork.cbslocal.com/2016/05/09/tsa-port-authority-airports/ .

[390] Ciaramella C. J.: Abolish the TSA, *The Washington Post* (April 16, 2015), dostupno na: https://www.washingtonpost.com/posteverything/wp/2015/04/16/abolish-the-tsa/

[391] Paolino R.C.: All Aboard: Making the Case for a Comprehensive Rerouting Policy to Reduce the Vulnerability of Hazardous Rail-Cargoes to Terrorist Attack, *Military Law Review*, Volume 193, Department of Army Pamphlet, 2007, p. 144

Američke privatne obezbjednosne kompanije se aktivno bave željezničkim saobraćajem, kako teretnim tako i putničkim, kao i tranzitnim obezbjeđenjem na svim nivoima zaštite. Bezbjednost masovnog tranzita doživljava se kao najizraženija oblast rasta privatnih bezbjednosnih firmi u SAD, i procjenjuje se da su u 2016. godini ostvarile prihod od 1,57 milijardi dolara[392]. Kao jedan od primjera, Sekuritas (Securitas) pruža tri nivoa sigurnosti i bezbjednosti železnice, usmjerava saobraćaj na željezničkim objektima, nadgleda parking objekte i pruža usluge službe bezbjednosnog praćenja u određenim okolnostima. Navedena kompanija je intenzivirala aktivnosti u pružanju bezbjednosnih usluga u velikoprodajnim lancima u jednom dijelu SAD[393]. Industrija privatne bezbjednosti bila je posebno uspješna u prelasku u nekad najmanje efikasna područja djelovanja javne policije - zaštitu u sredstvima javnog prevoza. Čini se da privatizacija u ovoj oblasti nije privremena, a kada se ovaj nesporni trend poveže sa povećanjem broja putnika, onda je to prostor u kome postoje još veće mogućnosti za razvoj privatnog sektora[394]. Kao rezultat ovog rasta, dinamika u ovom području bezbjednosti se intenzivira, što se može reći i za teretni železnički transport.

Kao primjer učešća privatnog sektora bezbjednosti u SAD, poznat je primjer Amtraka (Amtrak) koji sprovodi niz mjera u cilju poboljšanja bezbjednosti na železnica. Iako ima svoju policijsku jedinicu, Amtrak se oslanja na privatne bezbjednosne partnere na različitim lokacijama i sarađuje sa mnogim od njih na teretnim linijama. U zavisnosti od lokaliteta i drugih faktora, bezbjednosna praksa može biti šematizovana ili posebno dizajnirana. Neki od uobičajenih Amtrak bezbjednosnih protokola su uniformisani policajci i mobilni timovi obezbjeđenja, slučajni pregled putnika i ručnog prtljaga, korišćenje K-9 jedinice, provjere i pregled prtljaga, bezbjednosne provjere i provjera identiteta. Pored navednog, koriste se i specijalizovane mobilne taktičke jedinice koje vrše slučajne pretrage prtljaga i druge bezbjednosne radnje. Odredi mobilnih tima imaju različiti sastav, uključujući naoružanu specijalizovanu Amtrak policiju, jedinicu za detekciju eksploziva (K-9) i naoružane specijalne agente za borbu protiv terorizma u taktičkim uniformama. Mobilne jedinice su razvijene u saradnji sa saveznim, državnim i privatnim industrijskim sektorima radi poboljšanja bezbjednosti. Amtrak aktivno učestvuje i u Zajedničkoj radnoj grupi za borbu protiv terorizma (Joint Terrorism Task Force) u različitim regionima zemlje[395].

Kao što kontaminacija vode ima ogroman uticaj na javno zdravlje nacije, takav je slučaj i sa snabdijevanjem hranom. I ovdje postoji širok potencijal za nanošenje štete značajnom dijelu stanovništva. U tom smislu, poljoprivreda i prehrambeni sistemi su ranjivi na bolesti, štetočine ili otrovne agense koji se javljaju prirodno, odnosno nenamjerno, ili namjerno, kada su ranjivosti povezane sa terorističkim aktima. Američki poljoprivredni i prehrambeni sistem je obiman, otvoren, međusobno povezan, raznolik i sa složenom strukturom. Odgovornost za snabdijevanje hranom u SAD, pored privatnog bezbjednosnog sektora, imaju i tri državne agencije: Ministarstvo poljoprivrede, Agencija za životnu sredinu i Odjeljenje za unutrašnju bezbjednost.

---

[392] Spencer I.: Mass Transit Security Market on Track for Big Growth, Security Systems News January 2015, p. 2.

[393] *Securitas International, Case Study: Sound Transit*, Western Washington State, dostupno na:http://www.securitasinc.com/globalassets/us/files/casestudies/updated-case-studies/case-study---sound-transit.pdf

[394] Roberts M.: Keeping Mass Transit Ahead of the Curve, *Security Management*, ASIS International, November 2005, pp. 83-89

[395] *Partners for Amtrak Safety and Security*, Protecting America's Railroad, dostupno na: https://pass.amtrak.com/resources.html

Poljoprivredna industrija je izložena bezbjednosnim implikacijama koje su vezane za hranu i vodu, što prirodno u prvi plan ističe potrebu adekvatnog bezbjednosnog sistema i protokola neophodnih za ostvarivanje uspjeha na ovom tržištu. Ovo naročito važi za nerazvijena područja u svijetu, gdje siromaštvo i gladovanje hranu čine oružjem. Iako u Sjedinjenim Američkim Državama postoji najmanje desetak glavnih dobavljača poljoprivrednih proizvoda, svaki od njih izazove bezbjednosti hrane razmatra na ozbiljan i studiozan način, ponajviše zbog toga što su tu ulozi, ali i potencijalni gubici veoma visoki[396]. Vlada zauzima centralno mjesto u zaštiti opskrbe hranom u SAD, pri čemu Ministarstvo poljoprivrede preuzima vodeću ulogu. Za predmetno ministarstvo, zaštita i integritet američke poljoprivredne proizvodnje i snabdijevanja hranom su od suštinskog značaja za zdravlje i dobrobit domaćeg stanovništva i zajednica širom svijeta u koje se prehrambeni proizvodi izvoze[397].

Precizno definisanje kako obezbijediti bezbjednost u poljoprivrednoj sferi na području SAD nije jednostavan posao. Pored širokog asortimana proizvoda i usluga, postoji dodatna dilema višestruke odgovornosti agencija. Dok je za Ministarstvo poljoprivrede možda u prvom planu kreiranja politike vezane za hranu, na njenu sigurnost utiču brojne druge agencije, poput Uprave za hranu i ljekove (*U.S. Food and Drug Administration - FDA*) i Agencije za zaštitu životne sredine, koje imaju razrađene različite protokole vezane za bezbjednost hrane. U određenom smislu, pitanje bezbjednosti hrane, ocjenjuje se u svijetlu terorističkih akcija ili masovne kontaminacije, a znatno manje u pogledu prirodnog kvarenja ili gubitaka.

Miješanje djelovanja različitih agencija sa specifičnim pristupima sigurnosti bio je izazov za one koji štite snabdijevanje hranom u SAD. Drugim riječima, privatno obezbjeđenje i službenici agencija za sprovođenje zakona će probleme sa hranom vidjeti na različite načine. Dok će ih FBI ili carina posmatrati kroz prizmu primjene zakona, stručnjaci za bezbjednost hrane u Ministarstvo poljoprivrede ili Uprave za hranu i ljekove mogu vidjeti stvari iz drugačije perspektive. U vezi sa tim, Program strateškog partnerstva za agroterorizam (*Strategic Partnership Program on Agroterrorism - SPPA*) otklanja različite vizije i objedinjava različite perspektive u jedan okvir , koji se fokusira na sigurnost hrane. Podjednako kritično, predmetni program razmatra i privatnu industriju, od poljoprivrednika do prerađivača žita, od vlasnika stoke do kompanija za proizvodnju đubriva[398]. Uz ostale ciljeve koji su postavljeni pred Program strateškog partnerstva za agroterorizam, jedan od njih je da osigura podsektorski izvještaj u cilju utvrđivanja ranjivosti nacionalne kritične infrastrukture u ovom segmentu kao podršku Nacionalnom planu zaštite infrastrukture.

Kao hrana i voda, postrojenja i rezervoari za vodu, predstavljaju dio kritične infrastrukture, koja je široko rasprostranjena i čije eventualno uništenje ili zagađenje može prouzrokovati velike štete. Kao odgovor na napade 11. septembra 2001. godine, Agencija za zaštitu životne sredine (Environmental Protection Agency ERA) je formirala Odjeljenje za bezbjednost vode (Water Security Division - WSD) u okviru Kancelarije za podzemnu i pitku vodu (Office of Ground Water

---

[396] No free Lunch: Agribusiness and Risks to Food Security, dostupno na: http://www.preventionweb.net/english/hyogo/gar/2013/en/gar-pdf/chap10.pdf

[397] U.S. Department of Agriculture, Pre-Harvest Security Guidelines and Checklist, Government Printing Office, Washington, DC: U.S., 2006, pp. 3-5, dostupno na:http://www.usda.gov/documents/PreHarvestSecurity_final.pdf

[398] U.S. Food and Drug Administration, *Strategic Partnership Program Agroterrorism* (SPPA) Initiative: Final Summary Report, September 2005–September 2008, Appendix A, dostupno na: http://www.fda.gov/downloads/Food/FoodDefense/UCM181069.pdf

and Drinking Water)[399]. Industrija privatnog obezbjeđenja igra ključnu ulogu u zaštiti vodnog svijeta i pripadajućih vodnih dobara, posebno zato što ovi sistemi mogu biti preveliki da bi ih bilo koji vladin ili privatni entitet mogao u potpunosti nadgledati[400]. Primjer navedenom možemo naći u zaštiti brane Huver (*Hoover Dam*), kao i kod ogromih objekata za vodu u Denveru, Kolorado, u periodu 2014.-2016. godine[401].

Kao i sa prethodnim, donekle je slična situacija i sa energetskim sektorom, koji je jedan od najvažnijih u području kritične infrastrukture. Iz tih razloga se kao imperativ nameće da se za slučajeve katastrofa ili terorističkih napada iznađu precizna i izvediva rešenja. Kao što je poznato, energetski sektor je povezan sa mnoštvom drugih sektora što ga čini još značajnijim i ugroženijim od većine ostalih djelova kritične infrastrukture. Sa aspekta bezbjednosti, energetski sektor je posebno specifičan jer, na primjer, bezbjednost terminala za skladištenje nafte i postrojenja za njenu preradu zahtijeva znatno drugačije protokole od obezbjeđenja šipki za gorivo i plutonijumskih otpada u nuklearnoj elektrani. Rafinerije neprekidno traže specijalizovano osoblje za osiguranje visoko složenog i jednako opasnog okruženja u kojem se proizvodi i pakuju(nafta i gasovi) za potrebe isporuke. Na nivou rafinerije, mogućnosti za prirodne katastrofe i katastrofe koje uzrokuje čovjek su jasno vidljive. Većina kompanija ulaže u segmente zaštite koji omogućavaju pažljivo praćenje neovlašćenih aktivnosti i nadzor zaposlenih za koje postoje indicije da djeluju sa neprimjerenim ili sumnjivim motivima. Pored toga, rafinerijske instalacije moraju biti zatvorene u prirodnim katastrofama prvenstveno zbog uticaja na životnu sredinu. Privatni sektor bezbjednosti je uključen u zaštitu kritične inrastrukture energetskog sektora na različite načine. To su prvenstveno usluge procjene korporativnog rizika u borbi protiv unutrašnjih i spoljnih prijetnji, angažovanje u operacijama, istraživanjima i razvojnim programima. Pored toga privatni sektor nudi rešenja za bezbjednosnu tehnologiju koja uključuju platforme za izvještavanje o incidentima, kontrolu pristupa, upravljanje objektima, daljinski sistem zaštite, nadgledanje alarma kao i mogućnosti reakcije. Tu je i sistem upravljanja bezbjednosnim sistemima koji pružaju nadzor ulaska, provjeru identiteta posjetilaca, upravljanje video uređajima i alarmima, mobilne aplikacije i druga rešenja. Na kraju tu su i konsultantske usluge koje pomažu u ispunjavanju zahtjeva vladine regulative, uključujući bezbjednosnu ranjivost, kao i procjene, bezbjednosne planove i slično[402].

Kritična infrastruktura podrazumijeva veliku odgovornost onih kojima je povjerena zaštita aerodroma, mostova, tunela, brana i elektrana, jer sve ove strukture imaju centralnu ulogu u socijalnoj, ekonomskoj i vojnoj odbrani SAD-a. Pored navednih i drugi objekti, kao što su hemijska ili nuklearna postojenja i električne instalacije i sistemi, posebnu su izloženi opasnostima ugrožavanja ili oštećenja. Zbog toga je uloga privatnog obezbjeđenja koje osigurava bezbjednost i nesmetano poslovanje tih sistema nezamjenljiva. Skoro sve velike kompanije za obezbjeđenje nude i usluge zaštite kritične infrastrukture. Uloga privatnog sektora bezbjednosti u zaštiti institucija, njihovog

---

[399] U.S. Environmental Protection Agency, *Information about Public Water Systems*, dostupno na: http://www.epa.gov/dwreginfo/information-about-public-water-systems

[400] Oregon Health Authority, *Physical Security for Drinking Water Facilities*, 2009, dostupno na: https://public.health.oregon.gov/HealthyEnvironments/DrinkingWater/Preparedness/Documents/PhysicalSecurity-Oregon.pdf

[401] *Denver Board of Water Commissioners, Agreement for Armed Security Guard Services at Denver Water Facilities* (April 9, 2014), at http://www.denverwater.org/docs/assets/CF9D67A3-AAE5-1B28-92C82953B0D8C0A5/IIc.pdf .

[402] Nemeth P. C.: *Private security: an introduction to principles and practice*, Taylor & Francis Group, 2018, p. 543

osoblja i imovine jedna je od najistaknutijih funkcija ove grane industrije. Ona je od svojih ranih dana bila glavni akter u zaštiti objekata i prostora, bilo da se radi o industrijskim postrojenjima, javnim događajima, sportskim takmičenjima ili obrazovnim ustanovama. Usluge institucionalne bezbjednosti od strane aktera privatnog sektora mogu se koristiti u zatvorskim objektima, sudnicama, kongresnim centrima ili na sajamskim manifestacijama. Činjenica je da jednostavno postoji previše različitih vrsta poslova bezbjednosti i zaštite da bi ih bilo koji javni sistem mogao u potpunosti pokriti. Budućnost privatne bezbjednosti unutar kritične infrastrukture SAD čini se vrlo perspektivnom, s obzirom na dugu istoriju funkcionisanja i uspostavljene odnosa između javnog i privatnog sektora kao i ograničenih resursa vlade u tom području. Sve dok infrastruktura ima potencijal ostvarivanja široko rasprostranjenog ili masovnog uticaja u ekonomskom, socijalnom, kulturnom, političkom i komunalnom smislu, potrebe za angađovanjem privatnog sektora bezbjednosti će se vjerovatno povećavati.

4.3.1.3. Operacija „Saradnja“ (*Operation Cooperation*)

Operaciju „Saradnja“ finansira Zavod za pravnu pomoć Ministarstva pravde SAD, uz podršku Američkog društva za industrijsku bezbjednost (ASIS), Međunarodne asocijacije šefova policija (IACP) i Nacionalnog udruženja šerifa (NSA). Pokrenuli su je praktičari koji su uočili prednosti javno-privatnog timskog rada, udruživanja snaga za prevenciju, sprečavanja i rešavanja kriminalnih akata. Kretanja u poslednjih nekoliko godina definitivno idu u pravcu partnerstva, s obzirom na stalno povećanje broja programa partnerstva i tendencije daljeg rasta. Na navedeni rast posebno je uticalo enormno povećanje veličine i sofisticiranosti privatne bezbjednosti, tako da je u ukupnoj bezbjednosti privatna bezbjednost postala veliki igrač. S druge strane, rad policije u zajednici kao opšteprihvaćeni koncept, po svojoj prirodi poziva na uspostavljanje partnerstva i zagovara potrebu što potpunije saradnje sa privatnom bezbjednošću kao prirodnim partnerom. Jedna od prednosti partnerstva je i to što može biti uspostavljena na različite načine, kao formalna ili neformalna, opšta ili specifična po linijama rada, lokalna, regionalna i nacionalna. U tom kontekstu, njihova osnovna funkcija je zaštite života i imovine[403].

Partnerstvo može predstavljati saradnju između agencija za sprovođenje zakona i privatnog obezbjeđenja, ili između agencija za sprovođenje zakona i šireg poslovnog sektora, uključujući više od bezbjednosnih operacija. Kada su u pitanju agencije za sprovođenje zakona, saradnja može obuhvatiti ne samo opštinske policije i šerife, već i državnu i saveznu policiju i policijske akademije i kampove za obuku. Saradnja može biti uređena i između jedne kompanije i lokalne policije, ili između federalne agencije i kompanija širom zemlje.

Kao povod za uspostavljanje partnerstva, Savjetodavno vijeće za privatnu bezbjednost (*Private Security Advisory Council*) okarakterisalo je rad policije kao funkciju od javnog interesa. Međutim, javna policija ima širok spektar odgovornosti za zaštitu suštinskih javnih pitanja i njihovi napori su neposredno povezani za zakonom propisanim dužnostima i krivično-pravnim sistemom. Zbog toga je policija, između ostalog, opterećena zakonskim ograničenjima, jer mora da tumači i primjenjuje određene smjernice u vršenju svojih dužnosti na sprovođenju zakona. S druge strane,

[403] Marjanović M.: Partnerstvo između privatnog i javnog sektora bezbednosti, u:*Suprotstavljanje savremenim oblicima kriminaliteta –analiza stanja, evropski standardi i mere za unapređenje,Zbornik radova*, Kriminalističko-policijska akademija, Beograd, 2015, str. 277-278

javna policija je dodatno ograničena javnim proračunima i procesima finansiranja. Politike upravljanja policijom i administrativna hijerarhija u većini glavnih policijskih uprava moraju da procijene i rasporede svoje resurse u skladu sa potrebama i zahtjevima koji trenutno djeluju u okviru njihove strukture u zajednici. To su ujedno i razlozi, zbog kojih se očekuje da kooperativni poduhvat sa privatnim policijskim sistemom doživi rast i i procvetat u narednom periodu. U vezi sa tim, očekivanja su da javne policijske snage efektivno iskoriste svoje postojeće resurse udruživanjem snaga sa policijom privatnog sektora[404].

Pored navedenog, često se ističe činjenica da je jedna od tradicionalnih funkcija javne policije odvraćanje od kriminala, premda je u stvarnosti njihova sposobnost da to učine drastično ograničena. Tako, na primjer, policija ima malo ovlašćenja da mijenja uslove koji podstiču i doprinose ispoljavanju kriminala na određenom prostoru. S druge strane, privatne bezbjednosne snage mogu ponekad drastično da izmijene okruženje u kome djeluju. Kao primjer navedenom, može se pomenuti instaliranje detektora provala, postavljanje osvetljenja, određenih barijara i slično. Pored toga, privatni sektor direktno određuje svoje aktivnosti, odlučuje ko će biti zaposlen u kompaniji, sprovođenje unutrašnjih kontrola potencijalnih radnika i slično. Privatne bezbjednosne organizacije (uključujući bezbjednosne firme i odjeljenja za bezbjednost korporacija) sve više pružaju usluge koje tradicionalno pružaju javne službe za sprovođenje zakona. U mnogim slučajevima, vladina tijela sklapaju ugovore za pojedine usluge, kako bi se smanjili troškovi ili povećala pokrivenost, u okolnostima kada su lokalne službe za sprovođenje zakona preopterećene[405].

Praksa je ukazala da se saradnja između javnog i privatnog sektora bezbjednosti mora proširiti i izvan razmjene informacija na određenom prostoru. Proaktivni bezbjednosni napori i inicijative za planiranje u vanrednim situacijama takođe bi trebalo da uključuju sve koji su zainteresovani za bezbjednost. Dok kompanije svih vrsta sprovode planove prevencije i reagovanja na sve, od nasilja na radnom mjestu do prirodnih katastrofa, stručnjaci za bezbjednost preporučuju učešće lokalnih agencija za sprovođenje zakona i odgovarajućih stručnih lica. Uključivanje svih u planiranje i obuku omogućiće da planovi sadrže realnije situacije, a takođe će pomoći da se osigura njihova efikasnija primjena kada se dogodi najgori scenario. Praksa je pokazala da prirodne katastrofe takođe vode povećanom angažovanju privatnih bezbjednosnih kompanija, kojima se povjeravaju usluge koje tradicionalno pružaju službe za provođenje zakona. Kada je uragan Katrina u avgustu 2005. godine pogodio i jednice oružanih snaga SAD-a (Inženjerski vojni korpus u Nju Orleansu) zatražena je pomoć od firme za obezbjeđenje za 15 naoružanih stražara za zaštitu objekata i sredstava, jer su pripadnici te jedinice bili raspoređeni na kontroli brane za barže na rijeci Misisipi. Jedan od primjera je i da je tokom posjete Predsjednika SAD Nju Orleansu za vrijeme prirodne nepogode, bezbjednosne usluge u obezbjeđivanju šireg rejona vršila privatna bezbjednosna kompanija.[406]

[404] Hodgson K.:*SIA Update* (Oct. 14, 2011), dostupno na:http://www.securityinfowatch.com/article/10506940/sia-update
[405] Nemeth P. C.: *Private security: an introduction to principles and practice*, Taylor & Francis Group, 2018, p. 69
[406] *Operation Partnership, Trends and Practices in Law Enforcement and Private Security Collaborations*, U. S. Department of Justice, 2009, p. 48

4.4. Javno-privatno partnerstvo u zaštiti kritične infrastrukture Ujedinjenog Kraljevstva

Kao što je to slučaj i kod drugih država, i u Ujedinjenom Kraljevstvu nacionalnu infrastruktura sačinjavaju oni objekti, sistemi, veb lokacije (informacije), ljudi, mreže i procesi koji su neophodni za funkcionisanje jedne države i od kojih zavisi svakodnevni život. Pored toga, ta infrastruktura uključuje i neke funkcije, lokacije i organizacije koje nisu kritične za održavanje osnovnih usluga, ali kojima je potrebna zaštita zbog potencijalne opasnosti, kao što su nuklearna i hemijska postrojenja. U Velikoj Britaniji je definisano trinaest nacionalnih infrastrukturnih sektora: hemijska postrojenja, nuklearna postrojenja, odbrana, hitne službe, energija, finansije, hrana, vlada, zdravstvo, svemir, transport i voda. Nekoliko sektora ima i podsektore, pa tako u okvir hitne službe spadaju policija, hitna pomoć, vatrogasna služba i obalska straža. Svaki sektor pokriva jedno ili više nadležnih državnih odjeljenja odgovornih za njegovo funkcionisanje, odnosno za obezbjeđenje zaštite i bezbjednost kritične infrastrukture[407].

Kada se analizira problematika zaštite kritične infrastrukture u Ujedinjenom Kraljevstvu, iskristalisane su dvije najvažnije prijetnje - fizički napadi na instalacije i elektronski napadi na računare ili komunikacione sisteme[408]. Pored navedenog, britanski pristup posebno tretira operatore kritične infrastrukture koji su zaduženi za pružanje usluga, a takođe imaju i neposrednu ulogu u kriznim situacijama, a s druge strane promoviše hitne službe, lokalne vlasti, zdravstvene organizacije i slične službe[409].

4.4.1. Normativni i institucionalni okvir

Centar za zaštitu nacionalne infrastrukture (*Centre for the Protection of National Infrastructure - CPNI*), osnovan je 1. februara 2007. godine u cilju adekvatne zaštite britanske kritične infrastrukture od fizičkih i elektronskih napada. Pored toga, Centar pruža integrisane bezbjednosne savjete (kombinujući savjete vezane za informacionu, kadrovsku i fizičku zaštitu) kompanijama i organizacijama koje čine nacionalnu infrastrukturu. Davanjem savjeta i uputstava štiti se i nacionalna bezbjednost, jer se time smanjuje ugroženost nacionalne infrastrukture od terorizma i drugih prijetnji. Pored navednog, Centar dijeli relevantne informacije sa svojim partnerima, poput upozorenja o specifičnim prijetnjama i ranjivostima, kako bi operatori mogli da preduzmu odgovarajuće mjere zaštite, kao i periodične procjene prijetnji od elektronskih napada. Centar pruža savjete nacionalnim organizacijama za infrastrukturu na različite načine, uključujući organizovanje sastanaka sa timovima sektorskih i specijalizovanih savjetnika, sprovođenje obuke, informacije na internet sajtovima i pisane materijale savjetodavnog karaktera. Savjeti Centra su integrisani u različite fizičke, kadrovske i informaciono-bezbjednosne discipline, kako u skladu sa zahtjevima korisnika, tako i polazeći od dostignutih stručnih saznanja o tome kako nacionalnu infrastrukturu učiniti manje ugroženom[410].

---

[407] Centre for the protection of National Infrastructure, Critical National Infrastructure, dostupno na: https://www.cpni.gov.uk/critical-national-infrastructure-0

[408] Voeller G. J.: *Wiley handbook of science and technology for homeland security*, John Wiley & Sons, Inc, New Jersey, 2010, p. 883

[409] Nadav M.:*Comparative homeland security : global lessons,* John Wiley & Sons, Inc., New Jersey, 2011, p. 269

[410] *Center for the Protection of National Infrastructure, What We Do,* dostupno na: http://www.cpni.gov.uk/About/whatWeDo.aspx

Svoje nadležnosti Centar realizuje preko vladinih odjeljenja koja imaju opštu odgovornost za obezbjeđivanje i preduzimanje odgovarajućih mjera za unapređenje zaštite i bezbjednosti u svojim sektorima. Ta odjeljenja su takođe zadužena za identifikaciju kritične infrastrukture unutar svojih sektora, a u konsultacijama sa Centrom i sektorskim organizacijama. Pored navednog, Centar za zaštitu nacionalne infrastrukture ostvaruje saradnju sa Vladom, lokalnim zajednicama (hitne službe), Odjeljenjem za životnu sredinu, hranu i ruralne poslove (snabdijevanje hranom i vodom), Odjeljenjem za saobraćaj (hitne službe, transport), Ministarstvom zdravlja (hitne službe, zdravlje), Agencijom za standard hrane (bezbjednost hrane), Pomorskom i obalskom stražom (hitne službe) i drugi. Posebno je značajna uspostavljena saradnja sa policijom, prvenstveno sa Nacionalnim uredom za borbu protiv terorizma (National Counter Terrorism Security Office - NaCTSO) koji je koncipiran zajedno sa Nacionalnom mrežom specijalnih policijskih savjetnika za borbu protiv terorizma *(Counter Terrorism Security Advisers - CTSAs*) koji pružaju savjete u vezi za zaštitom kritične nacionalne infrastrukture.

Kada je riječ o javno-privatnom partnerstvu, Centar aktivno promoviše razmjenu informacija, pri čemu se rukovodi pretpostavkom da je dijeljenje informacija o rizicima korisno i za javni i privatni sektor. Na taj način je stvoren mehanizam putem kojeg jedna kompanija može učiti iz iskustava, grešaka i uspjeha drugih, bez straha da će osjetljive informacije biti dostupne medijima ili konkurenciji. Uspješnost razmjene informacija zasnovana je na ličnom povjerenju predstavnika koji dijele informacije na povjerljivim sastancima. Posredujući u održavanju neposrednih sastanaka, Centar pomaže u izgradnji zajednice kojoj vjeruje i sa kojom ima zajednički interes. Svaka organizacija članica može imati najviše dva predstavnika u ovom tijelu, bez mogućnosti da sastancima prisustvuju zamjenici predstavnika, jer u takvim okolnostima nije dozvoljena razmjena osjetljivih informacija.

Pored navedenog Centra, postoji i Savjet za upozoravanje i izvještavanje (*Warning Advice and Reporting Points - WARPs*) kao drugi način organizacije razmjene informacija, s tim što Savjet ima prvenstveno značaj u zajednici gdje članovi mogu da primaju i dijele najnovije savjete o prijetnjama o bezbjednosti informacija, incidentima i rešenjima. Trenutno, aktivnosti Savjeta za upozoravanje i izveštavanje se odvijaju na nivou lokalne samouprave, javnih službi, kompanija i volonterskih udruženja i ogranaka međunarodnih organizacija[411]

U okviru svih policijskih snaga u Velikoj Britaniji postoje stalni savjetnici za borbu protiv terorizma (*Counter terrorism security advisors - CTSAs*). Centralna nacionalna kancelarija za borbu protiv terorizma (*National Counter Terrorism Security Office - NaCTSO*), obučava i podržava CTSAs u pružanju obavještajnih podataka o prijetnjama privatnom sektoru i u pružanju savjeta u vezi sa antiterorističkim praksama. Sa svoje strane, CTSAs daju savjete i podršku u vezi sa pitanjima kao što su prijetnje podmetnutim bombama, pretresi zgrada, evakuacija, planiranje u vanrednim situacijama, teroristički incidenti, postupanje sa sumnjivim paketima, bezbjednost objekata, zaštita kritične imovine i sprečavanje kupovine opasnih materija od strane sumnjivih osoba. CTSAs imaju zadatak i da identifikuju ranjive lokacije i industrije i da pomognu u odabiru „pouzdanih kontakata“ unutar ovih lokacija i industrija, kojima će biti dozvoljeno da imaju uvid u osjetljivije informacije i koje bi

[411] Nacional Cyber Security Centre, *What is a WARP*, dostupno na:https://www.ncsc.gov.uk/information/what-warp

trebalo da sarađuju sa policijom na sačinjavanju planova za njihovu firmu ili objekat u slučaju nepredviđenih situacija[412].

Nacionalna kancelarija za borbu protiv terorizma (*National Counter Terrorism Security Office - NaCTSO*) predstavlja dio Centra za zaštitu nacionalne infrastrukture (*Center for the Protection of National Infrastructure - CPNI*), koji izvještava Udruženje glavnih policijskih službenika (*Association of Chief Police Officers - ACPO*), nevladinu organizaciju koju finansiraju matična kancelarija i lokalna kancelarija policijske vlasti dizajnirane za pružanje uputa za rad policije u zajednici. Udruženje glavnih policijskih službenika koje čine šefovi policije, njihovi zamjenici i pomoćnici, predstavlja značajan neformalni autoritet u sprovođenju politike u toj oblasti. Nacionalna kancelarija za borbu protiv terorizma objavljuje niz vodiča za različite sektore ekonomije koji su dizajnirani tako da pomognu tim sektorima u pripremi planova za vanredne situacije, planova kontinuiteta poslovanja i bezbjednosnih aranžmana. Pored toga, Kancelarija radi i multimedijalne simulacije za učesnike iz različitih privrednih sektora u okviru projekta Argus[413]. Tako, na primjer, Kancelarija sačinjava dokument za zdravstvene ustanove koji vodi menadžere i planere u tim ustanovama kroz proces u četiri koraka. Ti koraci uključuju prepoznavanje prijetnji, utvrđivanje ranjivosti i potreba za zaštitom, identifikovanje mjera za smanjenje rizika, te ponovnu vježbu i reviziju planova za vanredne situacije, planova za vanredne situacije i mere bezbjednosti. Ovo uputstvo se bavi problemima u rasponu od prijetnji, preko otkrivanja neprijateljskog izviđanja do kontinuiteta poslovanja, kontrole pristupa, mjera evakuacije, bezbjednosti osoblja i bezbjednosti informacija.[414]

Nacionalna kancelarija za borbu protiv terorizma izrađuje slične publikacije za pabove i noćne klubove, tržne centre, stadione, bioskope i pozorišta, hotele i restorane, komercijalne centre, škole i druga mesta okupljanja. Centar za zaštitu kritične infrastruktur izdaje i vodiče za planiranje koji su osmišljeni na način da pomognu industrijskim sektorima i pojedinim kompanijama da definišu operativne zahtjeve za sopstvene mjere bezbjednosti. U vezi sa tim, jedan od predloga koje Centar daje zainteresovanim stranama je da najpre izrade „operativni zahtjev nivoa 1“ *(level 1 operational requirement - OR),* kojim treba da definiše fizičku lokaciju, imovinu koju treba zaštititi, percipirane prijetnje, posledice koje nastaju zbog oštećenja imovine, kriterijume za uspjeh u bezbjednosti i moguća bezbjednosna rešenja, a da zatim sačine skup kontrolnih lista na osnovu fizičke lokacije, imovine koja se štiti, prijetnji, posledica i slično. Posle definisanja nivoa 1, zainteresovane strane se podstiču da izrade nivo 2 kojim se detaljnije fokusiraju na svaku oblast sklonu ugroženosti i na moguća rešenja za svako od područja koja su obrađena u operativnom nivou 1. Na primjer, ako je procjenom nivoa utvrđeno da je za objekat potrebna ograda perimetra sa kapacitetima koji omogućavaju pravovremeno otkrivanje, nivo 2 se usredresređuje na probleme kao što su vrsta sistema za otkrivanje uljeza po obodu, osvetljenje, video nadzor i slično[415].

---

[412] Howar P.: *Howard Safe Cities Project. Hard Won Lessons:HowPolice Fight Terrorism in the United Kingdom*, Manhattan Institute for Policy Research, New York, 2004, pp. 8-10

[413] Project Argus, City of London Police, dostupno na: https://www.cityoflondon.police.uk/advice-and-support/countering-terrorism/Pages/project-argus.aspx

[414] Nadav M.: *Comparative homeland security : global lessons*, John Wiley & Sons, Canada, 2011, p.277

[415]*Operational Requirements, Principles of assessing and implementing effective protective security*, Centre for the Protection of National Infrastructures, 2018, pp 9-11

Britanska bezbjednosna služba (MI 5) takođe pruža informacije kompanijama, između ostalog i o načinu sprovođenja procjene rizika, unapređenju bezbjednosnog dijela organizacione kulture, pravilnim bezbjednosnim procedurama informatičke zaštite, provjerama vezanim za zaposlene.

Kancelarija kabineta premijera (*Cabinet Office*) vlade Velike Britanije takođe izdaje odgovarajuća uputstva i metodologije za upravljanje kontinuitetom poslovanja osmišljene da pomognu kompanijama da izrade plan upravljanja kontinuitetom poslovanja (*business continuity management - BCM*). U tom kontekstu, poslovni subjekti se podstiču da prate proces u pet koraka kako bi analizirali uticaj poremećaja na svoje poslovanje i to:

- utvrđivanje prirode ključnih proizvoda i usluga koje kompanija proizvodi i vjerovatnog efekta poremećaja u njihovoj proizvodnji,
- utvrđivanje maksimalnog vremenskog perioda kojim se može upravljati prekidom u ključnim proizvodima i uslugama prije nego što to ugrozi održivost poslovnog subjekta,
- utvrđivanje vremena oporavka (*recovery time objective*) u kojem bi proizvodnja i (ili) pružanje usluga trebalo da budu nastavljeni nakon poremećaja,
- dokumentovanje kritičnih aktivnosti neophodnih za isporuku ključnih proizvoda ili usluga,
- kvantifikaciju resursa potrebnih tokom vremena da bi se održale ključne aktivnosti na prihvatljivom nivou i ispunili ciljevi vezani za vrijeme oporavka (recovery time objective)[416]

Kada je riječ o zaštiti kritične informacione infrastrukture, odgovornost leži na različitim subjektima koji imaju uloge u zaštiti različitih sektora kritične infrastrukture i na taj način doprinose njenoj zaštiti. Predmetne aktivnosti su koordinirane od strane Centra za zaštitu nacionalne infrastrukture, koji uključuje Centralni pokrovitelj za osiguranje informacija (Central Sponsor for Information Assurance - CSIA), Sekretarijat za civilne vanredne situacije (Civil Contingencies Secretariat - CCS), Sektor za bezbjednost u Kabinetu, Odjeljenje za unutrašnju bezbjednost i Vladino sjedište za komunikacije (*Government Communications Headquarters - GCHQ*).

Pored Centra, odgovornost za pružanje savjeta o fizičkoj zaštiti kritične nacionalne infrastrukture podijeljena je i na službe bezbjednosti i policiju. Centralni pokrovitelj za osiguranje informacija (CSIA) je zadužen za širu strategiju osiguranja informacija u Velikoj Britaniji, u okviru svih aspekata informacionog društva. Koordinacija vladinih napora za vanredne situacije i hitne intervencije (bez obzira na uzrok poremećaja) odgovornost je Sekretarijata za civilne vanredne situacije (CCS). Pored toga, postoji nekoliko javno-privatnih partnerstava na polju zaštite informacione infrastrukture, a po tim pitanjima vladina tijela blisko sarađuju sa privatnim sektorom. U okviru toga, Centar za zaštitu kritične infrastrukture dijeli odgovarajuće informacije sa vlasnicima i operatorima kritične infrastrukture.

Centar za zaštitu kritične infrastrukture vodi Kompjuterski tim za reagovanje u hitnim situacijama (*Computer Emergency Response Team - CERT*) za svoje partnere u privatnom sektoru koji upravljaju elementima nacionalne infrastrukture. Ova služba savjetuje kako da se reaguje na incidente i pruža savjete o bezbjednosnim pitanjima Kombinovanom timu za reagovanje na bezbjednosne slučajeve *(Combined Security Incident Response Team - CSIRT UK),* koji prima, pregleda i odgovara na izvještaje o incidentima sa računarskom bezbjednošću, pružajući savjete i srodne aktivnosti za svoje partnere. Važan dio upravljanja rizikom je učenje iz iskustva drugih, a

[416] Business continuity management (JSP 503), Cabinet Office,2011, pp. 6-7

nacionalne infrastrukturne organizacije mogu da kontaktiraju Kombinovani tim o potencijalnim bezbjednosnim ranjivostima, incidentima ili događajima, bilo da su u pitanju elektronski ili fizički incidenti, ili događaji povezani sa osobljem. Primljene informacije tretiraju se povjerljivo, a po potrebi se uklanjaju određeni detalji koji bi identifikovali pojedince ili organizacije kako bi se informacije mogle ugraditi u opšte savjete o bezbjednosti. Na ovaj način se može podijeliti dragocjeno iskustvo i pomoći drugima. Uz ojačavanje tradicionalne uloge CERT-a na pružanje sveobuhvatnih savjeta, uključujući fizička pitanja, pitanja osoblja i elektronike, CSIRT predstavlja centralnu tačku za prijavljivanje bezbjednosnih incidenata i za prijem savjeta i uputstva[417].

Bezbjednosna grupa za komunikacije i elektroniku *(Communications Electronics Security Group - CESG)* je nacionalno tehničko tijelo za osiguranje informacija u okviru sjedišta vladinih komunikacija (*Government Communications Headquarters - GCHQ*), koji je odgovoran unutar vlade za pružanje savjeta i osiguranje informacija organizacijama iz javnog sektora. Ova uloga uključuje pružanje mogućnosti za reagovanje u vanrednim situacijama organizacijama iz javnog sektora kojima će biti potrebna tehnička podrška i savjeti tokom perioda elektronskog napada ili drugih bezbjednosnih incidenata u mreži. Pored navedenog, treba pomenuti i *Get Safe Online*, koji je osmišljen da edukuje javnost o informacionoj bezbjednosti, i ujedno predstavlja rezultat saradnje vlade i kompanija iz privatnog sektora. Pomenuta veb stranica je dostupna od oktobra 2005. godine i nudi sveobuhvatne savjete o bezbjednoj upotrebi interneta za kućne korisnike i mikro preduzeća o tome kako da zaštite računare, mobilne telefone i druge uređaje od elektronskih napada. Cilj ove besplatne usluge je smanjenje pojava krađe ID-a, virusa i neželjene pošte obrazovanjem korisnika interneta i pomaganjem im da zaštite sebe i svoje računare od prijetnji na mreži[418].

U širok spektar organizacija i ustanova zaduženih za zaštitu kritične infrastrukture u Velikoj Britaniji spada i Grupa za elektroničku komunikaciju i otpornost (*Electronic Communication Resilience and Response Group - EC-RRG*) koja je odgovorna za sprovođenje Nacionalnog plana za vanredne situacije za industriju telekomunikacija u Velikoj Britaniji i izradu memoranduma o razumijevanju između industrije i vlade za saradnju u vanrednim situacijama. Telekomunikacione usluge u Velikoj Britaniji reguliše i *Ofcom*, nezavisni regulatorni organ koji je odgovoran Parlamentu i koji, u skladu s odredbama licenciranja, obezbjeđuje da spektar telekomunikacija bude dostupan vojsci za hitne komunikacije[419]

Pored organizacionog aspekta zaštite informacione infrastrukture, Velika Britanija ima i razrađen normativni okvir koga čini veći broj zakonskih akata, od kojih će u ovom dijelu rada biti pomenuti najvažniji. U Zakon o telekomunikacijama iz 1997. godine, koji je zamijenio istoimeni zakon iz 1984. godine, ugrađene su dodatne odredbe o sprečavanju prevara u vezi sa korišćenjem telekomunikacionog sistema[420]. Zakon o zaštiti podataka iz 1998. godine reguliše obradu informacija koje se odnose na pojedince, uključujući dobijanje, držanje, upotrebu ili otkrivanje takvih

[417] Bada M., at all: *Computer Security Incident Response Teams(CSIRTs), An Overview*, Global Cyber Security Capacity Centre, University of Oxford, 2014, pp. 10-11
[418] Get Safe Online Free expert advice, dostupno na:https://www.getsafeonline.org
[419] UK Department of Business Innovation and Skills, National Emergency Plan for the Telecommunications Sector, pp. 3-7, dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61807/emergency-plan-telecomms-sector.pdf
[420] Telecommunications (Fraud) Act 1997, dostupno na: http://www.legislation.gov.uk/ukpga/1997/4/contents

podataka[421]. Zakon o elektronskim komunikacijama iz 2000. godine, predviđa olakšavanje upotrebe elektronskih komunikacija i elektronskog čuvanja podataka. Takođe propisuje izmjene licenci izdatih u skladu sa članom 7 Zakona o telekomunikacijama iz 1984. godine[422]. Zakon o terorizmu iz 2000. godine, iako se odnosi na terorizam na prostoru Sjeverne Irske, definiše i krivično gonjenje i kažnjavanje za određena djela, propisije mjere na očuvanju mira i održavanju reda, a bavi se i namjerno uplitanjem ili ometanjem elektronskih sistema, što se propisuje kao posebno krivično djelo[423]. Zakon o policiji i pravdi iz 2006. godine, sadrži niz odredbi koji se odnose na policiju, kriminal i nerede i ujedno zamjenjuje Zakon o zloupotrebi računara iz 1990. godine[424]. Građanski Zakon o kriznim situacijama (*Civil Contingencies Act*) kao primarni zakon o pripremljenosti i reagovanju, zahtijeva da operatori kritične infrastrukture i javne službe i sektor u cjelini zajedno formiraju lokalne forume za otpornost (*Local Resilience Forums - LRFs*) zasnovane na policijskim nadležnostima kako bi pomogli koordinaciju lokalnog odgovora na vanredne situacije[425]. Svaki sektor kritične infrastrukture treba da funkcioniše u skladu sa postojećim strategijama, te da se povezuje i prima uputstva od nadležnog vodećeg odjeljenja vlade (*relevant lead government department - LGD*). Na primjer, telekomunikacioni operatori sarađuju sa Odjeljenjem za poslovne inovacije i vještine (*Department of Business Innovation and Skills -BIS*) u cilju obezbjeđenja da telekomunikacioni sistemi funkcionišu u vanrednim situacijama i da učinjene greške neće imati kaskadni efekat na ostale elemente sistema. Operatori mobilne telefonije (od kojih je najveći Britanski Telekom - BT) moraju da rade u skladu sa planom za vanredne situacije (*National Emergenci Alert for Telecoms - NEAT*)[426], koji funkcioniše u obliku konferencijskog poziva između provajdera i BIS-a (i regulatornih tijela za komunikacije u drugim djelovima vlade) koncipiranih na način da pružaju informacije o određenom problemu i dijele informacije na nivou vlade i industrije u realnom vremenu.

4.4.2. Privatni sektor bezbjednosti u zaštiti kritične infrastrukture

U srednjem vijeku (od V do XV vijeka), lična i imovinska sigurnost u Engleskoj je bila dostupna prije svega bogatim građanima koji su, uz ostalo, gradili spoljne jarke kako bi zaštitili svoju imovinu od potencijalnih uljeza. U tom periodu građani su sprovodili određeni vid bezbjednosti u zajednici. Tako je sistem desetina i stotina predstavljao strategiju organizacije zajednice koja je koristila rani oblik onoga što danas znamo kao komšijski nadzor u cilju bezbjednosti. Građani su živjeli u zajednicama sličnim današnjim malim gradovima, pri čemu su bili podijeljeni u grupe od po deset porodica, od kojih se svaka zvala desetina. Desetine su takođe bile raspoređene u desetine grupa,

[421] Data Protection Act 1998, dostupno na: http://www.legislation.gov.uk/ukpga/1998/29/contents
[422] *Electronic Communications Ast 2000*, dostupno na: http://www.legislation.gov.uk/ukpga/2000/7/contents
[423] *Terrorism Act 2000*, dostupno na: http://www.legislation.gov.uk/ukpga/2000/11/contents
[424] *Police and Justice Act 2006*, dostupno na: http://www.legislation.gov.uk/ukpga/2006/48/contents
[425] *Civil Contingencies Act 2004: a shortguide*, Civil Contingencies Secretariat, p.4, dostupno na: https://www.cambridge.gov.uk/media/1253/cca-short-guide.pdf
[426] *National Emergency Plan for the Telecommunications Sector*, pp. 5-7, dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61807/emergency-plan-telecomms-sector.pdf

tako da je svaka grupa od sto porodica birala svog šefa sa ovlašćenjem da nadgleda njihovu bezbjednost[427].

U kasnom XIII vijeku u Engleskoj su obični građani i dalje zavisili od bezbjednosti u zajednici. Zakonodavstvo je omogućavalo uspostavljanje noćnih patrola i straža koje su davali muškarci u gradovima u cilju podrške i pomoći naporima lokalnih policajaca da obezbijede bezbjednost. S druge strane bogati preduzetnici nisu uvijek bili zadovoljni nivoom sigurnosti koji su obezbjeđivale regularne snage[428].

U ranoj Engleskoj sprovođenje zakona se smatralo obavezom svih građana. Prije formalnih policijskih odjeljenja, pojedinci zvani hvatači lopova (thief-takers)[429] koristili su se kao vrsta privatnih policijskih snaga u Francuskoj i Engleskoj u periodu XVI do XVIII vijeka. Pomenuti thief-takers su bili privatni građani bez službenog statusa, koje je kralj plaćao za svakog uhapšenog zločinca (slično lovcima na ucijenjene glave američkog Zapada u XIX vijeku). Sve do XVII vijeka drumski razbojnici su uticali da putovanje kroz Englesku bude toliko opasno da se nijedan putnik nije osećao bezbjednim. U vezi sa tim, Parlament je 1693. godine svojim aktom predvidio novčane nagrade za hvatanje drumskih razbojnika, koje su pored novca obuhvatale i dobijanje njihovih konja, oružja i slično.

Sistem thief-takers je osim drumskih razbojnika proširen i na ulična razbojništva i provale, a ubrzo je uspostavljena i klizna skala nagrada. Na primjer, hapšenje provalnika ili pljačkaša (ulični razbojnik) vrijeđelo je isto kao i hvatanje drumskih razbojnika, ali je hvatanje kradljivca ovaca ili dezertera iz vojske donosilo znatno manju nagradu. U pojedinim oblastima su se vlasnici kuća udruživali i nudili dodatne nagrade za hvatanje drumskih razbojnika na njihovom području. Pored toga, tokom ozbiljnih talasa kriminala, Parlament je dodjeljivao posebne nagrade hvatačima lopova koji hapse određene kriminalce. U nizu slučajeva zločinac bi pristao da postane thief-taker da bi od kralja dobio pomilovanje za svoje zločine. Iz tih razloga su mnogi hvatači lopova bili bivši kriminalci[430].

Kompanije i industrije u Engleskoj su tokom industrijske revolucije aktivno uključene u djelovanje privatne policije. Tako je kompanija Crovlei's Iron Vorks, pripremila knjigu propisa Krovelove železare, koja je po formi ličila na građanski i krivični zakonik, sa odredbama koje se odnose na upravljanje i regulisanje položaja zaposlenih. U ruralnim oblastima, bogati vlasnici zemljišta plaćali su čuvare za zaštitu svoje imovine, dok su u malim gradovima trgovci srednje klase formirali dobrovoljna društva za zaštitu koja su jedna drugima pomagala u kontroli kriminala[431].

Sredinom XVIII vijeka u Engleskoj je primijenjen novi koncept sprečavanja kriminala. Inovacije u odgovorima na kriminal stvorile su mnoge promjene u načinu na koji zajednice sprovode svoje napore u oblasti bezbjednosti. U Londonu su grupe stanara u susjedstvu radile na sprečavanju kriminala naoružavanjem i patroliranjem ulicama, osiguravajući da kuće u zajednici budu fizički zaštićene. Ovi pojedinci su progonili kriminalce kroz uske uličice i postali su šire poznati kao trkači.

---

[427] Anson County (NC) Sheriff's Office, „History—The Middle Ages", dostupno na: http://www.ansonsheriff.com/TheOffice/History.aspx

[428] Smith F. C., Schmalleger F., Siegel J. L.: *Private Security Today*, Pearson Education, 2017, p. 4

[429] Pojam thief-takers - privatni građani koji su zarađivali za živothvatanje traženih kriminalaca. Oni su plaćeni prvo za svakog uhapšenog kriminalca, a kasnije i zauspešna osuda kriminalaca.

[430] Nemeth C.P.: *Private security : an introduction to principles and practice*, Boca Raton, CRC Press, 2018, p. 6

[431] Critchley T. A.: *History of Police in England and Wales*, 2nd edition, Legend, 1978, p. 28.

Ova volonterska služba je evoluirala u prvu detektivsku agenciju u Engleskoj, poznatu kao *Bov Street Runners*. Henri Filding, koji je živio u ulici Bov, formirao je grupu plaćajući aktivne i bivše policajce za lociranje i hapšenje ozbiljnih prestupnika. Iako je njihova motivacija bila slična lopovima i drugim kriminalcima, uz Fildingov nadzor, grupa je postajala sve organizovanija i profesionalnija[432].

Uporedo sa sve većom urbanizacijom i industrijalizacijom, London je bio suočen sa nabujalim kriminalom na ulicama, što je pokrenuo ozbiljne debate i zahtjeve za formiranjem profesionalne policije. Iako je na terenu sasvim sigurno bilo dovoljno krivičnih djela da opravdaju formiranje policije, većina građana Londona u početku nije željela formalno ustrojenu profesionalnu policiju iz dva bitna razloga. Naime, mnogi građani su smatrali da će policijske snage ugroziti njihovu tradiciju slobode, a sa druge strane, postojalo je veliko povjerenje u zasluge i sposobnosti aktera privatne bezbjednosti, zbog čega nijesu željeli da u te svrhe troše javna sredstva. Pored toga, pojedini trgovci su angažovali čuvare da vode računa o njihovoj imovini. Trgovačka udruženja su formirala trgovinsku policiju kako bi čuvala prodavnice i skladišta. Stanovnici različitih kvartova u koje su bili podijeljeni veliki gradovi Engleske angažovali su parohijalnu policiju. Pored toga, bila je uobičajena praksa da i sami građani nose oružje radi zaštite[433]. U razvoju odnosa javnog i privatnog sektora u Londonu značajna je i 1828. godina kada je donijet prvi policijski zakon, Zakon o unapređenju policije u metropoli (*The Metropolitan Police Act*).Ovim činom uspostavljena je prva masovna, uniformisana, organizovana, plaćena civilna policija u tom gradu. Iako je predstavljala civilnu snagu, bila je organizovana po vojnim principima, a oficiri su imali prepoznatljive uniforme[434].

U istoriji razvoja privatnog sektora u Velikoj Britaniji, jedan primjer posebno zalužuje pažnju jer predstavlja preteču moderne policije i bezbjednosne industrije. U pitanju je Pomorska policijska ustanova, koja je uspostavljena kao rezultat gubitaka značajnih količina tereta iz londonske luke, tada najprometnije na svijetu. Naime, tada moćna Zapadnoindijska kompanija je finansirala rad privatne bezbjednosne kompanije u cilju smanjenja gubitaka i krađa, a rezultati rada te privatne bezbjednosne službe bili su impozantni. Nakon ovog uspjeha, vlada je usvojila Zakon o morskoj policiji iz 1800. godine, preuzimajući Pomorsku policijsku ustanovu u javne ruke, mada je istu neko vrijeme i dalje finansirala Zapadnonidijska kompanija. Posle uvođenja policijskih reformi, dotadašnja policija rijeke Temze je postala dio nove Metropolitanske policije, i kao takva postoji i danas[435].

Nedvosmislena je činjenica da su vremenom određene uloge koje je izvršavala država postale dio odgovornosti privatnih kompanija, koje svoje usluge ugovaraju sa klijentima i korisnicima, kao i aktera korporativne bezbjednosti. Jedna od prvih specijalizovanih kompanija za poslove zaštite u Velikoj Britaniji bila je *Night Watch Services*, osnovana 1935. godine. Vremenom je ova kompanija, poznatija po novom imenu Securicor, postala jedna od najvećih u sektoru privatne bezbjednosti u toj zemlji. Pedesetih godina XX veka došlo je do značajnog rasta u industriji privatne bezbjednosti. Tada je osnovana firma *Plant Protection*, koja će biti prethodnik današnjih najvećih kompanija za obezbjeđenje. Nakon nekoliko promjena imena, Plant Protection je postala Group 4 Total Security Ltd. Konačno 2004. godine, posle dužeg perioda gdje su se kompanije iz te oblasti gasile ili spajale, Group 4 i Securicor su se integrisali da bi stvorili Group 4 Securicor (poznatija kao G4S), danas

[432] Smith F. C., Schmalleger F., Siegel J. L.: *Private Security Today*, Pearson Education, 2017, p. 4
[433] Dempsey S. J.: *Introduction to Private Security, Second Edition*, Wadsworth, Cengage Learning, 2011, p. 6
[434] Smith F. C., Schmalleger F., Siegel J. L.: Private Security Today, Pearson Education, 2017, p. 5
[435] Bruce G., Simon K.: The History of Private Security and Its Impact on the Modern Security Sector, In: Gill M.: *The Handbook of Security, 2nd Edition*, Palgrave Macmillan, New York,2014, p. 29

najveća privatna bezbjednosna kompanija na svijetu, koja posluje u preko 120 zemalja, sa preko pola miliona zaposlenih i godišnjim prometom od 7,3 milijardi funti u 2012. godini[436].

O značaju i ulozi koju privatne bezbjednosne kompanije imaju na prostorima Velike Britanije govore egzatni pokazatelji iz 2012. godine, vezani za organizaciju Olimpijskih igara u Londonu. Naime, poznata svetska bezbjednosna kompanija G4S je sa organizatorima Olimpijskih igara potpisala ugovor vrijedan 443 miliona dolara[437], koji je između ostalog obuhvatio angažovanje 10.000 pripadnika obezbjeđenja za zaštitu sportista, zvanica i posjetilaca koji su se okupili u Londonu na Ljetnjim olimpijskim igrama[438]. Ovaj veliki poduhvat je pored angažovanja privatnog sektora bezbjednosti obuhvatio i saradnju sa gotovo 13.000 policajaca i više od 18.200 britanskih vojnika koji su bili raspoređeni da čuvaju olimpijske lokacije, aerodrome, hotele i javne prostore. Pored toga, privatni sektor je bio angažovan i na zaštiti informaciono komunikacione infrastrukture Olimpijade. U obavljanju tih zadataka su bili gotovo neprimijetni, omogućavajući nesmetan rad 25.000 novinara i miliona zainteresovanih za trenutni pristup olimpijskom vebsajtu. Inače, troškovi bezbjednosnih operacija tokom pomenutog šestonedeljnog događaja iznosili su više od 897 miliona dolara[439].

Privatni sektor bezbjednosti je u savremeno doba na više načina angažovan u borbi protiv terorizma. Jedan od modaliteta njegovog angažovanja je i ispomoć vojnim snagama na bojnom polju. Međutim, terorističke prijetnje nisu ograničene samo na tradicionalno ratište, što je između ostalog uticalo na uključivanje privatnog sektora bezbjednosti i na drugim lokacijama. To je ujedno i posledica činjenice da je za efikasno suprotstavljanju terorizmu neophodno stvaranje bliskih odnosa između privatnog sektora i lokalnih policijskih snaga kako bi se osiguralo uspostavljanje mehanizama za razmjenu neophodnih informacija. U Londonu, na primjer, kompanije pristupaju mreži privatne bezbjednosti i policije kako bi redovno razmjenjivale informacije radi obavještavanja i dolaska do adekvatnog odgovora na eventualne događaje.[440]

Uspješan rad sa privatnim bezbjednosnim firmama na otkrivanju, odvraćanju i reagovanju na potencijalne terorističke incidente zavisi od uspostavljanja i održavanja povjerenih kontakata u privatnim firmama i razvoja kanala za redovnu komunikaciju. Na primjer, u Londonu Metropolitanska policija održava redovne brifinge za ključne članove poslovne zajednice, u cilju razmjene mišljenja o potencijalnim prijetnjama i davanja smjernica o odgovarajućim bezbjednosnim mjerama. Metroliten policija je takođe kreirala i širi program upozoravanja putem e-pošte i mobilnih aplikacija, koji po potrebi za nekoliko hiljada ključnih poslovnih ljudi u Londonu može proslijediti uputstva u realnom vremenu u slučaju napada ili sumnje na teroristički napad. Obije ove mjere su pomogle da se olakša razmjena obavještajnih podataka između policije i privatnog sektora i da se unaprijedi koordinacija efektivnih planova za vanredne situacije u slučaju napada. Očigledno je da

[436] Bruce G., Simon K.: The History of Private Security and Its Impact on the Modern Security Sector, In: Gill M.: The Handbook of Security, 2nd Edition, Palgrave Macmillan, New York,2014, p. 30

[437] London Olympic Security Contractor Called 'Incompetent' by Panel, *Los Angeles Times, July 17, 2012*, dostupno na: https://latimesblogs.latimes.com/world_now/2012/07/british-olympics-security-contractor-faces-grilling-from-lawmakers-.html

[438] Smith-Spark L.: London's Olympic Security Headache, *CNN International, July 26, 2012*, dostupno na: https://edition.cnn.com/2012/07/26/sport/olympic-security-overview/index.html

[439] Beckford M.:London 2012 Olympics: Met Police Spend 6 Million Pounds on Officer's Accommodation, *The Telegraph, May 9, 2012*, dostupno na: https://www.telegraph.co.uk/sport/olympics/news/9252868/London-2012-Olympics-Met-Police-spend-6m-on-officers-accommodation.html

[440] Smith F. C., Schmalleger F., Siegel J. L.: *Private Security Today*, Pearson Education, 2017, pp. 228-229

su policijsko-poslovna partnerstva posebno važna u oblasti zaštite nacionalne kritične infrastrukture. Razlozi za to su u činjenici da su kreatori politike u Velikoj Britaniji prepoznali da se u modernoj ekonomiji tehnologija i poslovni odnosi tako brzo mijenjaju da postoji stvarna potreba za lokalnim i regionalnim savjetima o potencijalnim ranjivostima. Nakon što se utvrde ove ranjivosti, policija bi trebalo da identifikuje „pouzdane kontakte" na tim mjestima koji će dobiti više povjerljivih obavještajnih podataka nego što je dostupno široj javnosti i koji mogu blisko sarađivati sa policijom na razvijanju planova za slučajeve vanrednih situacija i napada[441].

Izvjesno je da nijedan nivo vlasti, bilo državni ili lokalni, nema mogućnosti da rasporedi dovoljno resursa kako bi zaštitio svaki potencijalni teroristički cilj. Štaviše, kada se te snage suviše koncentrišu, postoji rizik da zaista bitne tačke neće dobiti zaštitu kakvu zaslužuju. Kao rezultat tog uvida, službe bezbjednosti i Nacionalna kancelarija za borbu protiv terorizma, zajedno sa nadležnim vladinim odjeljenjima u Velikoj Britaniji, definisali su prilično rigorozan skup smjernica za klasifikaciju takvih lokacija. Kada je riječ o stanju na terenu, sigurno je da policija i rukovodioci obezbjeđenja na licu mjesta često neće moći da obezbijede adekvatnu zaštitu cijelom objektu. Međutim, radeći sa rukovodiocima obezbjeđenja lokacije, policija bi trebala biti u mogućnosti da sprovede dodatnu analizu i identifikuje najvažnije tačke u objektu koje su ključne za opstanak ili zaštitu lokacije i na taj način štite prostor koji im je povjeren. Iz tih razloga se nakon što policija identifikuje objekte kritične nacionalne infrastrukture moraju uspostaviti stalni odnosi sa tim lokacijama putem „pouzdanih partnera" u okviru organizacije, s kojima će dijeliti obavještajne podatke, razvijati planove za vanredne situacije i koordinirati operacije u slučaju kriza i incidenata. U tom smislu, policija treba da u planiranje vanrednih situacija uključuje i druge relevantne agencije - na primjer, lokalne vatrogasne i zdravstvene službe – u slučajevima kada se suoči sa mjestom koje sadrži opasnost, a koje je van njihove nadležnosti. Jednom kada policija uspostavi povjerljive kontakte, izvrši pregled, odgovori na potencijalne ranjivosti i uspostavi planove za vanredne situacije, trebalo bi uvježbavati i redovno ažurirati te planove kako bi se osiguralo da oni ostanu aktuelni. Dodatna prednost proaktivnog pristupa prepoznavanju i zaštiti lokacija kritične nacionalne infrastrukture je u tome što će ovi odnosi biti korisni u širokom rasponu scenarija u kojima će se očekivati da policija reaguje – teroristički napad, prirodne katastrofe ili teške tehnološke havarije. Bez obzira na to koji se incident dogodio, ako policija ima vjerodostojne planove za reagovanje u vanrednim situacijama za lokalna mjesta kritične infrastrukture koja redovno uvježbava, oni će biti u mnogo boljoj situaciji da reaguju i smanje neizbježni pritisak na svoje službenike u nastaloj situaciji[442].

U skladu sa Zakonom o reformi policije iz 2002. godine, Engleska i Vels aktivno nastoje da podstaknu saradnju između privatnih bezbjednosnih službi i policije putem programa usmjerenog na bezbjednost u zajednici. Navedeno se prvenstveno odnosi na pojedine funkcije privatnog bezbjednosnog osoblja, čuvara i zaštitara, čuvara vozova i slično. Osoblje koje obavlja ove zadatke ima priznat kurs za obuku, mogu nositi posebnu značku i imati pristup posebnim ovlašćenjima kao što su izricanje mandatnih kazni, konfiskacija švercovanog alkohola i duvana. Prema podacima iz 2010. godine, preko 2000 službenika je dobilo akreditaciju za ovu djelatnost. Prednost ovog programa

[441] Howard P.: Hard Won Lessons*: How Police Fight Terrorism in the United Kingdom*, Police Institute at Rutgers University,2004, p. 8, dostupno na: https://media4.manhattan-institute.org/pdf/scr_01.pdf
[442] Ibidem, pp. 8-9

je što omogućava da se na određenim lokacijama (parkovi, tržni centri, bolnice, željeznice) obezbijedi efikasno održavanje reda i mira, čime se policija rasterećuje i omogućava joj se da se koncentriše na važnije zadatke. S obzirom da je pomenuto osoblje privatnog sektora obučeno i osposobljeno, to daje policiji sigurnost i doprinosi povećanom stepenu integrisanosti privatnog sektora bezbjednosti[443].

S druge strane, službenici obezbjeđenja u sudovima u Engleskoj i Velsu su regrutovani iz privatnog sektora i posjeduju širok spektar posebnih ovlašćenja, saglasno odredbama Zakona o sudovima iz 2003. godine. Ti službenici imaju ovlašćenja za pretragu, ovlašćenja za isključivanje i uklanjanje iz prostorije i objekta, ograničavanje pristupa licima, oduzimanje predmeta i slično[444].

Aerodromska bezbjednost, uključujući pregled i pretragu putnika, pregled prtljaga, kontrolu pristupa, bezbjednosne patrole na aerodromu, nadzor i servis ostavljenih, izgubljenih i pronađenih stvari, samo su neki od zadataka privatnog sektora bezbjednosti u obezbjeđivanju aerodromskog prostora u velikoj Britaniji. Pored navedenog, privatni sektor bezbjednosti je uključen i u druge aktivnosti kojima se sprečavaju određena lica da ugroze bezbjednost putnika i aviosaobraćaja. Evidentno je da je znatan dio rutinske bezbjednosti aerodroma u rukama privatnih zaštitara. S obzirom na značaj nesmetanog funkcionisanja vazdušnog saobraćaja i uloge koje ima privatni sektor bezbjednosti, sva lica koja su anagažovana na obezbjeđenju aerodromskog prostora moraju biti licencirana što podrazumijeva da su adekvatno obučena i osposobljena za obavljanje svoje djelatnosti. U vezi sa tim, prisutan je trend proširenja nadležnosti privatnog sektora, a u skladu sa odgovarajućim odredbama Zakona o krivičnom pravosuđu iz 1991. godine i drugim zakonskim izmjenama[445].

Velika Britanija je poznata kao prva država u pomorskom sektoru privatne bezbjednosti (V. Britanija 40%, Kipar 16%, SAD-6% i ostale države 38%)[446]. Ovaj sektor posluje izvan državne teritorije, a za razliku od američkog modela nisu mu neophodna posebna odobrenja. Britanska vlada se odlučila za samoregulativni pristup zasnovan isključivo na podizanju standarda u industriji bezbjednosti pomoću dobrovoljnih kodeksa ponašanja koje nadgledaju treće strane (npr. Međunarodni kodeks ponašanja i Američki nacionalni institut za standarde - Američko udruženje za industriju, bezbjednosni standardi i slično), te primjeni državnih ugovora kao načina da se podstakne privatni sektor bezbjednosti da se pridržava etičkih i profesionalnih standarda. S obzirom na tradicionalnu britansku otvorenost prema industriji privatne bezbjednosti, nije iznenađenje da je britanska vlada bila među prvima u Evropi u upotrebi privatnog sektora u obezbjeđenju brodskih trgovačkih plovila, kao odgovarajućeg rešenja za prijetnje koje potiču od piraterije, preferirajući ovu opciju u odnosu na vojnu alternativu.[447].

---

[443] Button M.: *State Regulation concerning Civilian Private Security Services and their Contribution to Crime Prevention and Community Safety*, United Nations Office on Drugs and Crime (UNODC). 2014, p. 15

[444] Ibidem, p. 32

[445] Exemptions from Security Industry Authority SIA Licensing, https://www.caa.co.uk/Commercial-industry/Security/Regulation/Exemptions-from-Security-Industry-Authority-SIA-Licensing/

[446] *Privately Contracted Armed Maritime Security*, Ocean Beyond Piracy, dostupno na: http://oceansbeyondpiracy.org/sites/default/files/attachments/Privately_Contracted_Armed_Maritime_Security_IssuePaper.pdf

[447] Cusumano E., Ruzza S.: Security privatisation at sea: Piracy and the commercialisation ofvessel protection, *International Relations, Vol. 32(1),* 2018, pp. 87-88, dostupno na: https://journals.sagepub.com/doi/pdf/10.1177/0047117817731804

Velika Britanija je u savremenom dobu putem Nacionalne strategije za pomorsku bezbjednost definisala rizike poput „poremećaja vitalnih pomorskih trgovinskih pravaca kao rezultat rata, kriminaliteta, piraterije ili promjene međunarodnih normi“, ili „sajber napada protiv brodske ili pomorske infrastrukture“. Britanska vlada radi na promociji najviših standarda, uključujući i zaštitu ljudskih prava, u svim privatnim kompanijama za pomorsko obezbjeđenje. Kancelarija za spoljne i zajedničke odnose podržava britansku službu za akreditaciju na planu sprovođenja programa za akreditaciju sertifikacionih tijela koja će samostalno sertifikovati privatne kompanije za pomorsku bezbjednost (Private Maritime Security Companies - PMSCs)u skladu sa standardima ISO 28000. Na ovaj način se uspostavljaju smjernice privatnim kompanijama za pomorsku bezbjednost koje na zahtjev angažuju naoružano osoblje obezbjeđenja na brodovima[448].

4.4.3. Projekat „Grifin“ (Project Griffin)

Zadatak projekta „Grifin“ je da menadžere, službenike privatne bezbjednosti i zaposlene u javnom i privatnom sektoru savjetuje i informiše o pitanjima bezbjednosti i borbe protiv terorizma, kao i o pitanjima prevencije kriminala. Jedan od polaznih stavova u promovisanju pomenutog projekta je da u čuvanju Londona od prijetnje terorizmom svi moraju da imaju određenu ulogu - ne samo policija i bezbjednosne i obaveštajne službe, nego i cjelokupna zajednica. Inicijativu za projekat „Grifin“ je pokrenula londonska policija, a isti je prvi put uveden u aprilu 2004. godine u centralnom finansijskom i poslovnom dijelu Londona kao zajednička akcija londonske policije i Metropoliten policije, kako bi se pomoglo u zaštiti od terorističkih prijetnji i kriminala. Kao najvažniji ciljevi programa su označeni:

- podizanje svijesti o aktuelnim pitanjima terorizma i kriminala,
- dijeljenje i prikupljanje obavještajnih podataka i informacija,
- građenje i održavanje efikasnih poslovnih odnosa,
- traženje rešenja za suzbijanje terorizma i kriminala,
- održavanje povjerenja u policiju i druge organe i
- omogućavanje i osposobljavanje ljudi da prijavljuju sumnjive aktivnosti i ponašanje.

Kurs koji je povezan s programom uči polaznike različitim vještinama, uključujući: eksplozive, identifikaciju prijetnje, očuvanje mjesta kriminalnog događaja, upravljanje prijetnjom eksplozivnom napravom, upravljanje ABHO, rešavanje konflikata, izviđanje, upravljanje kordonom, strategiju za smanjenje kriminala i pravna pitanja. Učesnici koji završe kurs dobijaju sertifikat i njihovo ime ulazi u policijski registar u slučaju potrebe za njihovim angažovanjem pri većim incidentima ili u vanrednim situacijama. U vezi sa tim, pošlo se od teze da pripadnici privatne bezbjednosti nisu antiteroristički borci, ali se nalaze na liniji fronta. Zbog toga ima smisla da iskoriste svoja zapažanja, vještine i stečeno znanje na obučen i koordinisan način.

Bilo da pomaže da se odvrate ili poremete terorističke ili ekstremističke aktivnosti, ili da se smanji kriminal i pomogne nadležnim službama u hitnim slučajevima ili katastrofama, privatna

[448] *The UK National Strategy for Maritime Security*, 2014, pp. 17, 30, dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/322813/20140623-40221_national-maritime-strat-Cm_8829_accessible.pdf

bezbjednost je pokazala svoju posvećenost tom projektu i podržava svaku priliku da bolje edukuje svoje osoblje kako bi bilo snažnije i na odgovarajući način uključeno u pomaganje da se spriječe veći incidenti. Međutim, ako vlada i policija ne pokažu potpunu posvećenost i ne dodijele odgovarajuća sredstva i resurse kako bi se osigurao dugoročni uspjeh na tom planu, onda se ne može očekivati ni od privatne bezbjednosti da investira više vremena i novca u projekat koji ne pruža dodatnu operativnu korist ili unapređeni nivo angažovanja.

Projekat „Grifin" je alat koji policija i vlada mogu da koriste za obuku i angažovanje privatne bezbjednosti za bezbjedniju zajednicu. Program objedinjuje policiju, vatrogasce, hitnu pomoć, sektor privatne bezbjednosti i druge vladine agencije u odvraćanju i ometanju terorističkih i ekstremističkih aktivnosti, kao i podržavanje rada svake organizacije s lokalnim informacijama i resursima tokom velikih vanrednih situacija. Projekat „Grifin" je sada operativan u 100 policijskih jedinica širom Velike Britanije. Njegova osnovna premisa je da djeluje s partnerima od povjerenja u zajednicama kojima služi. Projekat ima potpunu podršku Vlade i priznat je kao izvor dobre prakse u pružanju strategija i smjernica, podizanju svijesti, borbi protiv terorizma, obezbjeđivanju procedura i politika za prevenciju kriminala. Projekat „Grifin" je dobrovoljna i neprofitna organizacija. Finansiraju ga učesnici: policijske snage, organizacije, poslovne kompanije i bezbjednosni organi privatnog sektora, a njime upravlja Reprezentativni komitet za upravljanje. Kako se projekat „Grifin" razvija, policija, zajednica, kompanije i radnici obezbjeđenja rade zajedno, dijele informacije i koordiniraju svoje aktivnosti. Nakon uspjeha u centralnom Londonu, projekat „Grifin" počinju da prihvataju i druge policijske snage širom Velike Britanije. Proizveo je, takođe, veliko interesovanje i podršku da se usvoji i u inostranstvu, posebno u Kanadi, Singapuru, Južnoj Africi, SAD-u, Australiji i na Novom Zelandu[449].

4.5. Evropska unija i javno-privatno partnerstvo u zaštiti kritične infrastrukture

Trendovi povećanih prijetnji i izazova za evropska društva, koji su se manifestovali poslednjih godina promijenili su, između ostalog, i sam sistem, odnosno strukturu subjekata zaduženih za bezbjednost na prostoru zemalja članica Evropske unije. S druge strane, u uslovima nedostajućih resursa, a posebno ograničenih finansijskih sredstava, poljuljano je povjerenje javnosti u državama članicama EU u sposobnosti i kapacitete javnog sektora bezbjednosti da garantuje odgovarajući nivo bezbjednosti građana i neophodni stepen zaštita privrednih subjekata. Suočene sa sve većim rizicima i kriminalnim prijetnjama, veliki broj poslovnih subjekata se okreće alternativnim modelima zaštite, bilo na način da sami organizuju poslove korporativne bezbjednosti, bilo da tarže usluge specijalizovanih bezbjednosnih kompanija. To su razlozi zbog kojih se poslednjih decenija u Evropi ubrzano razvijaju usluge privatne policije[450] i privatnog obezbjeđenja, što se odvijalo uporedo sa razvojem koncepta rada policije u zajednici[451].

[449] Marjanović M.: Partnerstvo između privatnog i javnog sektora bezbjednosti, u: *Suprotstavljanje savremenim oblicima kriminaliteta – analiza stanja, evropski standardi i mere za unapređenje*, Tom 3, (zbornik radova), Kriminalističko-policijska akademija, Beograd, 2015, str. 226-227

[450] Button M.: *Private Policing*. Willan Publishing, UK, 2002, p. 7

[451] Brogden M., Nijhar P.: *Community Policing*, Routledge, UK, London, 2013, p. 18

Bezbjednosno okruženje se u navedenom periodu radikalno izmijenilo – od sistema sa dominantnim javnim sektorom koji finansira država, do stanja u kome se odgovornost dijeli između javnih i privatnih aktera. Privatna bezbjednost se proširila prvenstveno kao odgovor na povećanu potražnju koja je vezana za građane i privredne subjekte, ali se u novije vrijeme i države obraćaju privatnom sektoru radi pružanja bezbjednosnih usluga, koje su fleksibilnije i jeftinije, a u nekim slučajevima i specijalizovanije nego što je to slučaj sa subjektima javne bezbjednosti. Privatne bezbjednosne kompanije danas igraju sve važniju ulogu u prevenciji i suzbijanju kriminala, upravljanju bezbjednosnim rizicima i pružanju drugih bezbjednosnih usluga na efikasan i racionalan način. Eksponencijalni rast privatne bezbjednost širom svijeta predmet je različitih rasprava koje se tiču državnog suvereniteta, legitimiteta i autoriteta u domenu javnog sektora bezbjednosti. Kada se razmatraju aktuellni odnosi između javnog i privatnog sektora bezbjednosti, u literaturi dominiraju modeli koji naglašavaju takmičarski ili saradnički odnos[452].

Ukoliko se analizira razvoj javno-privatnog partnerstva u oblasti bezbjednosti na nivou EU, može se uočiti da ne postoji univerzalni scenario kako stvoriti zajednički uspješan model, jer nešto što djeluje savršeno u jednoj državi članici, može biti izazovno i teško primjenljivo u drugoj. Do ovakve prakse dolazi uglavnom zbog bezbjednosnih specifičnosti i kulturnih razlika, kao i činjenice da se opšti odnos između javnog i privatnog sektora bezbjednosti razlikuju među zemljama članicama Unije. U nekim državama sa tog prostora, formalna uređenost je najvažniji dio javno-privatnog partnerstva u sektoru bezbjednosti, dok je u drugim zemljama prisutniji pragmatičan pristup. Ipak, pitanja javno-privatnog partnerstva u ovoj oblasti nalaze se na dnevnom redu nadležnih institucija EU i vlada država članica, što im osigurava snažnu političku podršku za dalji razvoj zakonodavstva[453].

Evidentan je trend da se u bezbjednosnom sektoru Evropske unije sve više i više nadležnosti oduzima od javne bezbjednosti u korist privatnog sektora. Kao posledica navednog je i sve veća prisutnost privatnih bezbjednosnih kompanija i privatnih zaštitara u javnom domenu. Razlozi za to su brojni, a između ostalog i:

- sve veći osećaj nesigurnosti među različitim djelovima evropskog društva,
- ograničeni resursi policije i drugih organa javne bezbjednosti,
- sve veći kvalitet i profesionalizam privatnih bezbjednosnih službi, i
- inovativnan i fleksibilan pristup sektora privatne bezbjednosti, koji pruža sve kvalitetnije usluge, dugogodišnje prakse i stručnosti pripadnika[454].

To su razlozi koji potvrđuju da adekvatno definisano, dobro upravljano i nadgledano javno-privatno partnerstvo predstavlja efikasan i djelotvoran koncept, čija primjena pozitivno utiče na bezbjednosno okruženje pojedinca, organizacije, zajednice i države. Da bi bila uspješna, javno-privatna partnerstva moraju da ispune određene kriterijume, koji između ostalog obuhvataju:

- otvoreni dijalog između nadleđnih državnih organ i privatnih provajdera bezbjednosti,
- jasna uputstva u vezi sa ulogom svakog bezbjednosnog partnera,

[452] Hess M.K.: *Introduction to Private Security*, Fifth Edition, Cengage Learning, Wadsworth, 2009, pp. 14-15
[453] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, L 194/1
[454] Dempsey J.:*Introduction to private security*, Wadsworth, USA, 2011, pp. 31-32

- jasan pravni ili ugovorni okvir, i
- redovnu evaluaciju i potrebne korekcije za poboljšanja kada je potrebno[455].

Da bi se ispunili neophodni kriterijumi i da bi se optimizirao uspjeh i efikasnost javno-privatnog partnerstva i ujedno na viši novo podigla zaštita od bezbjednosnih prijetnji (terorizam, ekstremizam, sajber-kriminal i slično), od vitalnog je značaja da svaki bezbjednosni partner u potpunosti razumije svoju ulogu, odgovornosti i ograničenja svojih ovlašćenja. Usled nedostatka specifičnih znanja o ovim elementima, javno-privatna partnerstva u bezbjednosti u Evropi su i dalje nedovoljno razvijena i ne koriste se u mjeri koja osigurava da dostignu svoj maksimalni potencijal[456].

Postoji više razloga za uspostavljanje javno-privatnog partnerstva u oblasti bezbjednosti i zaštite kritične infrastrukture, ali je ekonomski interes najčešći razlog za zaključivanje ugovora o JPP na prostoru EU. U tom kontekstu, uobičajena je motivacija da privatni bezbjednosni sektor učestvuje u saradnji sa javnom sektrom u raznim oblastima bezbjednosti (na primjer, borba protiv sajber kriminala, trgovine ljudima, terorizma i slično). Međutim za uspješnu primjenu javno-privatnog partnerstva potrebno je identifikovati prepreke i stvoriti uslove za rast industrije bezbjednosti i stvaranje uslova za izvoz bezbjednosnih proizvoda i usluga. Jedan od načina rešenja ovog problema je i osnivanje posebnog tijela. Međutim, prepreke se mogu otklanjati i inoviranjem zakonodavstva u području industrije privatne zaštite, koje sužavaju mogućnosti uticaja na procese javno-privatnog partnerstva kako bi isti bili što je moguće više zaštićeni od nepotrebnih ili pretjerano opterećujućih prilagođavanja.

Modeli javno-privatnog partnerstva u evropskim zemljama mogu biti posledica implementacije posebnih zakona koji se bave tim pitanjima kada se to smatra potrebnim, pri čemu vlade država članica EU, uz uvažavanje prihvaćenih standarda, suvereno odlučuju koji je model JPP najpodesniji za primjenu u specifičnim okolnostima koje postoje u svakoj državi. U Regulisanje predmetne oblasti može da uključi i donošenje zakona koji pruža precizan okvir za saradnju između privatne i javne bezbjednosti. U aktuelnoj evropskoj praksi se ova vrsta zakona pretežno uopšteno bavi pitanjima javno-privatnog partnerstva, sa osnovim ciljem podsticanja ekonomije, ali i unapređenja politike bezbjednosti (unutrašnje i spoljne) koja postaje sve važnije pitanje svake od ovih država. Kada je riječ o odnosu sa javnošću, vlade država članica EU omogućavaju sektoru privatne bezbjednosti da pruži doprinos novom zakonodavstvu o bezbjednosti, pružajući mu priliku da bude uključen u saradnju u procesu izrade Strategije nacionalne bezbjednosti ili Strategije unutrašnje bezbjednosti EU. Razlozi zbog kojih bi se sektor privatne bezbjednosti uključivao u takve aktivnosti su prije svega vezani za mogućnost umrežavanja sa vladama i drugim javnim i privatnim subjektima (rad u zajednici), te samim tim dijeljenja znanja, vještina i ekspertiza[457]. Društveni interes je u ovom slučaju posebno važan jer se označava kao pokretačka snaga koja se manifestuje kroz motivaciju za široku diskusiju o bezbjednosnim pitanjima u državama članicama Unije i za postavljanje

[455] Born H., Caparini M., Cole E.: Regulating private security in Europe:status and prospects. Geneva: Geneva Centre for the Democratic Control ofArmed Forces: Policy Paper, No. 20, 2007, pp. 5-6 dostupno na:https://www.dcaf.ch/sites/default/files/publications/documents/PP20_Born_Caparini_Cole_.pdf

[456] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (5th White Paper, Berlin, 23 April 2015). CoESS – Confederation of European Security Services, Belgium, 2015, p. 52 , dostupno na: http://www.coess.org/newsroom.php?page=white-papers

[457] Renewed European Union Internal Security Strategy 2015–2020, approved by the European Council, No. 9798/15, dostupno na: http://data.consilium.europa.eu/doc/document/ST-9798-2015-INIT/en/pdf

bezbjednosti na visokom nivou politike EU.[458] Za privatni sektor bezbjednosti, to je od posebnog značaja jer mu omogućava napredak i razvoj u kontinuitetu.

Iz navedenog se može zaključiti postojanje niza razloga za uspostavljanje javno-privatnog partnerstva u sektoru bezbjednosti. Primarni razlozi su ekonomske i socijalne prirode, ali postoje drugi raznovrsni motivi koji opredjeljuju učešće privatnih i javnih bezbjednosnih subjekata u ostvarivanju zajedničkih interesa (Tabela br.14).

Razlozi privatnog sektora za učešće u partnerstvu	**Razlozi javnog sektora za učešće u partnerstvu**
pristup znanju i informacijama iz javnog sektora (zakonodavstvo EU, borba protiv sajber kriminala, terorizma i slično)	bolje razumijevanje industrije bezbjednosti uopšte
uvjerenje da su proizvodi i usluge kvalitetni, jer to garantuje vlada	stvaranje sinergije između različitih inicijativa privatnog sektora
mogućnost uticaja na nacionalno zakonodavstvo i obavezne standarde	pristup resursima privatnog sektora, što olakšava postavljanje standarda i dobrih praksi
pristup javnim sredstvima	
dijeljenje znanja, iskustava i dobrih praksi	
pomaganje u postizanju otpornosti bezbjednosnog sistema	
povećanje povjerenja između svih subjekata partnerstva, bolja informisanost i proaktivan stav u slučaju bezbjednosnih prijetnji, nesreća i krize	
uspostavljanje direktnih i pouzdanih kontakata sa drugim organizacijama	

Tabela br. 14.: Razlozi za učešće u javno-privatnom partnerstvu

Kao zaključak se nameće to da i pored drugih različitosti i specifičnosti evropskog prostora, tradicija i kulturna dimenzija spadaju u najvažnije odrednice za uspostavljanje, razvoj i funkcionisanje javno-privatnog partnerstva u bezbjednosnom domenu. Usled kulturnih razlika ne postoji univerzalni scenario o tome kako stvoriti uspješan model javno-privatnog partnerstva, jer način na koji se to čini u jednoj neće nužno odgovarati drugoj državi članici. Važna tačka koju treba uzeti u obzir u vezi sa javno-privatnim partnerstvom jeste i da se zakoni, kako na nacionalnom tako i na evropskom nivou, moraju uskladiti, što znači da postojanje modela bezbjednosnog partnerstva treba da bude normativno legitimisano. U suštini, analiza trenutnog regulatornog okvira javno-privatnog partnerstva u bezbjednosnom sektoru zemalja članica EU pokazuje da još uvek nije došlo do usklađivanja zakonodavstva koje se odnosi na segment privatne bezbjednosti na evropskom nivou. Posledica toga je da se nacionalni propisi privatne bezbjednosti razlikuju od države do države i odražavaju različita kulturna okruženja i druge specifičnosti. Takođe, neke oblasti privatne

[458] *Shared Vision, Common Action: A Stronger Europe. Global Strategy for the European Union's foreign and security policy*, High Representative of the European Union for Foreign Affairs and Security Policy, 2016, dostupno na:http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

bezbjednosti su više regulisane od drugih, kao što je to slučaj sa pružaocima usluga aerodromske bezbjednosti. Te usluge su obuhvaćene uredbom EU kojom se uspostavljaju zajednička pravila u oblasti bezbjednosti civilnog vazduhoplovstva, a koja sadrže određena pravila koja direktno utiču na privatno osoblje obezbjeđenja. Primjera radi, Uredba reguliše da će svo osoblje, koje zahtijeva pristup oblastima restriktivnog bezbjednosnog režima, biti podvrgnuto minimalnoj petogodišnjoj provjeri i redovnom obučavanju iz oblasti vazduhoplovne bezbjednosti[459].

I površnom analizom bezbjednosnih strategija na nivou EU otkriva se da se one zasnivaju na relativno širokom razumijevanju bezbjednosti sa obije strane spektra odgovora na prijetnje. Uz to, skoro sve Strategije vezane za bezbjednost na nivou EU usvojene u poslednjoj deceniji ukazale su na ključnu ulogu privatnog sektora kada je u pitanju suzbijanje širokog spektra savremenih bezbjednosnih prijetnji. Kao primjer, napomenimo da su strategije EU potencirale ulogu aktera privatnog sektora u pomorskoj bezbjednosti, uključujući izgradnju kapaciteta, upravljanje rizikom, zaštitu kritične morske infrastrukture i odgovore na krizu[460] prevenciju kriminala[461], zaštitu privatnih podataka, zatvaranje veb stranica sa sadržajem zlostavljanja djece, borbu protiv utaje poreza i korupcije[462]. Nekoliko drugih zvaničnih dokumenata EU takođe zagovara veću ulogu privatnog sektora u istraživanju i razvoju u oblasti bezbjednosti. Tako je i Evropska komisija objavila svoju politiku za industriju bezbjednosti, u kojoj se navodi da „industrija bezbjednosti predstavlja sektor sa značajnim potencijalom za rast i zapošljavanje“[463].

4.5.1. Normativni okvir javno-privatnog partnerstva u zaštiti kritične infrastrukture

Evropska unija i njene države članice su poslednjih godina u svojim dokumentima pozvale na veći angažman privatnog sektora kada je u pitanju suzbijanje različitih savremenih prijetnji bezbjednosti. Na primjer, Strategija unutrašnje bezbjednosti EU iz 2010. godine četiri puta pominje izraz „privatni sektor“, dok izričito naglašava njegov značaj u sprečavanju finansijskog kriminala, nestašice i prekida isporuke energije, ugrožavanja informaciono-komukacione tehnologije i pandemija[464]. Upućivanja na ključnu ulogu privatnog sektora mogu se pratiti i u drugim strategijskim dokumentima na nivou Evropske unije koji se odnose na bezbjednost i akcionim planovima za njihovo sprovođenje. Rastuća uloga različitih aktera iz privatnog sektora bezbjednosti u pružanju sigurnosti prepoznata je i u široj literaturi u društvenim naukama. Sveukupno, uprkos mnogim neslaganjama o njegovom uticaju i posledicama, čini se da postoji široki konsenzus da se na evropskom prostoru odvija pluralizacija bezbjednosti u više oblasti (inter)nacionalne bezbjednosti.

---

[459] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 establishing common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002. Official Journal of the European Union, 2008/L 97/72, dostupno na: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex:32008R0300

[460] *For an open and secure global maritime domain: Elements for aEuropean Union maritime security strategy*, European Commission, 2014, rr.8-9, dostupno na: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52014JC0009

[461] *Specific programme: Preventing and combating crime* (2007–2013), European Council, 2007, art. 3,5, dostupno na: http://publications.europa.eu/resource/cellar/b3df8abe-7038-4cc9-8f8f-21a36eca9998.0005.02/DOC_2

[462] *The Stockholm programme - An open and secure Europeserving and protecting the citizens*, Council of the European Union, 2009, dostupno na: http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf

[463] *Security industrial policy*, European Commission, 2012, p. 2, dostupno na: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF

[464] *Internal security strategy for the European Union*, European Council, 2010, pp.23-24, dostupno na: https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf

Tako privatni, a ne javni subjekti danas snose sve veći dio tereta reagovanja na nove bezbjednosne prijetnje, poput terorizma i organizovanog kriminala.

U različitim dokumentima vezanim za bezbjednost EU, na javno-privatno partnerstvo se često gleda kao na *win-win* rešenja, što važi i za aktere u javnom i privatnom sektoru kada je u pitanju reagovanje na nove bezbjednosne prijetnje. Stvarni rezultati i do sada ostvareni dometi javno-privatnog partnerstva u području bezbjednosti ostaju, međutim, predmet rasprave. Naime, rezultati istraživanja o ulozi privatnih finansijskih institucija u borbi protiv finansiranja terorizma ukazuju na to da javno-privatno partnerstvo ne proizvodi uvijek očekivana rešenja za dobitak ni za javni ni za privatni sektor. Kao razlog navedenom često se ističu neslaganja oko definicije, obima i metoda analize prijetnje terorizma za pojedine privatne finansijske institucije, poteškoće sa razmjenom informacija koje proizilaze iz zakonskih prepreka za dijeljenje tajnih podataka između javnih agencija i privatnih kompanija, nedostatka povjerenja mnogih njihovih predstavnika, kao i razlika između „bolje vrabac u ruci nego golub na grani“ logike državnih agencija za sprovođenje zakona i gesla „profit na prvom mjestu“ privatnih kompanija[465].

Kao moguće rešenje za sva tri izazova, Strategija za sajber bezbjednost EU se zalaže za usvajanje novog zakonodavstva EU u toj oblasti sa ciljem da se osigura da privatne kompanije u brojnim ključnim oblastima infrastrukture (energija, transport, bankarstvo, berze i provajderi ključnih internet usluga) „procijene rizike sajber bezbjednosti sa kojima se suočavaju, osiguraju pouzdane i otporne mreže i informacione sisteme preko odgovarajućeg upravljanja rizikom i da dijele identifikovane informacije sa nadležnim organima nacionalne informacione infrastrukture[466]. Sva tako koncipirana zakonodavna rešenja, međutim, u osnovi su u suprotnosti sa ključnom logikom koja stoji u konceptu javno-privatnog partnerstva, jer po svojoj suštini predstavljaju nametanje „partnerstva“ od strane „vrha“. To se smatra posebno problematičnim, jer iako postoji mnogo različitih konceptualizacija javno-privatnog partnerstva, vjerovatno nijedna od njih ne uključuje hijerarhijski odnos od vrha prema dolje između javnih i privatnih aktera. U perspektivi javnog upravljanja, javno-privatna partnerstva po svojoj prirodi predstavljaju „uspostavljanje odnosa saradnje između vlade, profitnih kompanija i neprofitnih privatnih organizacija za obavljanje političke funkcije.[467] U Strategiji sajber bezbjednosti EU nije zanemarena ni važnost principa dobrovoljnosti javno-privatne saradnje, budući da se u tom dokumentu navodi da „zakonske obaveze ne smiju da zamijene niti spriječe razvoj neformalne i dobrovoljne saradnje, uključujući javni i privatni sektor, s ciljem povećanja nivoa bezbjednosti i razmjene informacija i najbolje prakse“[468].

U tom kontekstu, Evropska unija je uvela novi pojam “otpornost“ u dvije strategije bezbjednosti EU (Strategija unutrašnje bezbjednosti EU iz 2010. godine i Evropski program za zaštitu kritične infrastrukture iz 2013. godine) kao i kroz postojeće javno-privatno partnerstvo koje se odnosi

---

[465] Bures O.: Political corporate social responsibility: Including high politics? *Journal ofBusiness Ethics*, Volume 129, Issues 3, Springer Netherlands, 2015, pp. 690–700

[466] Cybersecurity strategy of the European Union, European Commission, 2013, p. 6, dostupno na: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organizedcrime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf.

[467] LinderS. H., Rosenau P. V. : Mapping the terrain of the public-private policy partnership. In: Rosenau V. P.(ed.): *Public-private policy partnerships*, MIT Press,Cambridge, 2000, p. 5

[468] Cybersecurity strategy of the European Union. European Commission, 2013, p. 6, dostupno na: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organizedcrime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf.JOIN(20

na bezbjednost - Evropsko javno-privatno partnerstvo za otpornost (European Public-Private Partnership for Resilience-EP3R)[469] koje bi trebalo da igra presudnu ulogu u naporima širom EU da se zaštiti kritična informaciona infrastruktura. Kao takva, stvorena konceptualizacija otpornosti EU usredsređena je prevashodno na infrastrukturu, koja ima svoje korijene u inžinjerskoj nauci. Ovo nije iznenađujuće s obzirom na rasprave o tome šta čini određenu infrastrukturu kritičnom u mjeri u kojoj bi njena nesposobnost ili uništenje imalo negativan efekat na nacionalnu bezbjednost. Pri tome kao primjeri najčešće se navode bankarstvo i finansije, državne službe, telekomunikacije i informacione i komunikacione tehnologije, hitne i spasilačke službe, energetika i električna energija, zdravstvene usluge, transport, logistika i distribucija, kao i snabdijevanje vodom[470], postoji konsenzus da je veći dio te infrastrukture u privatnom vlasništva i (ili) njome upravlja privatni sektor. Zbog privatizacije i deregulacije javnog sektora od 1980-ih godina, kao i globalizacionih procesa od kraja hladnog rata, privatni sektor kontroliše blizu 85% kritične infrastrukture u većini zapadnih država.

Ove promjene su nastale kao rezultat uvida da je nemoguće ostvariti potpunu zaštitu cjelokupne nacionalne infrastrukture, prije svega zbog njene veličine i ogromnih troškova koji bi to podrazumijevali, pri čemu čak i najbolje organizovane i sprovedene mjere bezbjednosti ponekad ne garantuju uspjeh. Pristalice ovakvog razumijevanja otpornosti stoga tvrde da bi veći naglasak trebalo staviti na oporavak od svih vrsta katastrofa kako bi se oštećena infrastruktura mogla što lakše ekonomski obnoviti[471]. Kao takav, ovaj pristup takođe ima prednost što je znatno jeftiniji od ulaganja u specifične nadogradnje infrastrukture kojima se pristupa kako bi se izbjegli određeni scenariji rizika koji se mogu ili ne moraju dogoditi“[472]. Ovdje se zadržava mogućnost da bi pristup otpornosti na infrastrukturu bio prihvatljiviji za privatne kompanije, čiji bi motiv profita trebalo da ih natjera da budu veoma zainteresovani da što prije obnove i pokrenu svoje poslovanje. U području zaštite kritične infrastrukture, koncept otpornosti infrastrukture može stoga predstavljati obećavajući način za uključivanje privatnih kompanija u pružanje sigurnosti.

U trenutnoj konceptualizaciji EU otpornost se uglavnom, shvata kao sposobnost sistema da se oporavi od nevolja, bilo da se vrati u prvobitno stanje ili u prilagođenu poziciju na osnovu novih zahtjeva. Pomenuti koncept preusmjerava pažnju sa bezbjednosnih prijetnji na širok spektar bezbjednosnih rizika (od prirodnih opasnosti i neuspjeha funkcionisanju kritične infrastrukture do terorističkih napada, pa do sprečavanja, odvraćanja i zaštite od prijetnji, te ublažavanja posledica nakon što se katastrofa dogodi). U ovom svijetlu, naglasak EU na otpornosti u nekim od donijetih strateških dokumenata može se tumačiti kao namjerni pokušaj „korekcije“ odozdo prema gore umjesto dosad nefunkcionalnih partnerstava “odozgo na dolje, nametnutih privatnom sektoru putem zakonskih propisa javne vlasti“. Naime, umjesto da pogrešno očekuju da će privatne kompanije preduzeti sve neophodne korake da obezbijede maksimalnu bezbjednost bez obzira na troškove koji su sa tim povezani, sastavljači ovih dokumenata EU su prihvatili neoliberalni oblik obavljanja vlasti,

---

[469] *European public private partnership for resilience (EP3R)*, ENISA, 2014, dostupno na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[470] Dunn-Cavelty M., Kristensen K. S.: *Securing ‘the Homeland’: Ciritical infrastructure, risk and (in)security,* Routledge, London, 2008, pp.1-2

[471] Pursiainen C.: The challenge for European critical infrastructure protection, *European Integration*, 31(6), November 2009, p. 728.

[472] De Bruijne M., Van Eeten M.: Systems that should have failed: Critical infrastructureprotection in an institutionally fragmented environment, *Journal of Contingencies and CrisisManagement*, 15(1), 2007, p. 24

koji stavlja naglasak na individualnu prilagodljivost i mobilizaciju nedržavnih socijalnih aktera, „koji su neophodni za upravljanje u društvu koje se brzo mijenja i u kojem se ni tržište ni država ne mogu odvojeno usmjeravati ili sprovoditi potrebne promjene“.[473]

Rast javno-privatnih partnerstava koji je u početku bio jedna od komponenti tzv. novog javnog menadžmenta i neoliberalnih modela uloge države, prerastao je u opšti proces privatizacije javne infrastrukture i postao važno sredstvo za privlačenje privatnih resursa za dalje projekte javne izgradnje. Glavni pokretač za formiranje tipičnih javno-privatnih proizvoda su razmatranja troškova i efikasnosti ili s tim povezana politika javne vlasti. Zajednička definicija o javno-privatnom partnerstvu još uvijek ne postoji, međutim, način finansiranja i prenos rizika sa javnog na privatni sektor zajedničke su karakteristike u različitim jurisdikcijama širom svijeta, pa i u okviru Evropske unije. Glavna korist od uključivanja privatnog sektora u pružanje javnih usluga putem formata javno-privatnog partnerstva pripisuje se činjenici da javni sektor u tim okolnostima ne mora da angažuje sopstvena kapitalna sredstva, kao i da se ostvaruje značajan prenos rizika na privatni sektor[474].

U modernom sektoru informaciono-komunikacione tehnologije odnosi između javnih i privatnih aktera pokazuju različite karakteristike. Za razliku od mnogih drugih ključnih ekonomskih i društvenih infrastruktura, internet je dominantno privatni konstrukt, još od ranih 1980-ih godina. To znači da su klasična javno-privatna partnerstva za izgradnju i pružanje usluga relativno rijetka u urbanim područjima, naprednim ekonomijama, kao i u pogledu standardne infrastrukture u oblasti telekomunikacija[475].

Pored toga, javno-privatna partnerstva služe i kao široko primjenjivani instrumenti za uticaj na privatne aktere koji djeluju, podupiru i pružaju usluge u sajber-prostoru, uklapajući se u šire političke diskurse o inovacijama, konkurentnosti i nacionalnoj bezbjednosti[476]. Ovo je stvorilo situaciju da veoma širok spektar političkih inicijativa, foruma i platforma za konsultacije u sektoru informaciono-komunikacionih tehnologija bude označen kao javno-privatno partnerstvo[477], što izlazi iz okvira definicija koje postoje kada je riječ o konvencionalnim javno-privatnim partnerima.

Kada se pristupa problemu bezbjednosti u drugim infrastrukturnim i industrijskim sektorima, mogla bi se očekivati klasična rasprava o potrebi obavezujućih propisa ili pravila o odgovornosti u odnosu na razmatranja o ekonomskoj konkurentnosti[478]. Širok spektar instrumenata dobrovoljnog i privatnog upravljanja koji se nalaze pod različitim nazivima, kao što su društvena odgovornost kompanija ili, u kontekstu EU, otvorene metode koordinacije često se preispituju kao potencijalna

---

[473] Joseph J.: Resilience as embedded neoliberalism: A governmentality approach. Resilience, *International Policies, Practices and Discourses*, 1(1), 2013, p. 38

[474] Dunn Cavelty M.: From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse,*International Studies Review*, 15(1), 2013, pp. 105–106,

[475] LaRose R., Bauer J. M., DeMaagd K., ChewH. E., Ma W., Jung Y.: Publicbroadband investment priorities in the United States: An analysis of the broadband technologyopportunities program. *Government Information Quarterly*, 31(1), 2014, pp. 54–55

[476] Carr M.: Public–private partnerships in national cyber-security strategies, *International Affairs, 92(1),*2016, pp. 46–49

[477] *Cooperative models for effective public private partnerships*, ENISA, 2011, p. 8, dostupno na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-privatepartnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships/at_download/fullReport

[478] Heritier A.: Market integration and social cohesion: The politics of public services in European regulation,*Journal of European Public Policy*, 8(5), 2001, 826

alternativa hijerarhijskoj regulaciji zbog brzine, fleksibilnosti, dometa i podrške zainteresovanih strana u procesima implementacije.

Dvije agencije Evropske Unije, ENISA i EUROPOL, glavni su javni operativni i izvršni akteri u oblasti sajber bezbjednosti. Oba subjekta su u velikoj mjeri zavisna od saradnje sa privatnim akterima, pri čemu ostvaruju različite mandate i odnose. Agencija Evropske unije za bezbjednost mreže i informacija (ENISA), glavna je organizacija za sajber bezbjednost na infrastrukturnom i tehničkom (logičkom) nivou. ENISA je osnovana 2004. godine i postepeno se etablirala kao vodeći pružalac tehničkih usluga u Evropi. U 2013. godini ENISA je dobila proširenu i stalnu pravnu osnovu, koja je definisala njen organizacioni mandat da „agencija treba da doprinese visokom nivou bezbjednosti mreže i informacija, boljoj zaštiti privatnosti i ličnih podataka i razvoju i promociji kulture mrežne i informacione sigurnosti u korist građana, potrošača, kompanija i organizacija javnog sektora u Uniji i na taj način doprinose pravilnom funkcionisanju unutrašnjeg tržišta.[479]

U svijetlu navedenog, redovne interakcije između javnih i privatnih aktera očigledno su ključne za rad ove agencije. Na generalnom nivou, ovo se može ilustrovati uključivanjem privatnih predstavnika u takozvanu stalnu grupu zainteresovanih strana, koja bi trebalo da pomogne upravljanju ENISA-om nakon poslednje revizije njegovog mandata[480]. Pored navedenog, predmetna agencija je sprovela opsežno istraživanje o različitim modelima i potencijalu javno-privatnog partnerstva u sektoru informaciono-komunikacione tehnologije. Na osnovu toga, agencija naglašava da privatni akteri često ne žele da razmjenjuju informacije na dobrovoljnoj osnovi i da su neophodni formalni sporazumi ili strukture da bi se obezbijedila operativna korisnost partnerstva, kako privatnim, tako i javnim akterima[481].

Istovremeno, usmjerenost ENISA-e na više infrastrukturnih slojeva sajber bezbjednosti sugeriše da su interakcije između javnog i privatnog sektora vjerovatnije u obliku koregulacije za postavljanje opštih standarda ili sertifikata o bezbjednosti. To se odražava na niz različitih interesnih grupa, kao što su forumi za upravljanje koje nadgleda ENISA, poput „referentne grupe za sigurnost i otpornost na internet infrastrukturi ENISA[482], i „Referentne grupe za elektronske komunikacije (Electronic Communications Reference Group-ECRG). Ove grupe su u interakciji sa drugim forumima za tehničku samoregulaciju, posebno sa Međunarodnom organizacijom za standarde (ISO), Evropskim institutom za elektronske standarde (European Electronic Standards Institute-ETSI) i CENCELENEC za ostale industrijske standarde[483].

ENISA takođe uključuje niz širih obrazovnih aktivnosti i aktivnosti podizanja svijesti koje bi trebalo da podstaknu veća ulaganja u sajber bezbjednost kako javnih tako i privatnih aktera. Pored takozvane „Zajednice za podizanje svijesti“ ENISA-e - koja je, čini se, prekinuta posle 2010. godine, najveći koordinirani napor je takozvani “Mjesec svijesti o sajber bezbjednosti“ koji uključuje različite

---

[479] European Union, *Regulation (EU) No 526/2013 of the European Parliament and of theCouncil of 21 May 2013 concerning the European Union Agency for Network and InformationSecurity (ENISA) and repealing Regulation (EC) No 460/2004*, 2013, p. 43

[480] Videti: https://www.enisa.europa.eu/about-enisa/structure-organization/psg

[481] Cooperative models for effective public private partnerships, Desktop ResearchReport, ENISA. 2011, dostupno na:http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships/at_download/fullReport.

[482]Videti: https://resilience.enisa.europa.eu/internet-infrastructure-security-and-resilience-referencegroup

[483] Purser S.: Standards for Cyber Security, In: Hathaway E. M. (ed.*): Best Practices in Computer Network Defense: Incident Detection and Response*, IOS Press, 2014, pp. 103-104

privatne organizacije[484]. Međutim, ove edukativne aktivnosti ne mogu se u potpunosti smatrati održivim i značajnim javno-privatnim partnerstvima, jer je njegova ciljna grupa difuzna i ne očekuje se da učesnici stupe u redovne veze sa ENISA-om.

4.5.2. Javno-privatno partnerstvo na prostoru Evropske unije u zaštiti kritične infrastrukture – studije slučajeva

4.5.2.1. Javno-privatno partnerstvo u zaštiti kritične infrastrukture u Kraljevini Španiji

Španija je svojim Nacionalnim planom za zaštitu kritične infrastrukture (Plan Nacional de Proteccion de las Infraestructuras Crıticas) definisala nacionalnu kritičnu infrastrukturu kao „one instalacije, mreže, usluge, fizičku opremu i informacione tehnologije čiji bi prekid ili uništenje imali ozbiljan uticaj na zdravlje, bezbjednost, ekonomsko blagostanje građana ili efikasno funkcionisanje državnih institucija i javne uprave“. Pored toga, određeno je i dvanaest strateških sektora - hemijska industrija, nuklearna industrija, istraživački kapaciteti, institucije državne vlasti, kosmos, energetski sektor, telekomunikacije, saobraćaj, snabdijevanje vodom, hrana, finansijski sektor i zdravstvo. Na osnovu definisanih sektora izrađen je katalog nacionalne kritične infrastrukture koji sadrži 3.500 kritičnih instalacija širom Španije. Kao i kod drugih država, i za Španiju je karakteristično da zaštita kritične infrastrukture obuhvata između ostalog i saradnju nadležnih ministarstava, kao i to da je Nacionalni centar za zaštitu kritične infrastrukture pod nadležnošću Ministarstva unutrašnjih poslova[485].

Prema odredbama Zakona o privatnoj bezbjednosti, subjekti privatne bezbjednosti u Španiji vrše obezbjeđenje privatnih, poslovnih i javnih objekata, aerodroma, luka, pristaništa, vojnih objekata, industrijskih postrojenja i resursa kritične infrastrukture, poslove lične zaštite, tranzit novca i vrijednosti, pratnju transporta eksplozivnih i opasnih materija, obezbjeđivanje zatvora, popravnih domova i prihvatilišta za strance, suzbijanje piratstva na moru, poslove privatnih istraga, instaliranje i održavanje alarmnih sistema i kontrolnih centara.[486]

Španski Zakon o privatnoj bezbjednosti predstavlja kompromisnu opciju uspostavljanja nacionalnog sistema bezbjednosti koji integriše privatnu sa javnom bezbjednošću. S jedne strane, policijska uprava kontroliše privatne kompanije za obezbjeđenje, ali je takođe razvijeno rešenje koje integriše privatnu bezbjednost u nacionalni sistem bezbjednosti. Predmetni model odnosa između privatnog i javnog sektora stvara dvostruku lojalnost privatnih kompanija za obezbjeđenje, kako prema javnom sektoru, tako i prema svojim klijentima. S jedne strane, akteri privatne bezbjednosti imaju korporativne i ekonomske izazove vezane za obavljanje njihove djelatnosti, a s druge strane zakon zahtijeva od njih da sarađuju sa javnim sektorom bezbjednosti i da obavještavaju policijske snage kad god je to potrebno za održavanje javnog reda. Značaj odredbi Zakona o privatnoj bezbjednosti je i u tome što precizno definišu aktivnosti koje su dozvoljene privatnim bezbjednosnim

---

[484] *European Cybersecurity Month*, ENISA, dostupno na:https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month

[485] Voeller G. J.: *Wiley handbook of science and technology for homeland security*, John Wiley & Sons, Hoboken, New Jersey, 2010, pp. 854-857

[486] Alós R., Urbano X.: *Report on the Trade Unions and Employers Organisations in the Sector of Private Security in Spain*, QUIT, Universitat Autònoma de Barcelona, Barcelona 2003, pp. 4-5.

korporacijama i što propisuju stroge zahtjeve za obavljanje takve djelatnosti sa stanovišta finansija i resursa: osnovni kapital, osoblje, sredstva, garancije i slično, uz detaljno razrađene kaznene mjere za nepoštovanje odredbi Zakona[487].

S druge strane, Španija predstavlja i dobar primjer sistema regulacije i kontrole koji omogućava subjektima privatnog obezbjeđenja da podrže javni sektor, a posebno organizacione jedinice državne policije na različite načine. U vezi sa tim, propisima je definisano osnivanje mješovitih koordinacionih komisija radi podsticanja saradnje i javno-privatnog partnerstva između nadležnih državnih institucija i privatnih kompanija, uključujući centralnu i lokalne komisije. Njihove funkcije, između ostalog, uključuju i savjetovanje Ministarstva unutrašnjih poslova o opštim kriterijumima primjene, koordinaciji i razvoju zakonodavstva za privatnu bezbjednost, kao i podsticanje razmjene iskustava iz različitih sektora zastupljenih u komisiji, te formulisanje predloga za nove načine i metode borbe protiv kriminala u oblasti privatne bezbjednosti. Pored navednog, tu su i informisanje o onim područjima rada za koje je privatni sektor odgovoran prema planovima za sprečavanje kriminala, kao i analize i procjene obrazovnih aktivnosti potrebnih za osoblje privatnog obezbjeđenja i predlaganje kriterijuma za koordinaciju između kompanija za obezbjeđenje, neposrednog obezbjeđenja i policije[488].

U Kraljevini Španija postoji uspostavljena struktura koja omogućava razmjenu operativnih informacija između javnog i privatnog sektora o pitanjima kao što su registarske tablice, informacije o predstojećim štrajkovima i demonstracijama, ili distribucija fotografija najtraženijih terorista. Ranije analize su sugerisale da ovaj vid razmjena više favorizuje javni sektor, ali je činjenica da su u proteklom periodu privatne bezbjednosne službe efektivno integrisane u ostvarivanje osnovnih ciljeva javne bezbjednosti, uključujući i područje kritične infrastrukture. U vezi sa tim, u Španiji je propisano da svi ugovori potpisani između privatnih kompanija za obezbjeđenje i njihovih klijenata moraju biti registrovani u policiji, uključujući broj uključenog osoblja za obezbjeđenje i usluge koje će se nuditi. U cilju efikasnije komunikacije sa privatnim pojedincima i kompanijama, policija je uspostavila 24-časovne namjenske telefonske linije za brzu komunikaciju u vanrednim situacijama[489].

Zakonodavstvo i propisi u Španiji su u procesu stalnog unapređenja kako bi se postojeća saradnja i partnerstvo javnog i privatnog sektora dodatno podržali i učvrstili. To se odnosi i na aktuelni Zakon o privatnoj bezbjednosti, u čijoj se preambuli navodi da snage bezbjednosti države moraju biti aktivno angažovane na razvoju aktivnosti privatnih bezbjednosnih struktura. Pored toga, u tom dijelu zakonskog teksta je navedeno da je prepoznata efikasnost, važnost i djelotvornost javno-privatnog partnerstva kao sredstva za suočavanje i rešavanje različitih gorućih problema bezbjednosti koji su prisutni u društvu. U tom smislu, industrija privatnog obezbjeđenja se smatra dijelom mjera usmjerenih na zaštitu društva i odbranu legitimnih prava i interesa građana[490].

Zakonodavac je odredbama posebno definisao zaštitu kritične infrastrukture kao stratešku oblast. Tako je, na primjer, za angažovanje pripadnika privatnih bezbjednosnih službi u zaštiti

---

[487] Giménez-Salinas A: New approaches regarding private/public security, *Policing and Society*, vol. 14, No. 2 2004, pp. 163-164.
[488] Ibidem, p. 164.
[489] *State Regulation concerningCivilian Private Security Servicesand their Contribution to Crime Preventionand Community Safety*, United Nations Office on Drugs and Crime (UNODC), Vienna, 2014, p. 40
[490] Act 5/2014 on Private Security, p.3, dostupno na: https://www.aproser.es/web/wp-content/uploads/2016/06/Act-5-2014-on-Private-Security.-Unofficial-translation.pdf

kritične infrastrukture, propisano da su privatne kompanije dužne da obezbijede sertifikat koji garantuje njihovu usklađenost sa relevantnim administrativnim, radnim, socijalnim i poreskim propisima[491]. Pored navednog, Zakon utvrđuje da poslove privatnog obezbjeđenja mogu obavljati samo lica koja su stručna i osposobljena za obavljanje poslova kao što su bezbjednost eksplozivnih materija, privatni telohranitelji, pripadnici obezbjeđenja u ruralnim oblastima i za to vezane specijalnosti (čuvar lovišta, čuvar morskog ribarstva i slično), šef obezbjeđenja, privatni detektiv. Pritom je zakonodavac ostavio mogućnost da se za potrebe zaštite kritične infrastrukture angažuju i druge specijalnosti u skladu sa zakonom. Kada je riječ o zaštiti kritične infrastrukture, predviđeno je da privatne bezbjednosne službe predmetnu uslugu pružaju sa vatrenim oružjem kada se to zahtijeva zbog specifičnosti i okolnosti[492].

Za angažovanje privatnih bezbjednosnih službi u strateškim oblastima definisanim kao kritična infrastrukturama, privatne kompanije za obezbjeđenje moraju da isporuče potvrdu izdatu od ovlašćenog sertifikacionog subjekta, koja garantuje njihovu osnovnu usklađenost sa relevantnim administrativnim, radnim, socijalnim i poreskim propisima.

Sa aspekta kritične infrastrukture posebno značajnim aktivnostima privatnog sektora bezbjednosti u Španiji se smatraju:

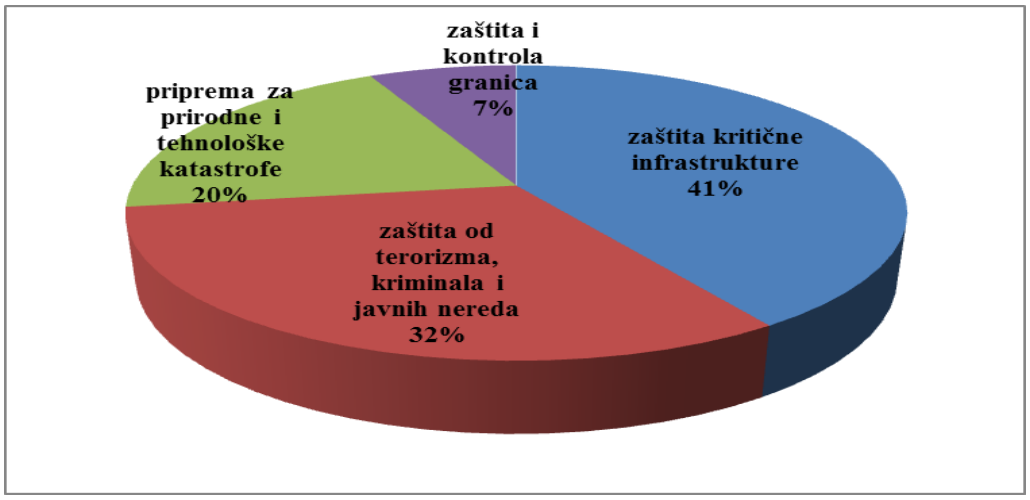
- nadgledanje i zaštita imovine, objekata, mjesta (javnih i privatnih), događaja, kao i lica koja su prisutna u njima,
- održavanje uređaja i instalacija, opreme, mehanizama i bezbjednosnih sistema povezanih sa centralnim alarmnim sistemom ili sjedištem za video nadzor, i
- rad u centrima za povezivanje, prijem, verifikaciju i prenosa alarma, kao i nadgledanje signala pomoćnih uređaja za bezbjednost lica, pokretne i nepokretne imovine ili izrečenih mjera i izvještavanje nadležnih organa za sprovođenje zakona u tim slučajevima[493].

Španija je tokom istorije bila poznata kao pomorska sila, a i u savremeno doba ta država posvećuje posebnu pažnju bezbjednosti u pomorskom saobraćaju. Kao jedan od ključnih činilaca za postizanje ciljeva pomorske bezbjednosti se naglašava zajedničko djelovanje i partnerstvo privatnog i javnog sektora, kao i saradnja između institucija i agencija na svim nivoima. U cilju jačanja pomenute saradnje, od posebnog interesa je stvaranje virtuelnog okruženja kako bi se za agencije koje intervenišu u određenim situacijama omogućilo dijeljenje potrebnih informacija u realnom vremenu, te obezbijedila korelacija i analiza podataka o morskom okruženju, uz podsticanje učešća javnog i privatnog sektora u projektima koji se odnose na nacionalnu pomorsku bezbjednost. Podsticanjem saradnje sa akterima privatnog sektora koji imaju interese u morskom okruženju, omogućava se da javno-privatno partnerstvo u području bezbjednosti bude efikasno, ali i profitabilno za angažovane subjekte privatne bezbjednosti. Inače, španska vizija pomorske bezbjednosti podrazumijeva usaglašene akcije, koje na efektivan način uključuju potrebne resurse države i privatnog sektora. Ovakav pristup ima za cilj postizanje zajedničkih strateških ciljeva koji omogućavaju predviđanje,

[491] Act 5/2014 on Private Security, section 19. 4
[492] Act 5/2014 on Private Security, section 40. 4
[493] Private Security, Act 5/2014, section 5., a,f i g.

sprečavanje i, ako je potrebno, efikasno reagovanje na rizike i prijetnje koji nastaju u ili iz pomorskih područja pod španskom odgovornošću[494].

U Španiji danas funkcioniše veliki broj privatnih bezbjednosnih agencija koje su specijalizovane za različite oblasti djelovanja. U cilju adekvatnog predstavljanja privatnog sektora bezbjednosti Španije u zaštiti kritične infrastrukture, poslužićemo se rezultatima istraživanja koje je sprovedeno 2014. godine na osnovu preporuka Evropske komisije vezanih za dalji razvoj bezbjednosnog sektora EU[495]. Prema navednom istraživanju, privatna bezbjednost u Španiji uglavnom je orijentisana na prevenciju terorizma i zaštitu od kriminala, što je očekivano zbog višedecenijskog prisustva terorističkih organizacija kao što je ETA na španskom tlu. Stav anketiranih zainteresovanih strana je da predstavljena distribucija kompanija po „kategoriji prijetnji" prekomjerno predstavlja broj firmi koje se bave zaštitom kritičnih infrastruktura. To bi se moglo objasniti dvosmislenom definicijom kritične infrastrukture Evropske unije koja omogućava široku, vjerovatno previše opsežnu i ekstenzivnu interpretaciju ovog koncepta (Grafikon br. 5).



Grafikon br. 5.: Djelatnost privatnog sektora bezbjednosti u Španiji (broj odgovora)[496]

S druge strane, manji broj privatnih kompanija koje su aktivne u oblastima „zaštite granica i kontrole" i „prirodnih katastrofa i katastrofa nastalih od čovjeka" u skladu je s očekivanjima, jer su ovi segmenti specijalizovaniji i stoga se od kompanija privatnog sektora bezbjednosti zahtijeva da raspolažu odgovarajućim vještinama, tehnologijom i sertifikovanim uslugama. Prema pomenutom istraživanju, skoro 41% anketiranih organizacija isporučuje proizvode i usluge za zaštitu kritične infrastrukture u Španiji. Nasuprot tome, svega oko 7% privatnih kompanija je aktivno u pružanju proizvoda i usluga vezanih za „zaštitu i kontrolu granice".

[494] *National Maritime Security Strategy*, 2013, dostupno na: https://www.lamoncloa.gob.es/documents/20131333estrategiadeseguridadmartima_ingls.pdf
[495] *Study on the development of statistical data on the European security technological andindustrial base*, Security Sector Survey Analysis: Spain, Ecorys, The Netherlands, 2015, dostupno na: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/reference-documents/docs/final_security_survey_descriptive_analysis_es_en.pdf
[496] Idid

4.5.2.2. Javno-privatno partnerstvo u domenu bezbjednosti evropskih aerodroma

Savremeni aerodromi predstavljaju složene cjeline sa mnoštvo različitih funkcija. Pored kontrolisanog pristupa djelovima aerodromskog prostora i vazduhoplovima, aerodromi uglavnom imaju i veliko područje koje je dostupno javnosti, kao što su prodavnice, supermarketi, restorani, različite usluge, konferencijski i kancelarijski kompleksi, kao i hotelski sadržaji. Vazdušne luke su integrisane u lokalnu i transregionalnu saobraćajnu infrastrukturu, tako da putnici, potrošači i druge zainteresovane strane u njima mogu da koriste različite sadržaje. Aerodromi se mogu posmatrati i kao konkretan prostor za sprovođenje međunarodne bezbjednosti koji zbog svoje osjetljivosti ima poseban društveni i politički značaj. Pored pružanja usluga koje doprinose globalnoj povezanosti, vazdušne luke su prostor u kome se razvijaju različiti odnosi između javnih i privatnih aktera u ostvarivanju bezbjednosti[497].

Sa stanovišta bezbjednosti, precizno razgraničenje aerodroma od ostalih pratećih sadržaja nije nimalo jednostavno. S druge strane, oblici i stepen povezanosti i partnerstva između službi bezbjednosti na aerodromima su raznoliki. U te odnose mogu biti uključene nacionalne, regionalne ili lokalne policijske, carinske i imigracijske vlasti, aerodromski operatori ili privatni pružaoci bezbjednosnih usluga, u zavisnosti od stanja nacionalne bezbjednosti i odgovarajućeg pravnog okvira. Nacionalni organi uglavnom učestvuju u kontroli prelaska granice, jer su odgovorni za zaštitu državne granice i za carinski nadzor, a aerodromi, ukoliko se ne radi o unutrašnjem avioprevozu, su i granice za ulazak i izlazak iz određene države. Kao rezultat saradnje i javno-privatnog partnerstva, u nekim slučajevima može doći do preklapanja nadležnosti bezbjednosnih aktera, iako je regulativa kao u slučaju standarda za kontrolu putnika sada u značajnoj mjeri usklađena na međunarodnom nivou. Nezavisno od toga, savremeni aerodromi zahtijevaju usklađivanje niza različitih interesa i kompetencija, koju moraju biti adekvatno koordinirane u jedinstven bezbjednosni aranžman[498].

U Evropi je bezbjednost na aerodromima tradicionalno predstavljala monopol države i njenih službi, ali je period koji je nastupio krajem osamdesetih godina XX veka, usled izraženog povećanja broja letova i putnika, te ograničenih resursa javnog sektora, uzrokovao ograničenja u preduzimanju bezbjednosnih mjera, što je dovodilo i do problema vezanih za potrebni nivo bezbjednosti na aerodrumima. To je primoralo mnoge evropske države da potraže nove i bolje načine ostvarivanja bezbjednosti vazdušnih luka. U vezi sa tim, Akt o deregulaciji vazduhoplovstva u Velikoj Britaniji iz 1988. godine predstavljao je i početak privatizacije, outsourcing-a i ugovornog partnerstva u bezbjednosti na nizu lokacija evropske aerodromske infrastrukture. S druge strane, neke druge zemlje, uključujući i Njemačku, bile su tih godina skeptične prema procesima deregulacije i oklijevale su da pristupe mjerama koje bi vodile liberalizaciji bezbjednosti aerodroma. Tek 90-ih godina, kada su budžetska ograničenja prouzrokovala neminovne promjene u raspodjeli finansijskog tereta, ukazala se jasna potreba za preduzimanje odgovarajućih promjena na tom planu. Tako je obezbjeđenje aerodroma u Njemačkoj bilo u isključivoj javnoj nadležnosti sve do 1992. godine, kada je ugovaranje operacija njihovog nadgledanja postalo pravno moguća opcija. Tek 1995. godine počelo je

[497] Lahav G.: Mobility and border security: The U.S. aviation system, the state, and the rise of public–private partnerships, In: Salter M.B. (ed.): *Politics at the Airport*, University of Minnesota Press Minneapolis 2008, p. 81

[498] Leese M., Wildi L.: Security Measures at Zurich Airport, *Analyses in Security Policy No 208*, Center for Security Studies, Zurich, 2017, pp. 1-2

ugovaranje operacija skrininga sa privatnom bezbjednosnim kompanijama, pri čemu su aerodromi u Štutgartu i Hamburgu bili prvi u kojima je zaživjio novi način obezbjeđenja[499].

Danas većina njemačkih aerodroma angažuje privatne kompanije i povjerava im kontrolu putnika i prtljaga, pri čemu je uspostavljen složen zajednički vladin i privatni sistem bezbjednosti i nadzora, koji i dalje ostaje u velikoj mjeri pod nadzorom države, a u kome privatni akteri rade u strogo definisanom institucionalnom okviru. U vezi sa tim, privatne firme koje obavljaju kontrolu na aerodromima moraju biti zvanično sertifikovane. Na tom planu postoje definisani zahtjevi, uključujući procjenu solventnosti firme, opsežne provjere direktora, rukovodilaca i osoblja za skrining, te praksu zaključivanja dugoročnih ugovora kako bi se omogućio razvoj karijere i zadržavanje ključnog osoblja. U ponudi za javno-privatno partnerstvo se navode i minimalne zarade i naknade. Uz to, projektanti moraju da dobiju pojedinačnu dozvolu, koja zahtijeva obimnu početnu i ponavljajuću obuku, prvo kao oficir za bezbjednost, a zatim kao specijalizovani agent za vazduhoplovnu bezbjednost. S druge strane, državna kontrola i praćenje su veoma rigorozni, pri čemu nadležni vazduhoplovni organi vrše periodične revizije kvalifikacije i obuke zaposlenih. U isto vrijeme, na kontrolnim punktovima se vrše nasumični testovi, a pripadnici Federalne granične straže su stalno prisutni i nadgledaju funkcije skrininga. Pored toga, postoji mogućnost sankcionisanja slabih performansi angažovane kompanije, na način da će se suspendovati licenca ili raskinuti ugovor kompanije na određenoj lokaciji. Budući da su u pitanju dugoročni ugovori, raskid saradnje i partnerstva je posebno efikasna sankcija, jer znači da kompanija neće biti u mogućnosti da pruža usluge na duži period. Na taj način se osigurava ostvarivanje visokih performansi kontrole putnika i prtljaga na njemačkim aerodrumima.

I u drugim evropskim državama privatni sektor je angažovan u sistemu bezbjednosti aerodroma na slične načine. Tako je, na primjer, za bezbjednost aerodroma u Cirihu odgovorna Aerodromska policija, (dio kantonalne policije), u čijoj je nadležnosti bezbjednost čitavog područja vazdušne luke. Pored njih, na tom aerodromu postoje i „službenici bezbjednosti aerodromske policije“, kao i „bezbednosni pomoćnici granične kontrole“ koji obavljaju dio poslova za Aerodromsku policiju, koji se odnosi na provjeru prtljaga, lica i pasoša. Osoblje kompanije Custodio, privatne kompanije za obezbjeđenje, vrši bezbjednosne provjere tereta i avio-pošte na ciriškom aerodromu. Zajedno sa kompanijom Protectas, ono je takođe odgovorno za bezbjednosne kontrole zaposlenih na aerodromima. Pored njih, na aerodromu su i medicinske i vatrogasne službe grada Ciriha koje pružaju usluge iz svoje nadležnosti, zaokružujući model javno-privatnog partnerstva koji je tu u primjeni[500].

Aerodrom u Amsterdamu (Schiphol) ima složenu sturukturu bezbjednosnih subjekata. Čak 10% svih pripadnika privatnog sektora bezbjednosti u Holandiji radi na tom aerodromu. Riječ je o 3500 radnika privatnog obezbjeđenja, podijeljenih između tri najveće kompanije u zemlji (G4S, Securitas i Trigion) i mnoštva manjih, specijalizovanih kompanija. Veće kompanije prije svega isporučuju bezbjednosnu tehologiju, dok su se dvije manje kompanije (Pro-Check International and the International Security i Counter-Terrorism Agency, ISCA) specijalizovane za opštu bezbjednost,

[499] Hainmüller J., Lemnitzer M. J: Why do Europeans fly safer? The politics of airport security in Europe and The US, *Terrorism and Political Violence*, 15:4, 2003, p. 12

[500] Leese M., Wildi L.: Security Measures at Zurich Airport, *Analyses in Security Policy No 208*, Center for Security Studies, Zurich, 2017, p. 2

dok Kraljevska policija nadgleda sigurnost aerodroma. Svi subjekti bezbjednosti su uključeni u platformu (Security and Public Safety Schiphol) koja je postavljena kao odgovor na terorizam, a čiji je cilj postizanje integrisanog pristupa u kojem javni i privatni partneri koriste ista sredstva i tehnologije, svako za svoje specifične ciljeve i odgovornosti. Pored navedenih aktera, javno-privatno obezbjeđenje aerodroma uključuje i niz tehnologija, kao što je sistem za nadzor CCTV koji raspolaže sa 1350 kamera, razne biometrijske skenere, preko stotinu detektora metala, ograde, i niz drugih uređaja. U navedenom primjeru javno-privatnog partnerstva, velike privatne kompanije za obezbjeđenje, a prije svega G4S, Securitas i Trigion, imaju i najveću odgovornost za bezbjednost na aerodromu Schiphol [501].

Navedeni odnos javnog i privatnog sektora u ovom domenu ostaće i u budućnosti uglavnom nepromijenjeni, s obzirom da nijedan od učesnika partnerstva nema mogućnosti, kapacitete niti jasan podsticaj za promjenu trenutnog sistema. U tom smislu, vlade evropskih države gotovo su u potpunosti oslobođene finansijskog opterećenja za te namjene, jer se naknade za vazduhoplovnu bezbjednost neprestano povećavaju i pokrivaju većinu bezbjednosnih troškova na aerodromima. S druge strane, evidentno je da avio-kompanijama nedostaju mogućnosti da nadomjeste ukidanje bezbjednosne takse. Budući da to nema negativnog uticaja na konkurenciju i tržišnu poziciju, pošto svaki putnik mora da plati tu naknadu bez obzira na cijenu karte, većina avio-kompanija prestala je da lobira u tom smjeru i prihvatila je da u aktuelnim okolnostima nije realno da teret tih troškova prebace nazad na države[502]

Savremeni evropski aerodromi su zapravo glavni Primjeri fleksibilizacije do koje dolazi uspostavljanjem logike konkurentnog tržišta za sve vrste pružanja usluga, pa stoga liberalna stajališta vlada ne bi trebala da budu iznenađujuća, u smislu da bezbjednost ne predstavlja izuzetak od ove opšte tendencije. Međutim, kada im se pristupi iz ugla bezbjednosti, izbor privatnog partnera za ugovaranje poslova skrininga na aerodromima postaje manje očigledan. U vezi sa naraslim prijetnjama terorizma i međunarodnog kriminala, bezbjednost aerodroma u Evropi je u poslednje dvije decenije doživjela velika prilagođavanja u pogledu tehnoloških unapređenja i promjena politike. U tom kontekstu, poseban naglasak je stavljen na rizične tačke i preventivne pristupe, od kojih se neki pokreću mnogo prije nego što putnici stignu na aerodrom. Ova nova norma upravljanja na aerodromima je podržana inovativnim bezbjednosnim pristupom koji nastoji da konstantno implementira najnovije bezbjednosne tehnologije na skrining kontrolnoj tački. U navedenim slučajevima privatne kompanije kao subjekti javno-privatnog partnerstva ispunjavaju uslove za izvršavanje onoga što bi se moglo opisati kao policijske radnje (pretraga putnika i ručnog prtljaga u cilju otkrivanja opasnih i zabranjenih predmeta, pozivanje policije u slučaju da bude potrebno preduziamnje daljih mjera). Uloga privatnih bezbjednosnih aktera u tom odnosu može se označiti i kao „zamjena policije“.[503]

[501] Schouten R.: Security as controversy: Reassembling security at Amsterdam Airport, *Security Dialogue Vol. 45(1),* 2014, p. 31

[502] Hainmüller J., Lemnitzer M. J: Why do Europeans fly safer? The politics of airport security in Europe and The US, *Terrorism and Political Violence*, 15:4, 2003, p. 12

[503] Leese M.: Governing airport security between the market and the public good, *Criminology & Criminal Justice* 16(2), 2016, pp. 163-165

4.5.2.3. Kontroverzni tokovi ostvarivanja javno-privatnog partnerstva – Studija slučaja Bugarske

Pitanja koja se odnose na privatni sektor bezbjednosti u Bugarskoj, a prije svega uslovi za osnivanje i način funkcionisanja privatnih bezbjednosnih kompanija, te kontrola i nadzora nad njihovom radom, uređeni su Zakonom o djelatnosti privatnog obezbjeđenja iz 2004. godine, mijenjanim i dopunjavanim 2011. i 2014. godine. Prema odredbama ovog zakona, subjekti privatne bezbjednosti mogu pružati različite vrste usluga klijentima, uključujući poslove fizičkog i tehničkog obezbjeđenja lica, skupova i imovine, transporta vrijednosti, zaštite kritične infrastrukture, usluge privatnih istražitelja, ugradnju i održavanje alarmnih sistema i sistema elektronskog nadzora. Zakon o djelatnosti privatnog obezbjeđenja omogućava i oružane usluge privatne bezbjednosti.

Ministarstvo unutrašnjih poslova Republike Bugarske je do 2013. godine u svom sastavu imalo organizacionu jedinicu za poslove tehničkog obezbjeđenja, a u nadležnosti Ministarstva je bilo i obezbjeđenje objekata i službi koje čine nacionalnu kritičnu infrastrukturu. U sklopu sprovedenih reformi bugarske policije, a s obrazloženjem smanjenja troškova, pomenuta jedinica MUP-a je ukinuta. Privatne bezbjednosne kompanije u Bugarskoj su nakon toga započele da popunjavaju upražnjeni prostor. Ipak, i pored toga, policija nije prestala da vrši poslove zaštite objekata i službi kritične infrastrukture. To se posebno odnosi na vazdušne luke, metro u Sofiji, važnije autobuske i železničke stanice, koje i dalje obezbjeđuju pripadnici policije. O načinima obezbjeđenja objekata i resursa kritične infrastrukture rešava se na nacionalnom i lokalnim nivoima odlučivanja. Tako je Gradska uprava Ministarstva unutrašnjih poslova na listu obezbjeđivanih strateških objekata unijela metro u Sofiji. Shodno tome, poslovi obezbjeđivanja metroa ne mogu biti predmet javno-privatnog partnerstva, već isključive nadležnosti MUP-a. Nivo bezbjednosti i zaštite starteških objekata i službi u Bugarskoj, uključujući i jedan broj visokorizičnih objekata koji nisu uvršteni u tu kategoriju u proteklom periodu nisu bili predmet značajnije pažnje javnosti. Po pravilu, kontroverze oko zaštite i obezbjeđivanja objekata tog tipa izlazile su na površinu u medijima tek posle ozbiljnih havarija, koje su za posledice imale gubitke ljudskih života i značajnu materijalnu štetu.

Nakon što je 2005. godine u Bugarskoj prvi put u pravnu terminologiju uveden termin kritična infrastruktura, bugarska vlada je 2012. godine usvojila Uredbu o redosledu, načinu i nadležnim organima za određivanje kritične infrastrukture i procjenu njenih rizika. Tim aktom su regulisana pitanja koja se tiču redosleda, načina i određivanja organa u čijoj je nadležnosti razvrstavanje objekata kritične infrastrukture po kategorijama i vršenje procjene ugroženosti tih objekata. Uredba sadrži generalne smjernice za razvrstavanje i evidentiranje kritične infrastrukture, pri čemu se Ministarstvu unutrašnjih poslova dodeljuje uloga koordinatora tog procesa. Uredbom je definisano ukupno 19 sektora kritične infrastrukture, u koje spadaju i sektori energetike, saobraćaja i transporta, informaciono-komunikacionih tehnologija, ekologije, pošte, proizvodnje i prerade hrane, kao i zdravstva. Utvrđivanje kritičnih objekata i službi u pojedinačnim sektorima povjereno je odgovarajućim resornim organima u svakom od pomenutih sektora. U praksi postoje značajni

problemi i neusaglašenosti oko kriterijuma za utvrđivanje kritične infrastrukture, što utiče i na definisanje mjera na njihovoj zaštiti[504].

O realnom stanju i aktuelnom nivou javno-privatnih partnerstava u području bezbjednosti i zaštite kritične infrastrukture u Bugarskoj i svjedoče ocjene o fragmentiranosti normativnog okvira, neefikasnoj saradnji angažovanih aktera javnog i privatnog sektora, rasprostranjenoj korupciji, zloupotrebama u procesu javnih nabavki i namještanju tendera, sivoj zoni poslovanja, nedovoljnoj stručnosti jednog broja operatora, sukobima interesa, te spregama pojedinih subjekata privatne bezbjednosti sa kriminalnim i tajkunskim strukturama.[505]

U Bugarskoj je odsustvo djelotvornog partnerstva između učesnika i zainteresovanih strana u režimu zaštite kritične infrastrukture uzrokovano i postojanjem mnoštva mreža, objekata i djelatnosti koje potpadaju pod nadležnost raznoraznih državnih i privatnih aktera, što predstavlja prepreku za njihovu efikasniju zaštitu. I u situacijama kada se može govoriti o postojanju saradnje i partnerstva između nadležnih državnih organa i privatnih bezbjednosnih kompanija, ta saradnja se nerijetko ostvaruje ad hoc ili nezvanično. Poseban problem predstavljaju slaba i neefikasna kontrola i nadzor u ovoj oblasti, s obzirom na činjenicu da je područje bezbjednosne zaštite opterećeno različitim nepravilnostima u postupcima javnih nabavki koje se tiču bezbjednosnih usluga. Za značajan dio operatora je karakteristično da zbog neispunjavanja kriterijuma stručnosti i opremljenosti kod javljanja na tendere idu na kriterijum najniže cijene, često zaobilazeći ključne bezbjednosne probleme izradom neadekvatnih elaborata. Ovo može takođe da predstavlja faktor koji privatni sektor podstiče na prelazak u sivu zonu poslovanja, mimo formalno utvrđenih pravila i standarda[506].

Pored toga nedostatak stručnog znanja, strateškog usmjerenja i jasnoće opterećuju sprovođenje režima zaštite kritične infrastrukture. Na to ukazuju i činjenice da su predstavnici privatnog sektora i samostalni eksperti za bezbjednost u principu isključeni iz procesa utvrđivanja kritičnosti i procjene rizika. Ovo se može smatrati nedostatkom sistema s obzirom da privatni sektor raspolaže operativnim znanjima, situacionom sviješću i obavještajnim podacima o aktuelnim bezbjednosnim prijetnjama. Nedostatak komunikacije na strateškom ili taktičkom nivou otežava mogućnost vlade da vrši kontrolu i nadzor režima sprovođenja kada nije u pitanju njeno vlasništvo. U takvom kontekstu razmjene informacija može biti teško ustanoviti da li privatne organizacije zaista dostavljaju relevantne informacije. U ovom scenariju, država preuzima funkciju koordinatora, a ne oslanja se pretjerano na nadzor i kontrolu. Pojedini eksperti smatraju da se ovakvo odsustvo stvarne komunikacije i otežano praćenje može otkloniti primjenom modela mrežnog upravljanja, samoregulacijom i adekvatnim i efikasnim korišćenjem javno-privatnih partnerstava[507].

Iz navedenog proističe zaključak da javno-privatno partnerstvo u zaštiti kritične infrastrukture u Bugarskoj nije na nivou koji bi trebalo očekivati od države koja je članica Evropske unije. S druge

[504] Dzhekova R., Kojouharov A.: Mission Critical, Mission Impossible – The Role of PSCs in Protecting Critical Infrastructure in Bulgaria, In: Klopfer F., Amstel van N.(eds.): *Private Security in Practice: Case studies from Southeast Europe*, DCAF, 2016, p. 55-57

[505] Dzhekova R., Rusev A.: Bulgaria, In: Franziska K.,, Amstel van N. (eds), *A Force for Good? Mapping the private security landscape in Southeast Europe*, DCAF Geneva 2015, p. 33.

[506] Dzhekova R., Kojouharov A.: Mission Critical, Mission Impossible – The Role of PSCs in Protecting Critical Infrastructure in Bulgaria, In: Klopfer F., and Amstel van N.(eds.): *Private Security in Practice: Case studies from Southeast Europe*, DCAF, 2016, p. 63

[507] Dunn-Cavelty M., Suter M.: Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection, *International Journal of Critical Infrastructure Protection*, 2, 2009, pp. 179-187.

strane, paradoksalno je i u neskladu sa evropskim trendovima da određeni pokazatelji ukazuju da je strateška kritična infrastruktura od značaja za nacionalnu bezbjednost koja se nalazi u državnom vlasništvu i koja je dalje u nadležnosti javnog sektora bezbjednosti, efikasnije zaštićena od objekata i resursa u čije su obezbjeđenje uključeni ugovorno angažovani akteri privatne bezbjednosti.

4.5.2.4. Javno-privatno partnerstvo u državama kandidatima za članstvo u EU – Studija slučaja partnerstva u obezbeđenju HE Đerdap

Jedan od pozitivnih Primjera razvoja javno-privatnog partnerstva u sektoru kritične infrastrukture država kandidata za članstvo u Evropskoj uniji je ugovorno regulisano obezbjeđenje hidroelektrane (HE) Đerdap, koju Republika Srbija zajednički koristi sa Rumunijom. Inače, HE Đerdap je jedna od 16 hidroelektrana, koje zajedno sa osam termoelektrana zajedno čine Elektroprivredu Srbije (EPS). Hidroelektrana Đerdap je ujedno i prolaz za rečni prevoz Dunavom i granični prelaz Srbije sa Rumunijom. Sve do 2013. godine je stalne bezbjednosne usluge na HE Đerdap isključivo pružalo unutrašnje obezbjeđenje elektrane. Prenošenje bezbjednosnih usluga na privatne partnere je bilo postepeno, a taj proces su omogućile promjene u srpskom zakonodavstvu koje su se odnosile na postupak privatizacije, javno-privatno partnerstvo i na privatnu bezbjednost.

Stalnu bezbjednost na HE Đerdap danas zajednički ostvaruju obezbjeđenje elektrane i na ugovornoj osnovi angažovane privatne kompanije za obezbjeđenje, koji dijele i odgovornost sa pojedine segmente bezbjednosti hidroelektrane. Do 2013. jedini ugovor za poslove obezbjeđenja imala je firma ćerka kompanije HE Đerdap. Nakon aktivnijeg uključivanja subjekata privatnog sektora, matični odjeljak za bezbjednost pokriva 30% fizičke zaštite, 70% tehničke zaštite i 90% zaštite od požara, dok ugovorne kompanije pružaju 70% fizičke zaštite, te 30% tehničke zaštite HE Đerdap. U skladu sa potrebama, dodatnu bezbjednost pruža regionalna policijska uprava, koja te poslove obavlja u saradnji sa graničnom policijom Srbije. S obzirom da se HE Đerdap nalazi na granici, srpsko-rumunske policijske snage imaju uspostavljene oblike zajedničke saradnje.[508]

Početak javno-privatnih partnerstava na području HE Đerdap vezuje se za 2014. godinu kada je menadžment hidroelektrane raspisao tender za bezbjednosne usluge na osnovu Zakona o javnim nabavkama, koji između ostalog sadrži i odredbu da se ugovor o pružanju usluga mora dodijeliti ponuđaču koji ima najnižu cenu, ili čija je ponuda ekonomski najpovoljnija[509]. Posao na tenderu je tada dobila privatna bezbjednosna kompanija G4S, a ne dotadašnji provajder, Đerdap usluge. Pomenuta ćerka firma je nakon toga uložila znatna sredstva u povećanje svojih kapaciteta, što joj se i isplatilo, jer je ubrzo nakon toga uključena kao podizvođač u pružanju bezbjednosnih usluga. Ipak, glavni pružalac usluga ostao je G4S. Ta firma je zajedno sa VIP Security obezbjeđivala 55% radne snage za te poslove. Na samozaštitu HE Đerdap je otpadalo 30%, a na Đerdap usluge preostalih 15% udjela. I u 2015. godini je sproveden postupak javne nabavke, pri čemu je taj postupak bio znatno konkretniji u odnosu na prethodnu godinu, jer je između ostalog sadržavao i cijenu usluge. Naime, HE Đerdap (naručilac) je predvidio da se cijena rada može korigovati u skladu sa povećanjem

[508] Milošević M., Petrović P.: Privatising the Security of Critical Infrastructure in Serbia– The Case of Private Security at the Hydropower Plant Djerdap, In: Klopfer F., Nelleke van A: (Eds.): *Private Security in Practice: Case studies from Southeast Europe*, DCAF, 2016, pr. 68-69.

[509] Zakon o javnim nabavkama, „*Službeni glasnik RS*“, br. 124/2012, 14/2015 i 68/2015,čl. 85

minimalnih zarada, te utvrdio najnižu cijenu rada ispod koje neće biti uzete u razmatranje dostavljene ponude. Kao i godinu dana ranije, i na tenderu 2015. godine je najbolji ponuđač bio G4S, koji posjeduje i veliko iskustvo u obezbjeđenju kritične infrastrukture u drugim državama. Politika ove kompanije je različita u odnosu na modele partnerstva, jer kada radi za privatnog subjekta razvija nove radne procedure, a kada ostvaruje partnerstvo sa državom, onda se pridržava propisa koje je država uspostavila. Angažovanjem ove kompanije unaprijeđen je sistem zaštite HE Đerdap, naročito u domenu teničkog obezbjeđenja, s obzirom da je ugrađena nova savremena oprema za video nadzor.

U cilju potpunije analize predmetnog slučaja, napomenimo da u datom trenutku zakonski okvir u Srbiji nije propisivao jasno bezbjednosne zahtjeve u domenu obezbjeđenja kritične infrastrukture, pa nije bilo u potpunosti jasno da li akteri privatne bezbjednosti mogu ili treba da igraju aktivnu ulogu u zaštiti ove infrastrukture. Na primjer, u Zakonu o vanrednim situacijama osoblje privatnog obezbjeđenja u Srbiji nije izričito navedeno na listi obučenih pravnih lica od značaja za usluge zaštite i spašavanja. Tada tek donijeti Zakon o privatnom obezbjeđenju je, s druge strane, sadržao poglavlje o „obavezno obezbjeđenim objektima“ u kojem su opisani dužnosti lica ili pravnih subjekata koji su pravno odgovorni za radove na lokalitetima od strateškog značaja za Republiku Srbiju, a čije oštećenje ili uništavanje mogu prouzrokovati ozbiljne posledice za život i zdravlje ljudi ili koji su od interesa za nacionalnu odbranu.[510]

[510] Milošević M., Petrović P.: Privatising the Security of Critical Infrastructure in Serbia – The Case of Private Security at the Hydropower Plant Djerdap, In: Klopfer F., Nelleke van A: (Eds.): *Private Security in Practice: Case studies from Southeast Europe*, DCAF, 2016, pp. 72-73

PETI DIO

EMPIRIJSKO ISTRAŽIVANJE

5.1. Konceptualni okvir

Empirijsko istraživanje pod opštim nazivom "Teorijski i normativni okvir zaštite kritične infrastrukture u Crnoj Gori", koje je realizovano za potrebe doktorske disertacije, po svojoj suštini je predstavljalo naučno istraživanje kojim se težilo sagledavanju indikatora stanja i veza među pojavama u toj oblasti. Istraživanje je sprovedeno u prvoj polovini 2019. godine tehnikom anonimne ankete zasnovane na skali procjene. Empirijskim istraživanjem je obuhvaćeno 102 ispitanika, zaposlenih u relevantnim ustanovama i organizacijama u Crnoj Gori, čija je djelatnost po svojoj prirodi neposredno povezana sa problematikom kritične infrastrukture, kao što su Regionalni vodovod Crnogorsko primorje, JP Elektroprivreda Crne Gore, željeznička infrastruktura Crne Gore, „Putevi", D.O.O. Podgorica, Direkcija za saobraćaj, Luka Bar, HE Piva, HE Pljevlja, HE Perućica, JKP Vodovod i kanalizacija-Podgorica, Crnogorski elektroprenosni sistem AD Podgorica, Javno preduzeće za nacionalne parkove, AD Pošta Crne Gore, Direktorat za vodoprivredu, Ministarstva poljoprivrede i ruralnog razvoja, MUP Sektor za vanredne situacije Crne Gore. Pored navedenih ustanova i organizacija istraživanjem su obuhvaćeni i ispitanici iz privatnih bezbjednosnih kompanija u Crnoj Gori. Na ovaj način su, sa aspekta ovog rada, ispitivanjem obuhvaćeni svi relevantni akteri javnog i privatnog sektora od značaja za zaštitu kritične infrastrukture u Crnoj Gori.

Anketni upitnik koji je sadržavao ukupno 25 pitanja, može se uslovno podijeliti u tri cjeline. Prvi dio upitnika je obuhvatio četiri opšta pitanja vezana za same ispitanike. Drugi dio upitnika se odnosio na problematiku kritične infrastrukture, a poslednji dio na stanje i perspektive javno-privatnog partnerstva. Od učesnika ankete se tražilo da obilježavanjem određene ponuđene deskriptivne vrijednosti (npr. ne, djelimično/nepotpuno, da, ne mogu da ocijenim) utvrde uticaj jedne pojave (procesa) na drugu. Pojedina pitanja su ispitanicima davala mogućnost da sami unesu i rangiraju odgovore ili da uz ponuđene definicije daju i sopstvene. Cilj ovako zasnovane skale procjene u okviru upitnika bio je da se prikupe stavovi, pogledi i mišljenja ispitanika o stanju, problemima i perspektivama javno-privatnog partnerstva u zaštiti kritične infrastrukture u Crnoj Gori.

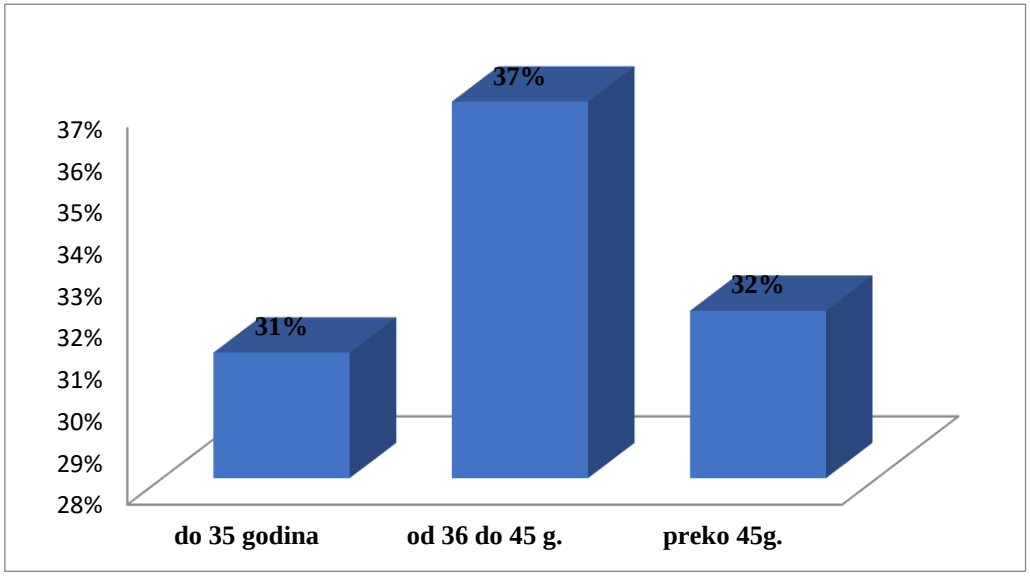
5.2. Rezultati ispitivanja tehnikom anonimne ankete

Prva četiri pitanja u anketnom upitniku bila su namijenjena utvrđivanju opštih podataka o ispitanicima koji su od značaja za predmetno istraživanje

1. Godine starosti i polna pripadnost ispitanika

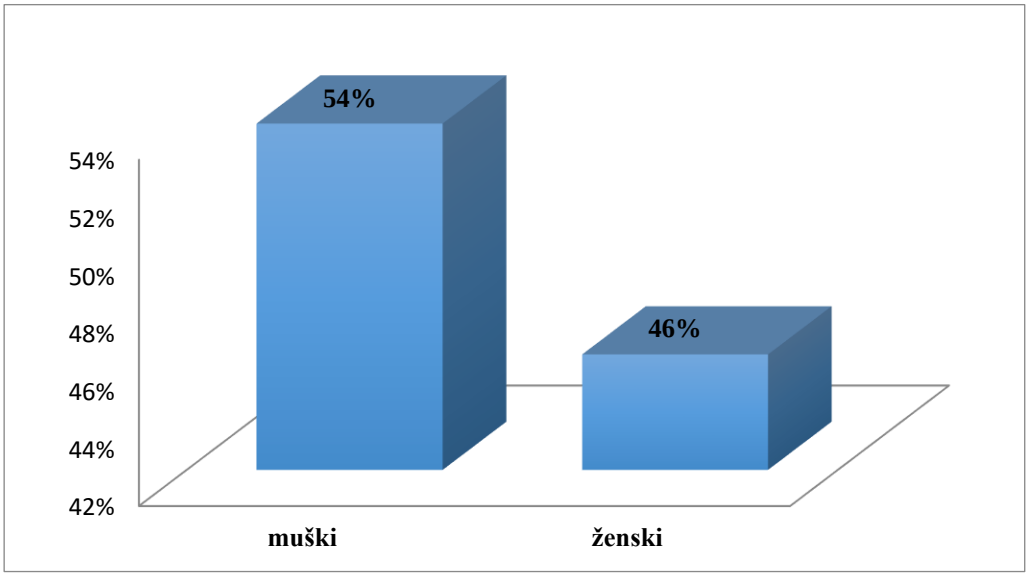
Kada se analizira starosna struktura ispitanika, možemo zaključiti da se radi o ravnomjernom rasporedu prema tri ponuđene kategorije. Povećan je broj ispitanika od 36 do 45 godina (37%), a zatim grupi ispitanika koji imaju preko 45 godina sa (33%), dok su najmanji procenat, 31% činili

ispitanici do 35 godina. To je ujedno i odraz stvarne starosne strukture stanovništva, s obzirom da se 40,16 % građana Crne Gore nalazi u grupi 25 do 54 godine života[511].



Grafikon br. 6.: Starosna struktura ispitanika

Polna struktura ispitanika ukazuje na relativno približnu zastupljenost oba pola među ispitanicima (muškarci 54%, žene 46%).

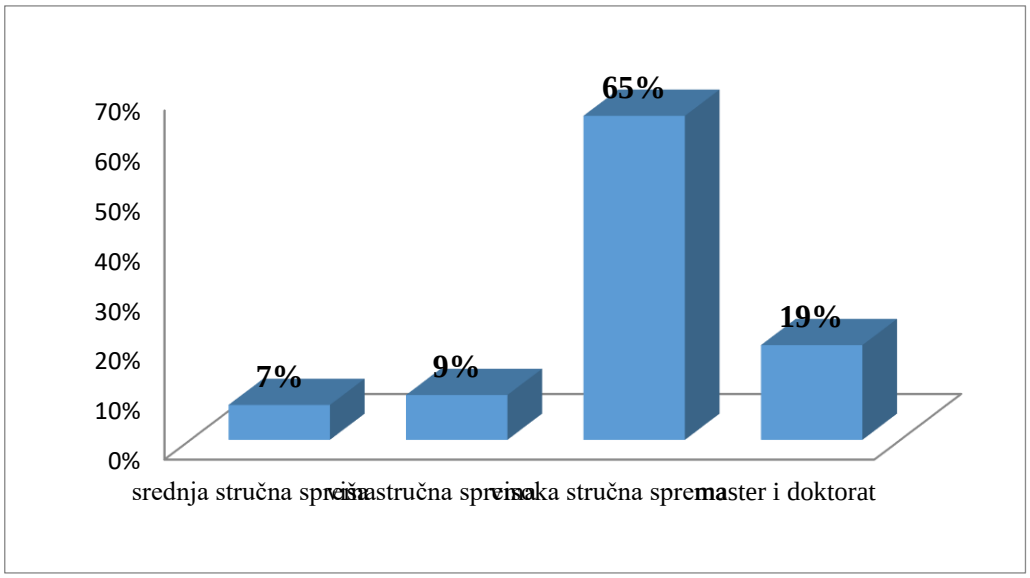


Grafikon br.7.: Polna zastupljenost ispitanika

2. Nivo stečenog obrazovanja

[511] Izvor: *CIA World factbook*, dostupno na: https://www.cia.gov/library/publications/resources/the-world-factbook/geos/mj.html

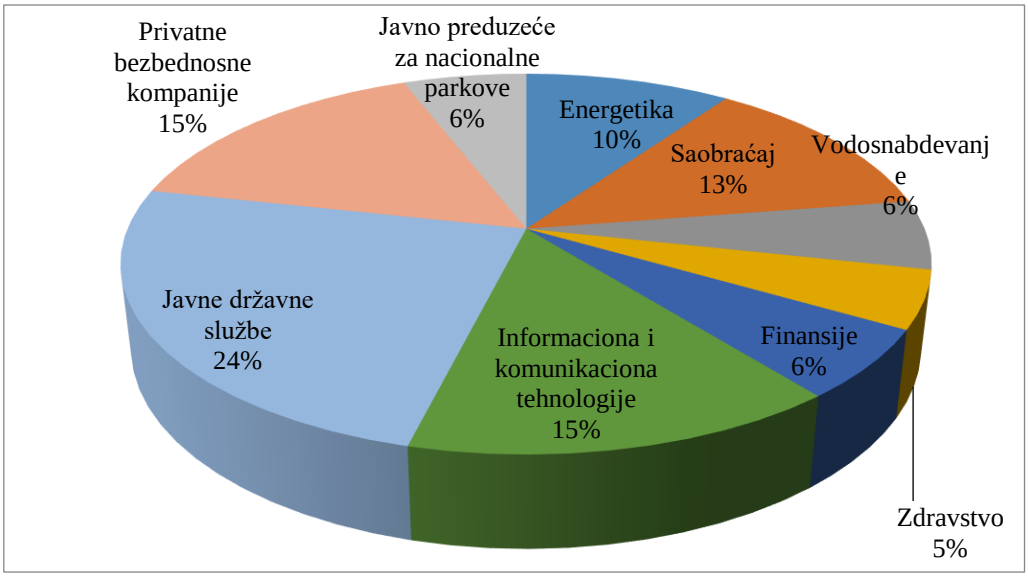
Školska sprema anketiranih lica je homogena, jer 65% njih ima visoku stručnu spremu, uz još 20 ispitanika (19%) sa završenim master studijama. S druge strane, svega 9% anketiranih je sa višom, a 7% sa srednjom stručnom spremom.



Grafikon br. 8.: Školska sprema ispitanika

3. Organizaciona cjelina zaposlenja ispitanika

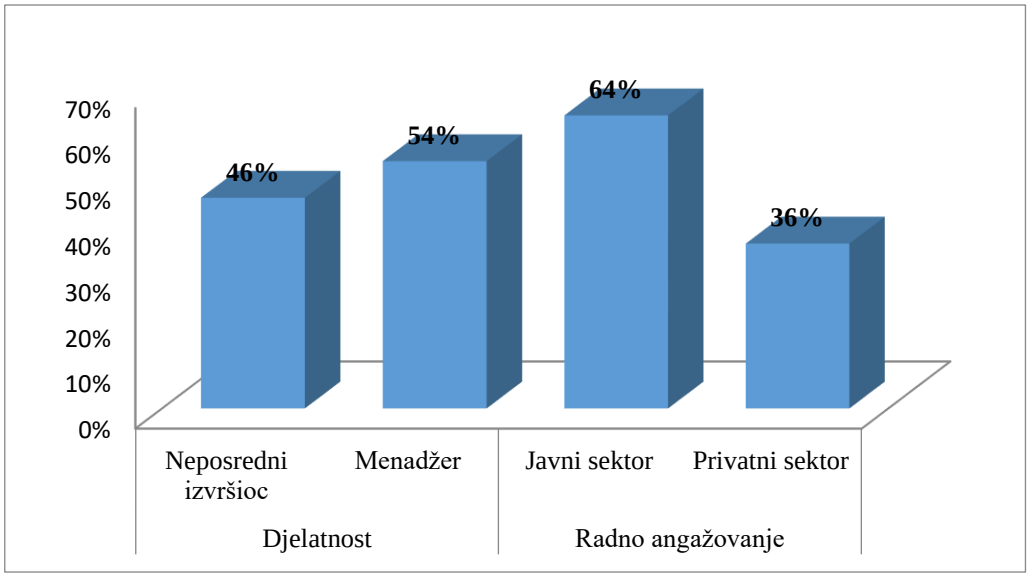
Iz ugla organizacionih cjelina iz kojih dolaze ispitanici, možemo zaključiti da uzorak u potpunosti odražava realnu strukturu različitih subjekata koji po svojoj prirodi mogu pripadati sektorima kritične infrastrukture Crne Gore.



Grafikon br. 10.: Organizacione cjeline u kojima su zaposleni ispitanici

4. Oblast stručnog angažovanja i poslova koje obavlja ispitanik

Iz ugla djelatnosti anketiranih, rezultati ispitivanja pokazuju da se 54% ispitanika nalazi na menadžerskim (upravnim) funkcijama, dok su 46% neposredni izvršioci. Sa aspekta radnog angažovanja ispitanika, 64% anketiranih je zaposleno u javnom, a 36% u privatnom sektoru.



Grafikon br. 9.: Djelatnost i radno angažovanje ispitanika

5.2.1. Kritična infrastruktura u percepciji ispitanika

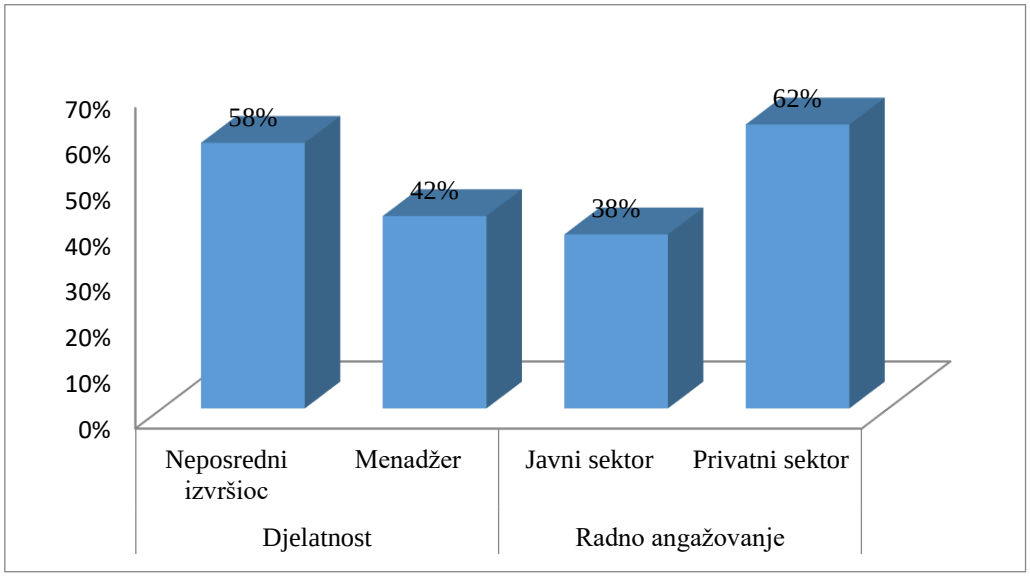
5. Šta Vi podrazumijevate pod pojmom kritična infrastruktura?

Ispitanicima su ponuđene tri definicije pojma kritična infrastruktura, a ostavljena im je i mogućnost da ponude sopstvenu. Analizom dobijenih odgovora, utvrđeno je da je relativna većina anketiranih (40%) prihvatila drugi predlog definicije, po kojoj kritična infrastruktura podrazumijeva „sisteme i sredstva bilo fizičke ili virtuelne koji su od vitalnog značaja za državu i čija nesposobnost ili uništenje može imati uticaj na bezbjednost, ekonomsku sigurnost, javno zdravlje ili bilo koju kombinaciju ovih stvari“. Navedeno određenje je ujedno definicija kritične infrastrukture SAD. Za treći predlog definicije se opredijelilo 31%, a za prvi 19% ispitanika. Učesnici ankete nisu koristili mogućnost da sami definišu pojam kritične infrastrukture. Analizirajući strukturu ispitanika koji su prihvatili drugi predlog možemo uočiti da se radi prvenstveno o muškim osobama starosti do 45 godina sa visokom stručnom spremom.

STAROSNA STRUKTURA			POL		ŠKOLSKA SPREMA			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
48%	34%	18%	63%	37%	25%	16%	42%	17%

Tabela br. 15.: Opšti podaci o ispitanicima koji su predložili drugi predlog definicije kritične infrastrukture

Analizirajući djelatnost ispitanika koji su pozitivno odgovorili na drugi predlog evidentno je da preovladavaju neposredni izvršioci kojima je ova definicija znatno jasnija i bliža u odnosu na one koji pripadaju upravljačkom dijelu organizacije u kojoj su zaposleni. S druge strane, najveći broj ispitanika koji se nalaze u privatnom sektoru (62%) je saglasan da je predmetna definicija optimalna za prostor Crne Gore. Ukoliko bismo dali neku opštu karakteristiku ispitanika koji su prihvatili drugi predlog onda je evidentno da se radi o mlađim licima muškog pola sa visokom stručnom spremom koji obavljaju određeni vid djelatnosti u privatnom sektoru.

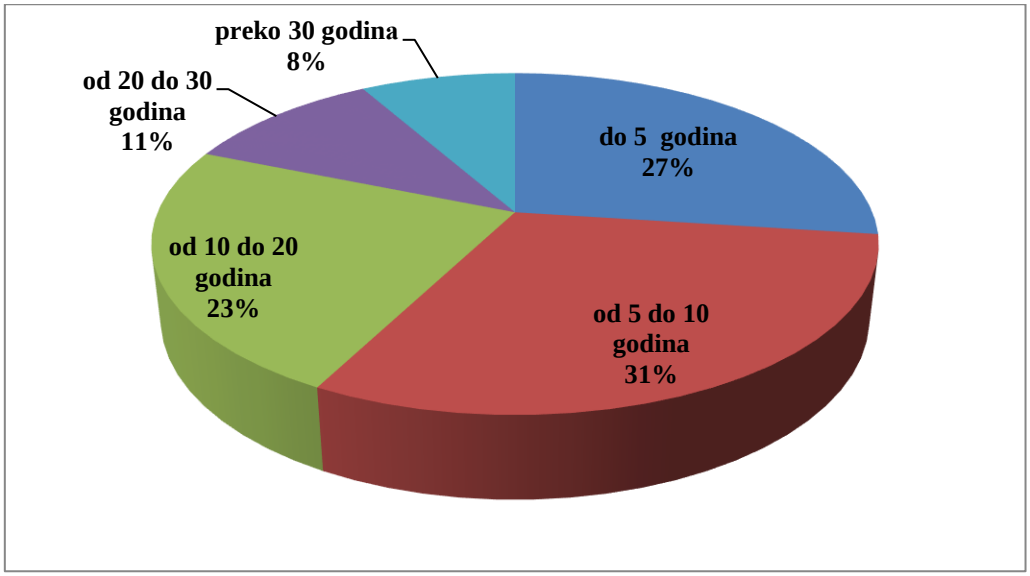


Grafikon br. 11.: Djelatnost i radno angažovanje ispitanika koji su prihvatili drugi predlog

6. Koliko godina se bavite poslovima vezanim za kritičnu infrastrukturu ?

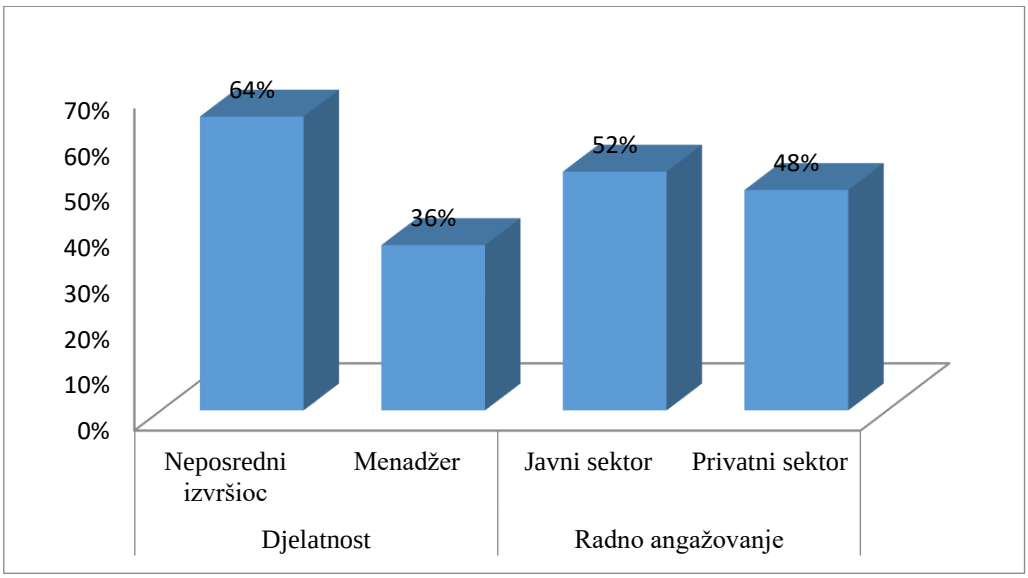
S obzirom da na percepciju ispitanika između ostalog utiče i njihovo bavljenje problematikom kritične infrastrukture, posebno pitanje bilo je vezano za vremenski period u kome se anketirana lica bave ovom problematikom. Iz dobijenih rezultata možemo uslovno zaključiti da je značajan dio

uzorka ispitanika još uvijek na „početku“ bavljenja djelatnostima vezanih za kritičnu infrastrukturu. Naime, 58% anketiranih se ovom oblašću bavi manje od 10 godina, dok je s druge strane najstarija grupa, sa preko 30 godina iskustva, najmanje zastupljena sa samo 8%. Navedeno ukazuje na opšti problem, jer je evidentno da u Crnoj Gori nedostaje kadar koji posjeduje odgovarajuće iskustvo u zaštiti kritične infrastrukture. Drugim riječima, nedostatak iskusnog kadra treba nadomjestiti kroz obrazovni proces mlađe populacije u cilju adekvatnog upravljanja zaštitom kritične infrastrukture na duži period. U vezi sa tim je od značaja planirati i izgraditi adekvatan i permanentan edukativni proces koji mora biti u funkciji zaštite kritične infrastrukture. U protivnom, upravljanje bezbjednošću kritične infrastrukture može biti prepušteno površnom i nedovoljno stručnom radu, što može predstavljati veliki problem naročito u kriznim situacijama kada profesionalan i stručan odnos ima prvorazredni značaj.



Grafikon br. 12.: Vremenski okvir bavljenja ispitanika poslovima kritične infrastrukture

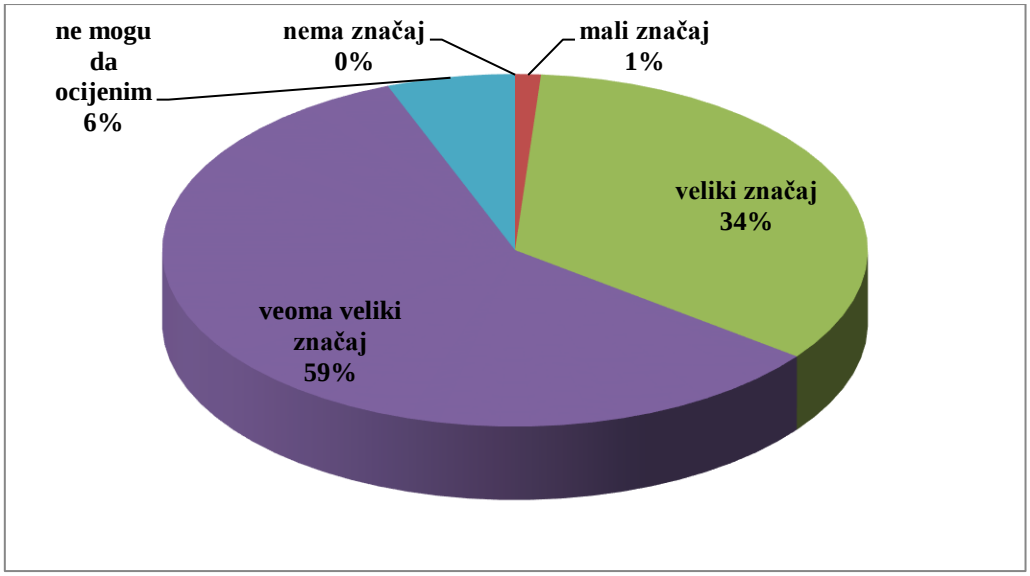
Potpunije analiziranje profila ispitanika koji u sektoru kritične infrastrukture obavljaju poslove manje od deset godina navodi na zaključak da se u najvećem broju slučajeva radi o neposrednim izvršiocima u svojim organizacionim cjelinama, pri čemu je njihovo radno angažovanje skoro ravnomjerno podijeljeno između javnog i privatnog sektora. Navedeno nas upućuje na ocjenu da je djelatnost kritične infrastrukture, bez obzira da li se radi o javnom ili privatnom sektoru, u značajnoj mjeri prepuštena mlađim kadrovima, što između ostalog znači i neophodnost njihovog pravilnog vođenja u izgradnji profesionalne karijere, uz već navedenu potrebu stalnog usavršavanja.



Grafikon br. 13.: Djelatnost i radno angažovanje najvećeg broja ispitanika koji se bave poslovima kritične infrastrukture

7. Koliki je značaj kritične infrastrukture za funkcionisanje države i društva?

Postavljanje pitanja o značaju kritične infrastrukture za funkcionisanje države i društva imalo je za cilj potpunije sagledavanje percepcije ispitanika u Crnoj Gori o toj problematici. Analiza dobijenih rezultata ukazuje da ispitanici to pitanje relativno ozbiljno shvataju, s obzirom da je 59% anketiranih odgovorilo da kritična infrastruktura ima veoma veliki značaj za funkcionisanje države i društva, a još 34% je taj značaj ocijenilo kao veliki. S druge strane, ostali ponuđeni odgovori su bili veoma malo zastupljeni, dok ponuđenu deskriptivnu vrijednost „nema značaja“ niko nije zaokružio.



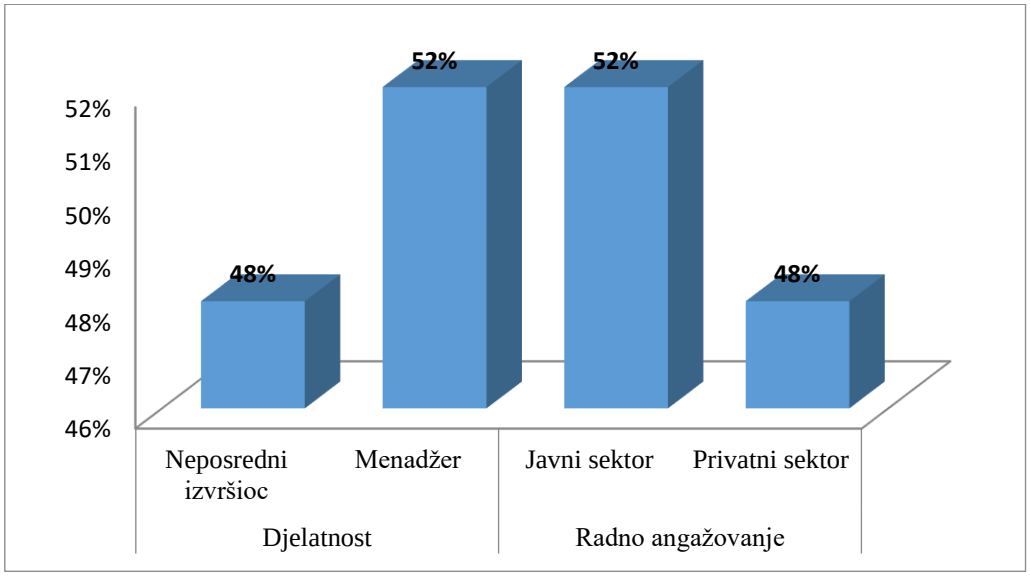
Grafikon br. 14.: Značaj kritične infrastrukture za funkcionisanje države i društva

U strukturi ispitanika koji smatraju da kritična infrastruktura ima veoma veliki značaj za funkcionisanje države i društva možemo uočiti ravnomjeran trend kada je u pitanju starosna struktura anketiranih. Drugim riječima, bez obzira da li se radi o mlađim ili starijim ispitanicima, opšte je prepoznat značaj funkcionisanja kritične infrastrukture. Ukoliko posmatramo polnu strukturu ispitanika, može se zaključiti da za anketirana lica muškog pola kritična infrastruktura ima veći značaj u odnosu na ispitanike ženskog pola. Analiza odgovora prema školskoj spremi anketiranih ukazuje da za visoko obrazovane ispitanike kritična infrastruktura ima znatno veći značaj od niže obrazovanih anketiranih lica.

STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
35%	33%	32%	56%	44%	11%	22%	35%	32%

Tabela br. 16.: Podaci o ispitanicima za koje kritična infrastruktura ima veoma veliki značaj

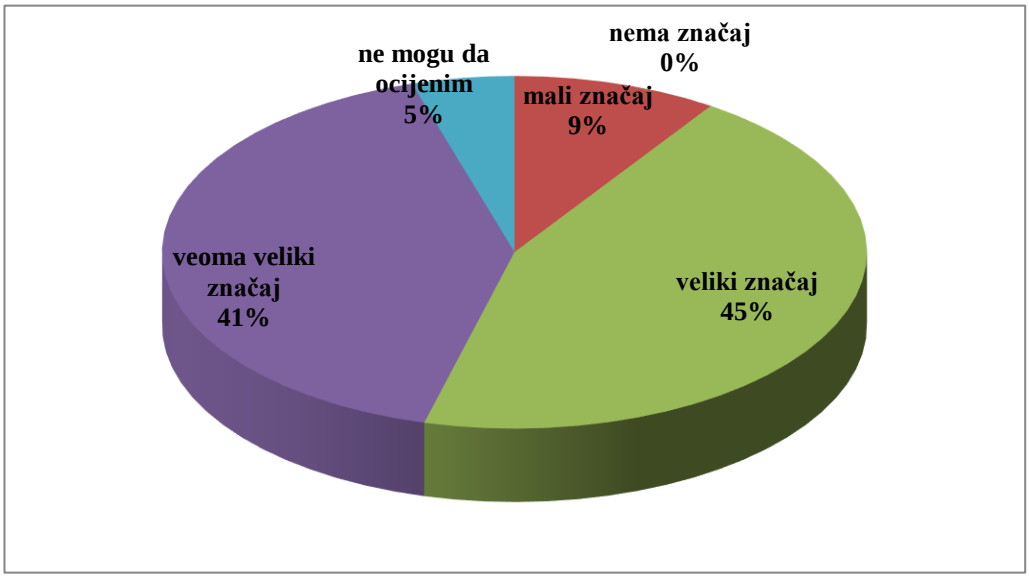
Podaci o navedenom uzorku ispitanika koji ukazuju na njihovu djelatnost i radno angažovanje su takođe donekle izjednačeni. Naime, bez obzira da li se radi o menadžerima ili neposrednim izvršiocima postoji saglasnost o značaju funkcionisanja kritične infrastrukture. S druge strane, i za ispitanike javnog, kako i privatnog sektora kritična infrastruktura ima veoma veliki značaj. Iz navedenog odgovora ispitanika možemo zaključiti da u Crnoj Gori postoji opšte razumijevanje i saglasnost o značaju kritične infrastrukture. To je od posebnog značaja jer predstavlja osnovu za dalje adekvatno razvijanje kulture i svijesti u ovoj oblasti.



Grafikon br. 15.: Podaci o djelatnostima i radnom angažovanju ispitanika za koje kritična infrastruktura ima veoma veliki značaj

8. Koliki je značaj vaše organizacije za funkcionisanje države i društva ?

Analiza dobijenih odgovora ukazuje da najveći broj ispitanika svoju organizaciju percipira kao značajnu za funkcionisanje države Crne Gore i crnogorskog društva u cjelini. U vezi sa tim, relativna većina anketiranih smatra da organizacije u kojima rade imaju veliki značaj 45%, a nešto manji broj ispitanika, tačnije 41%, taj značaj doživljava kao veoma veliki. Nasuprot tome, niko od anketiranih nije zaokružio odgovor „nema značaj“, a svega 5% njih nije moglo da taj značaj ocijeni. Odgovori na navedeno pitanje su u korelaciji sa prethodnim pitanjem u kome su takođe ispitanici potvrdili značaj, odnosno pravilan odnos i percepciju važnosti kritične infrastrukture za nesmetano funkcionisanje države i društva. Pored toga, navedeno potvrđuje doslednost ispitanika u ovom istraživanju, bez obzira da li se radi o javnom ili privatnom sektoru u Crnoj Gori.



Grafikon br. 16.: Značaj organizacije (ustanove) iz koje dolaze ispitanici za funkcionisanje države i društva

Kao i kod prethodnog pitanja i u ovom je slučaju struktura ispitanika ravnomjerno raspoređena iz ugla starosne strukture, dok je polna struktura na strani muškog dijela ispitanika. S druge strane, najveći broj ispitanika koji je svojoj organizaciji za funkcionisanje države i društva dao veliki značaj, pripada grupi visoko obrazovanih kadrova. Ukoliko odgovore na ovom pitanju uporedimo sa prethodnim pitanjem, možemo zaključiti da su ispitanici kritičnu infrastrukturu države prevashodno posmatrali iz ugla organizacije u kojoj su zaposleni i koja po prirodi pripada ovom sektoru.

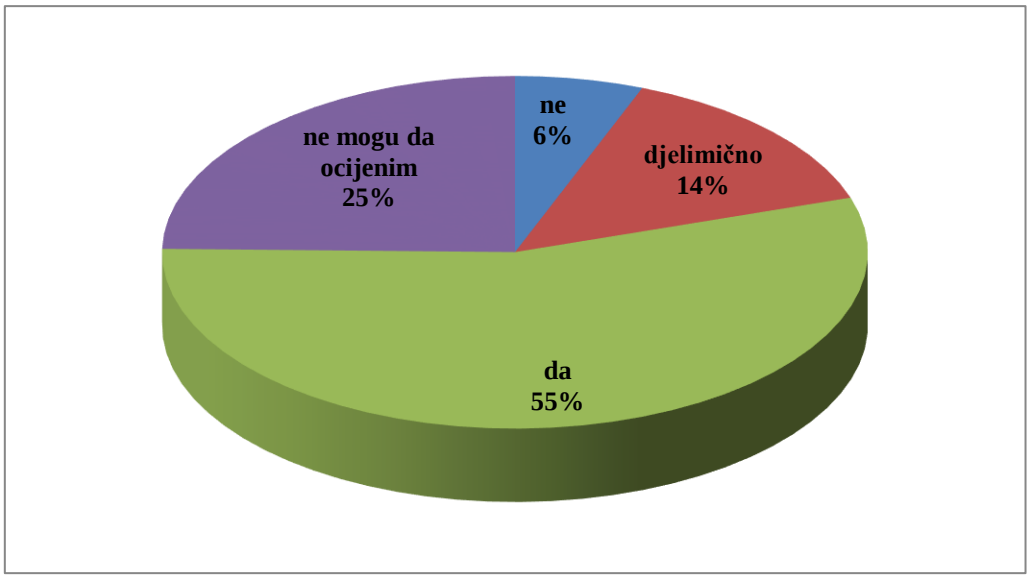
STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
32%	34%	34%	54%	46%	13%	24%	33%	30%

Tabela br. 17.: Podaci o isipitanicima koji su kao veliki značaj ocijenili svoju organizaciju za funkcionisanje države i društva

Kada se posmatra djelatnost i radno angažovanje navedenog uzorka ispitanika dobijamo rezultate koji su u velikoj mjeri identični prethodnim. Drugim riječima, 48% neposrednih izvršilaca i 52% menadžera opredijelilo se za opciju velikog značaja, kao što je to slučaj sa javnim sektorom (52%) i privatnim sektorom (48%). I u ovom slučaju postignut je veliki stepen homogenizacije ispitanika.

9. Da li je u Crnoj Gori potrebno donošenje posebnog zakona iz oblasti zaštite kritične infrastrukture?

Prema rezultatima ankete, ispitanici su nedvosmisleno potvrdili potrebu za zakonskim uređenjem zaštite kritične infrastrukture, s obzirom da se za donošenje posebnog zakona izjasnilo njih 55%. S druge strane, za drugačije (parcijalno/djelimično) rešenje ovog problema je bilo 14%, dok samo 6% ispitanika smatra da izmene zakonskog okvira nisu potrebne. Karakteristično je i da čak 25% anketiranih nije imalo stav o tom pitanju.



Grafikon br. 17.: Odgovori ispitanika o potrebi donošenja posebnog zakona o zaštiti kritične infrastrukture

O potrebi donošenja novih zakonskih odredbi se izjasnio najveći broj ispitanika koji pripadaju starosnim grupama do 45 godina, što se prethodno potvrdilo i u pojedinim navedenim odgovorima, prema kojima mlađa propulacija ima percepciju neophodnosti promjena u ovoj oblasti. Isti je slučaj i kada se posmatra školska sprema anketiranih lica, s obzirom da visoko obrazovani ispitanici takođe u značajnoj većini smatraju da je potrebno donošenje posebnog zakona koji bi u fokusu pažnje imao kritičnu infrastrukturu Crne Gore.

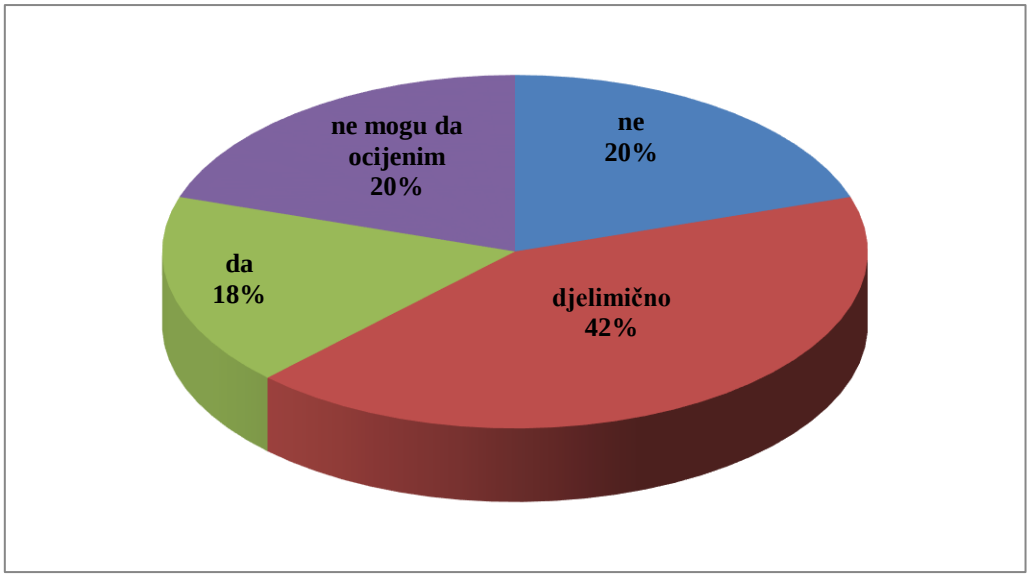
STAROSNA STRUKTURA			POL		ŠKOLSKA SPREMA			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
42%	43%	15%	52%	48%	15%	26%	31%	38%

Tabela br. 18.: Osnovni podaci o ispitanicima koji su iskazali potrebi donošenja posebnog zakona o zaštiti kritične infrastrukture

Kao i prethodnim slučajevima i ovdje postoji saglasnost javnog i privatnog sektora o neophodnosti donošenja posebnog zakona kojim bi bila regulisana predmetna oblast. U vezi sa tim, nije od značaja ni djelatnost ispitanika jer po ovom pitanju postoji saglasnost za novo zakonsko uređenje kritične infrastrukture.

10. Da li je postojeća zakonska regulativa zaštite kritične infrastrukture usklađena sa savremenim oblicima ugrožavanja (terorizam, organizovani kriminal) vaše organizacije?

Analiza dobijenih rezultata ukazuje na postojanje određenih nedoumica kod ispitanika, s obzorom na veoma raznoliku distribuciju stavova o usklađenosti aktuelne zakonske regulative u području zaštite kritične infrastrukture sa potrebom odgovora na savremene oblike ugrožavanja. Tako su odgovori „da“ (18%) i ne (20%) skoro približni, dok više nego dvostruko veći broj anketiranih (42%) percipiraju postojeće stanje kao djelimičnu usklađenost. Ukupno uzev, odgovori ipak ukazuju na potrebu dogradnje normativnog okvira. Procenat onih koji nemaju stav o tom pitanju je ponovo visok (20%).



Grafikon br. 18: Da li je postojeća zakonska regulativa zaštite kritične infrastrukture usklađena sa savremenim oblicima ugrožavanja (terorizam, organizovani kriminala) organizacije (ustanove) ispitanika

Analizirajući strukturu ispitanika koji su se izjasnili za djelimičnu usklađenost regulative u ovoj oblasti u odnosu na oblike ugrožavanja, prednjači mlađa populacija (starosna grupa do 35 godina) u odnosu na ostale grupe. S druge strane, analiza odgovora prema školskoj spremi pokazuje određenu podijeljenost među visokoobrazovanim ispitanicima.

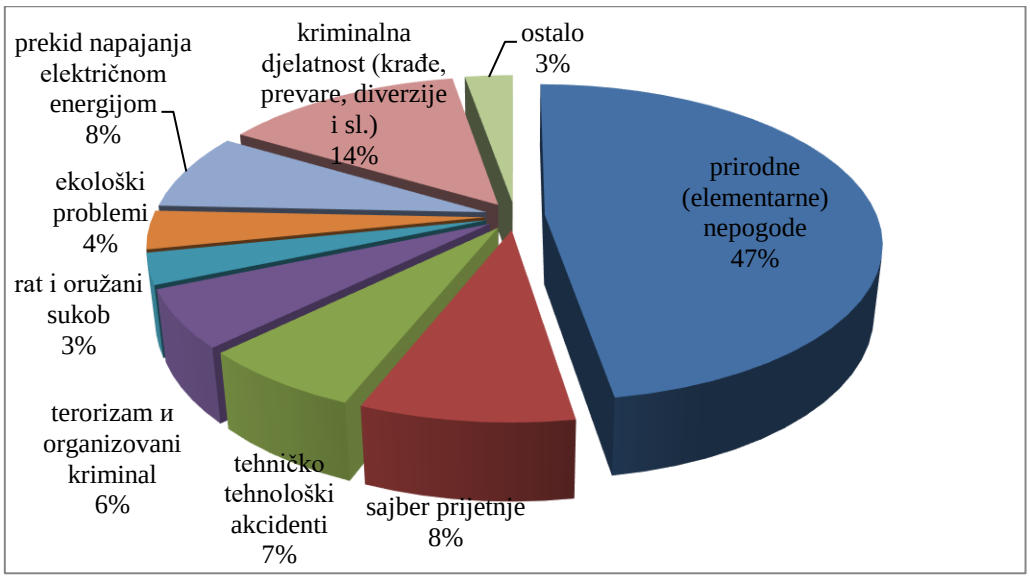
STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
47%	35%	28%	52%	48%	13%	24%	33%	30%

Tabela br.19.: Osnovni podaci o ispitanicima koji su se izjasnili da je postojeća regulativa zaštite kritične infrastrukture delimično usklađena sa savremenim oblicima ugrožavanja organizacije

Analizom djelatnosti i radnog angažovanja ispitanika uočava se ravnomjerna zastupljenost neposrednih izvršilaca i lica koja su raspoređena na upravljačke funkcije, nezavisno od toga da li se radi o privatnom ili javnom sektoru. Evidentno je da ne postoji razlika između javnog i privatnog sektora kada se radi o ocjeni postojeće regulative sa stanovišta savremenih oblika ugrožavanja organizacija iz kojih ispitanici dolaze. To je ujedno i zajednički imenitelj oba sektora, što možemo okarakterisati kao pozitivan trend, između ostalog i zbog činjenice da savremeni oblici ugrožavanja ne prave razliku između tih sektora.

11. Koja su tri najvažnija potencijalna rizika koja mogu dovesti do vanredne situacije u vašoj organizaciji ?

Ovo pitanje je bilo koncipirano na način da je ispitanicima ostavljena mogućnost da sami unesu i vrednosno rangiraju odgovore. Dobijeni rezultati ukazuju da najveći broj odgovora (47%) najvažnijim potencijalnim rizikom koji može dovesti do vanredne situacije u organizaciji smatra prirodne nepogode (poplave, zemljotresi). Daleko iza toga se kao potencijalni rizici percipiraju kriminalne djelatnosti (14%), sajber prijetnje (8%), te terorizam i organizovani kriminal (6%). Shodno ovim odgovorima, terorizam se ne smatra aktuelnom prijetnjom po bezbjednost kritične infrastrukture u Crnoj Gori. Uz to, ekološki problemi su veoma nisko na listi rizika (4%).



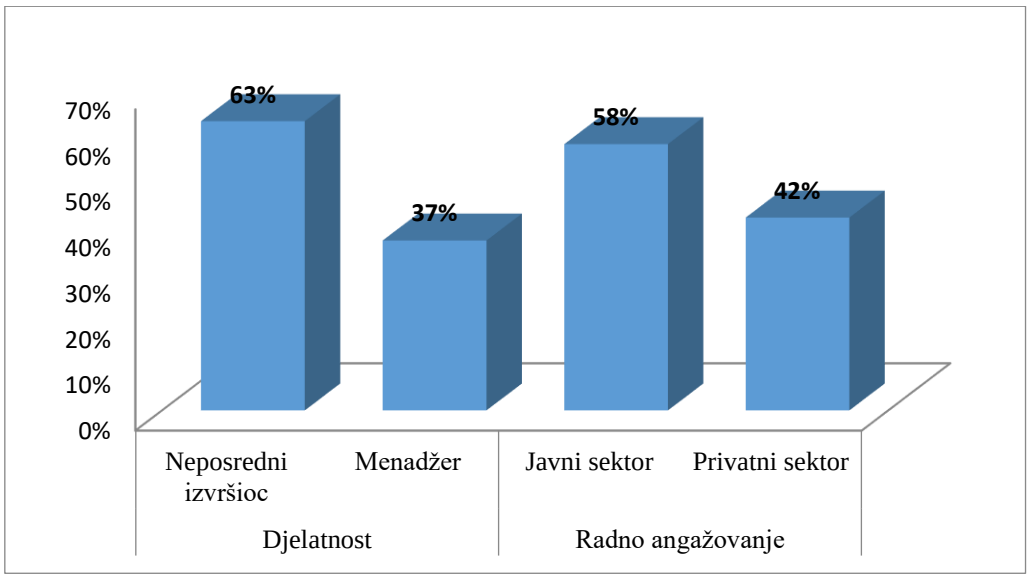
Grafikon br. 19.: Koja su tri najvažnija potencijalna rizika koja mogu dovesti do vanredne situacije u organizaciji iz koje dolaze ispitanici

U strukturi ispitanika koji su prirodne nepogode označili kao najvažniji rizik najveći stepen percepcije imaju ispitanici srednjeg doba, te najstarija grupa ispitanika. Interesantno je da je ovo jedno od pitanja u kojima ženska populacija imala najveći stepen homogenizacije. S druge strane, ispitanici sa višom i visokom stručnom spremom u najvećem broju smatraju da su elementarne nepogode najrasprostranjeniji rizik koji može dovesti do vanredne situacije u njihovoj organizaciji

STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
27%	42%	31%	48%	52%	23%	24%	33%	20%

Tabela br. 20.: Osnovni podaci o ispitanicima koji smatraju da elementarne nepogode mogu dovesti do vanredne situacije u organizaciji iz koje dolaze ispitanici

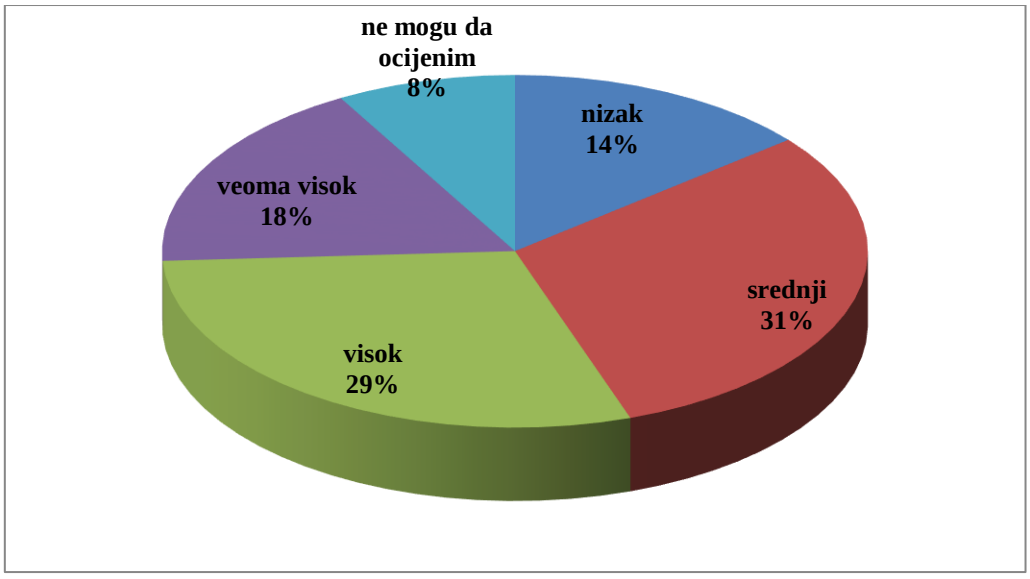
U odnosu na djelatnost ispitanika najveći je broj neposrednih izvršilaca koji smatraju da su elementarne nepogode najznačajniji oblik ugrožavanja bezbjednosti organizacije iz koje dolaze. Prema rezultatima istraživanja evidentno je da je javni sektor znatno više ugrožen elementarnim nepogodama u odnosu na privatni. To je donekle i opravdano s obzirom da je privatni sektor u Crnoj Gori u razvoju i da postepeno zadobija svoje mesto u društvenoj podjeli rada.



Grafikon br. 20.: Djelatnost i angažovanje ispitanika koji koji smatraju da elementarne nepogode mogu dovesti do vanredne situacije u organizaciji iz koje dolaze ispitanici

12. Koliki je stepen opasnosti od prirodnih i tehničko-tehnoloških rizika u vašoj sredini ?

Analiza odgovora ispitanika pokazuje da približno polovina njih stepen opasnosti od prirodnih i tehničko-tehnoloških rizika u svojoj sredini percipira kao visok (29%) ili veoma visok (18%). Kao srednji stepen opasnosti ga vidi 31% anketiranih, a kao nizak samo 8%, što ukupno ukazuje na relativno razvijenu svijest ispitanika o potrebi zaštite sredine gdje žive i rade.



Grafikon br. 21.: Stepen opasnosti od prirodnih i tehničko-tehnoloških rizika u sredini ispitanika

Analizirajući strukturu ispitanika koji su se opredijelili za srednji stepen opasnosti u svojoj sredini od prirodnih i tehničko-tehnoloških rizika, najveći broj anketiranih lica pripada srednjem starosnom dobu. S druge strane, to su ujedno i lica sa završenom školskom spremom u rasponu od

srednje do visoke. Evidentno je da najmanji broj ispitanika, najstarije starosne grupe i ujedno sa najvećim stepenom obrazovanja percipira stepen rizika od prirodnih i tehničko-tehnoloških rizika kao srednji.

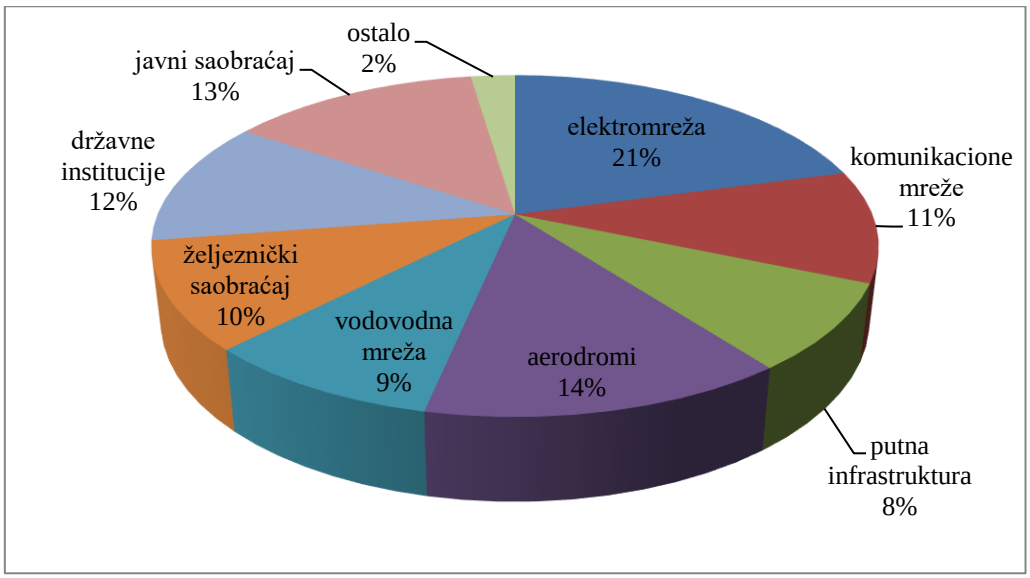
STAROSNA STRUKTURA			POL		ŠKOLSKA SPREMA			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
32%	48%	20%	52%	48%	26%	28%	33%	15%

Tabela br. 21.: Opšti podaci o ispitanicima koji su prihvatili srednji stepen opasnosti od prirodnih i tehničko-tehnoloških rizika u svojoj sredini

Ukoliko analiziramo djelatnost ispitanika onda srednji stepen opasnosti od prirodnih i tehničko-tehnoloških rizika u znatno većoj mjeri možemo vezivati za percepciju neposrednih izvršilaca (64%) u odnosu na menadžere (36%). S druge strane, kada je riječ o sektoru iz koga dolaze, ne postoji bitna razlika između javnog i privatnog sektora. Ovdje treba napomenuti da su u periodu prije realizacije istraživanja pojedini djelovi Crne Gore bili pogođeni elementarnim nepogodama, što je umnogome uticalo na percepciju ispitanika. Uz to, evidentno je da i kod ovog pitanja ne postoji bitna razlika između javnog i privatnog sektora.

13.Koja su tri objekta kritične infrastrukture u Crnoj Gori po vašem mišljenju najviše izloženi potencijalnim terorističkim napadima?

Ovo pitanje je bilo koncipirano na način da je ispitanicima ostavljena mogućnost da sami unesu i vrednosno rangiraju odgovore. Dobijeni rezultati ukazuju da veliku disperziranost odgovora, odnosno na stav da u Crnoj Gori nema objekata i resursa kritične infrastrukture koji odskaču daleko od ostalih u pogledu potencijalne ugroženosti terorističkim napadima. Interesantno je da najveći broj odgovora kao potencijalnu metu percipira elektromrežu (21%). Znatno niže su rangirani aerodromi (14%), javni objekti (13%), državne institucije (12%), komunikacione mreže (11%) i željeznički saobraćaj (10%).

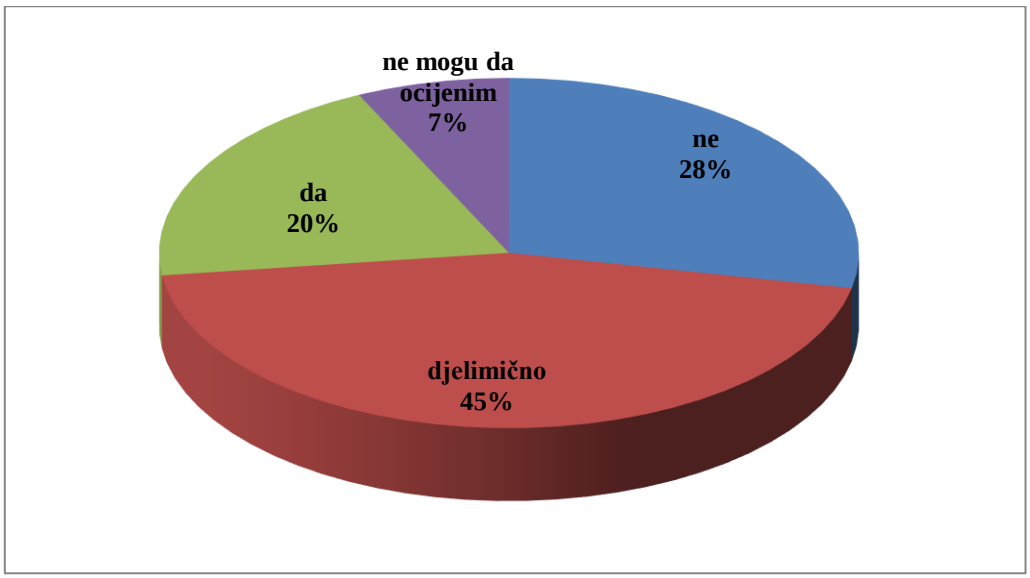


Grafikon br. 22.: Koji su objekti kritične infrastrukture u Crnoj Gori po vašem mišljenju najviše izloženi terorističkom napadu

Analizirajući rezultate odgovora za navedeno pitanje možemo doći do opšteg zaključka da ne postoji homogenizacija ispitanika prema mogućnostima ispoljavanja terorističkog akta na objekte infrastrukture. Evidentno je da ispitanici vide širok spektar objekata infrastrukture kao metu mogućih terorističkih napada, što ukazuje na različitu percepciju ovog problema. S druge strane, različita percepcija ispitanika je prvenstveno posledica mjesta njihovog radnog angažovanja, odnosno da se mogućnost terorističkog napada posmatra iz znatno užeg ugla iako je u stvarnosti nesumnjivo da navedeni objekti mogu biti potencijalne terorističke mete. Karakteristično je i da kod navedenih odgovora ne postoji polaritet između javnog i privatnog sektora, što možemo smatrati pozitivnim.

14. Da li je potpuni državni nadzor jedino adekvatno rešenje u zaštiti kritične infrastrukture ?

Posljednje pitanje u dijelu upitnika koje se odnosilo na kritičnu infrastrukturu ticalo se državnog nadzora kao jedinog adekvatnog rješenja u zaštiti kritične infrastrukture. Prema rezultatima ankete, mišljenja ispitanika oko toga su podijeljena. Relativna većina ispitanika (45%) se zalaže za određeni vid državnog nadzora, odnosno djelimično se slaže sa tim rešenjem. Protiv državnog nadzora je 28% anketiranih, a 20% njih je saglasno da je potpuni državni nadzor u toj oblasti jedino adekvatno rešenje za zaštitu kritične infrastrukture u Crnoj Gori. Ostali, odnosno 7% ispitanika nije u stanju da ocijeni ispravnost pomenute teze. Napomenimo da navedene rezultate treba posmatrati u svijetlu činjenice da Crna Gora, kao i zemlje u njenom okruženju, ima dugu istoriju i tradiciju dominacije javnog nad privatnim sektorom u mnogim segmentima društvenog života, pa i u domenu zaštite kritične infrastrukture.



Grafikon br. 23.: Da li je potpuni državni nadzor jedino adekvatno rešenje u zaštiti kritične infrastrukture

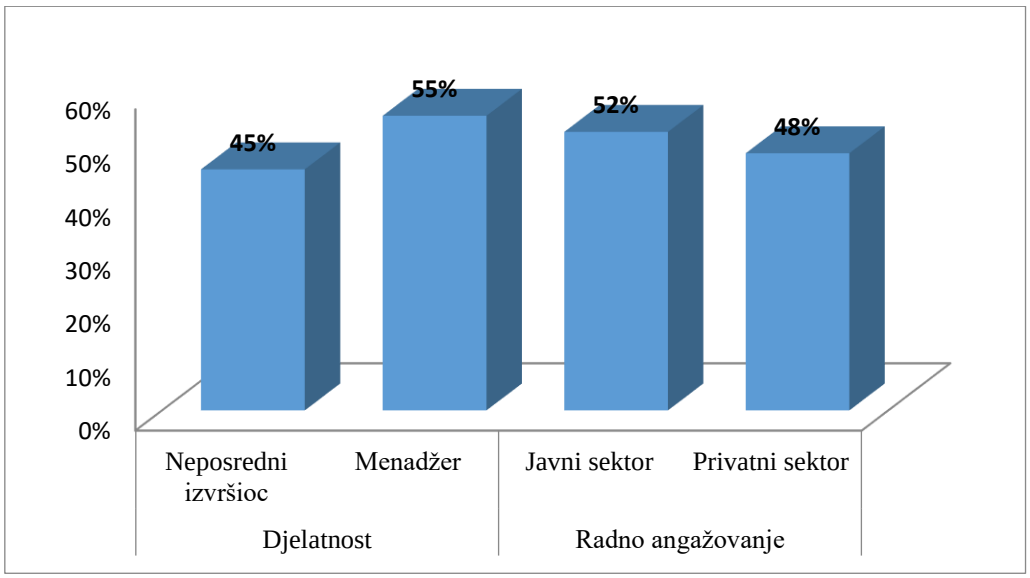
Analizirajući strukturu ispitanika koji potpuni državni nadzor u zaštiti kritične infrastrukture smatraju djelimičnim rješenjem, možemo zaključiti da se radi o mlađoj populaciji do 35 godina (48%), za razliku od najstarije grupe ispitanika koja smatra da država treba da ostane jedini akter u zaštiti kritične infrastrukture. To je u korelaciji sa mnogim odgovorima u prethodnim pitanjima, po kojima mlađa populacija zagovara nova rješenja u različitim segmentima.

S druge strane, kod odgovora na ovo pitanje je polna pripadnost donekle izjednačena i ne odudara u odnosu na prethodne odgovore. Kao i kod prethodnih pitanja, za djelimični nadzor države u zaštiti kritične infrastrukture se većinski izjašnjavaju ispitanici sa visokom školskom spremom.

STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
48%	30%	22%	52%	48%	18%	22%	33%	27%

Tabela br. 22.: Opšti podaci o ispitanicima koji su se odlučili za djelimični nadzor države u zaštiti kritične infrastrukture

Analizirajući djelatnost i radno angažovanje ispitanika evidentna je ujednačenost kao opšta karakteristika odgovora. Naime, i neposredni izvršioci kao i oni ispitanici koji pripadaju upravljačkom dijelu su se odlučili za djelimični nadzor države u zaštiti kritične infrastrukture. To je slučaj i kod kriterijuma radnog angažovanja anketiranih lica, što umnogome odgovara rezultatima kod prethodnih pitanja, što ujedno predstavlja šansu za izgradnju partnerstva između dva sektora.



Grafikon br. 24.: Djelatnost i radno angažovanje ispitanika koji su se odlučili za djelimični nadzor države u zaštiti kritične infrastrukture

Na osnovu svega navedenog, analiza rezultata istraživanja u domenu kritične infrastrukture može ukazati na neke opšte zaključke. Najvažniji zaključak je da u ovom segmentu ne postoji antagonizam između javnog i privatnog sektora vezano za izjašnjavanje po najvažnijim pitanjima. Pored navedenog, postoje i saglasnosti o određenim stavovima, na primjer da država ne može samostalno vršiti nadzor nad sektorom kritične infrastrukture, ili da se po pitanju zaštite kritične infrastrukture otvara potreba uspostavljanja javno-privatnog partnerstva sa privatnim sektorom bezbjednosti. Od značaja je i percepcija da je potrebna nova zakonska regulativa koja bi uključila savremeni koncept kritične infrastrukture. To je ujedno i realnost s obzirom na spoljno-političko opredjeljenje Crne Gore u procesu priključenja EU.

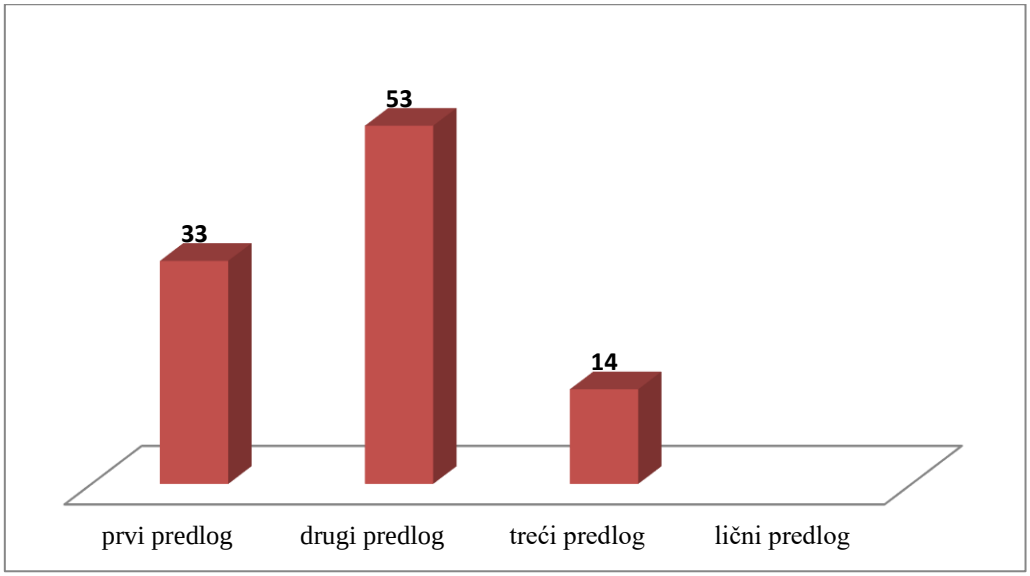
Analiza strukture ispitanika koji su većinski prihvatili navedena rješenja i predloge, evidentno je da se prije svega radi o mlađoj populaciji koja u suštini privatni sektor posmatra kao realnost u društvu, a samim tim i u zaštiti kritične infrastrukture. To je i očekivan odgovor s obzirom na opštu činjenicu da mladi ljudi u većoj mjeri teže određenim promjenama u društvu u odnosu na starije generacije. U vezi sa tim su i poklapanja očekivanih odgovora sa stepenom školske spreme ispitanika, posebno kada se posmatra visoko obrazovani kadar.

5.2.2. Privatni sektor bezbjednosti kao javno-privatno partnerstvo u percepciji ispitanika

15. Šta Vi podrazumijevate pod pojmom javno-privatno partnerstvo?

Ispitanicima su ponuđene tri definicije pojma javno-privatno partnerstvo, a ostavljena im je i mogućnost da ponude sopstvenu. Analizom dobijenih odgovora, utvrđeno je da je većina anketiranih (53%) prihvatila drugi predlog definicije prema kojoj predmetni pojam predstavlja „udruživanje između javnog i privatnog sektora zasnovano na obostranim interesima i ekspertizama partnera, koje najefikasnije zadovoljava definisane javne potrebe, uz adekvatnu upotrebu resursa, podjelu rizika i dobiti“. Trećina ispitanika (33%) smatra adekvatnom prvu ponuđenu definiciju, prema kojoj je javno-

privatno partnerstvo „zajedničko (kooperativno) djelovanje države s privatnim kompanijama u proizvodnji javnih proizvoda ili pružanju usluga“. Najzad, za treći predlog definicije („investicioni projekti transferisani privatnom sektoru koje je tradicionalno izvršavao ili finansirao javni sektor“), opredijelilo se 14% ispitanika. Učesnici ankete nisu koristili mogućnost da sami definišu pojam javno-privatnog partnerstva.



Grafikon br. 25.: Pojam javno-privatno partnerstvo-rezultati istraživanja

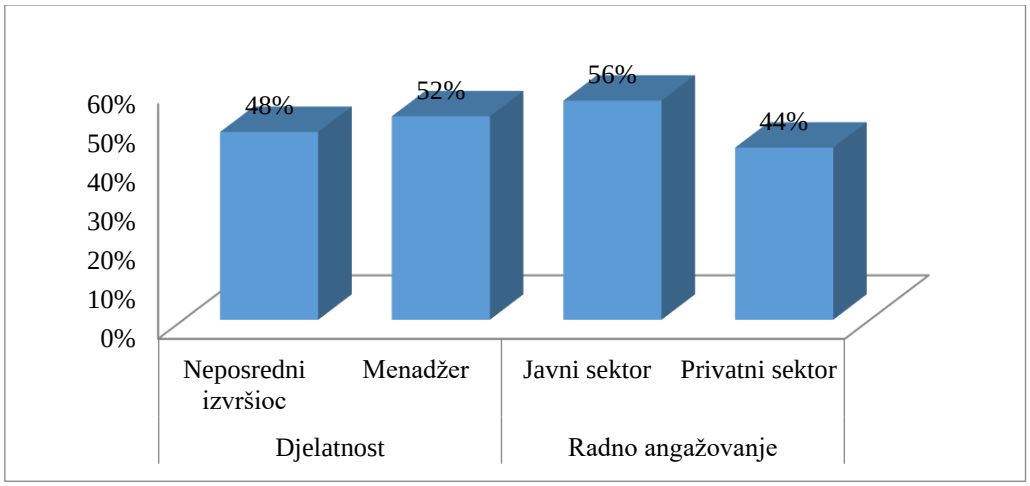
Analizirajući strukturu ispitanika koji su prihvatili drugi predlog definisanja javno-privatnog partnerstva, možemo zaključiti da se prvenstveno radi o licima starosti između 36 i 45 godina (48%), za razliku od starijih koji ovaj predlog ne percipiraju kao adekvatan za definisanje pojma javno-privatnog partnerstva. Analiza odgovora prema školskoj spremi anketiranih ukazuje da je za visokoobrazovane ispitanike drugi ponuđeni predlog i najprihvatljiviji jer odražava suštinu javno-privatnog partnerstva. Evidentno je da su navedeni rezultati u korelaciji sa strukturom ispitanika i u dijelu koji se odnosio na kritičnu infrastrukturu.

STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
32%	48%	20%	54%	46%	23%	22%	33%	22%

Tabela br. 23: Opšti podaci o ispitanicima koji su prihvatili drugi predlog definisanja javno-privatnog partnerstva

Na osnovu analize djelatnosti ispitanika, evidentno je da je predloženo određenje znatno bliže učesnicima ankete koji se nalaze u u upravljačkom dijelu svoje organizacije za razliku od onih koji su na pozicijama neposrednih izvršilaca. S druge strane, prihvaćeni predlog je bliži ispitanicima u

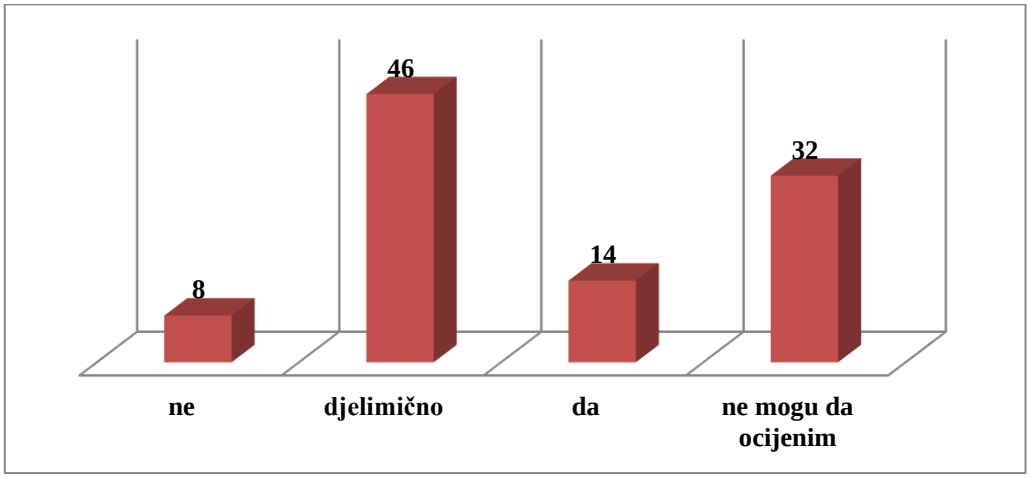
javnom sektoru. Većinski prihvaćeni predlog najpotpunije odražava suštinu javno-privatnog partnerstva, jer obuhvata najvažnije komponente kao što su ekspertiza učesnika partnerstva, javne potrebe i podjela rizika i dobiti, kao vodilje u saradnji javnog i privatnog sektora.



Grafikon br. 26.: Djelatnost i angažovanje ispitanika koji su prihvatili drugi predlog definisanja javno-privatnog partnerstva

16. Da li postojeći propisi adekvatno uređuju oblast javno-privatnog partnerstva u Crnoj Gori ?

Analiza dobijenih rezultata ukazuje na specifičnost materije javno-privatnog partnerstva u Crnoj Gori i na postojanje određenih nedoumica kod ispitanika, s obzirom da skoro trećina njih (32%) nije bila u stanju da se izjasni oko adekvatnosti postojećeg zakonskog okvira u toj oblasti, a da čak 46% anketiranih tu adekvatnost percipira kao djelimičnu. Rezolutni odgovori su u značajnoj manjini – „da“ 14% i „ne“ 8%.



Grafikon br.27.: Da li postojeća zakonska regulativa adekvatno uređuje oblast javno-privatnog partnerstva u Crnoj Gori

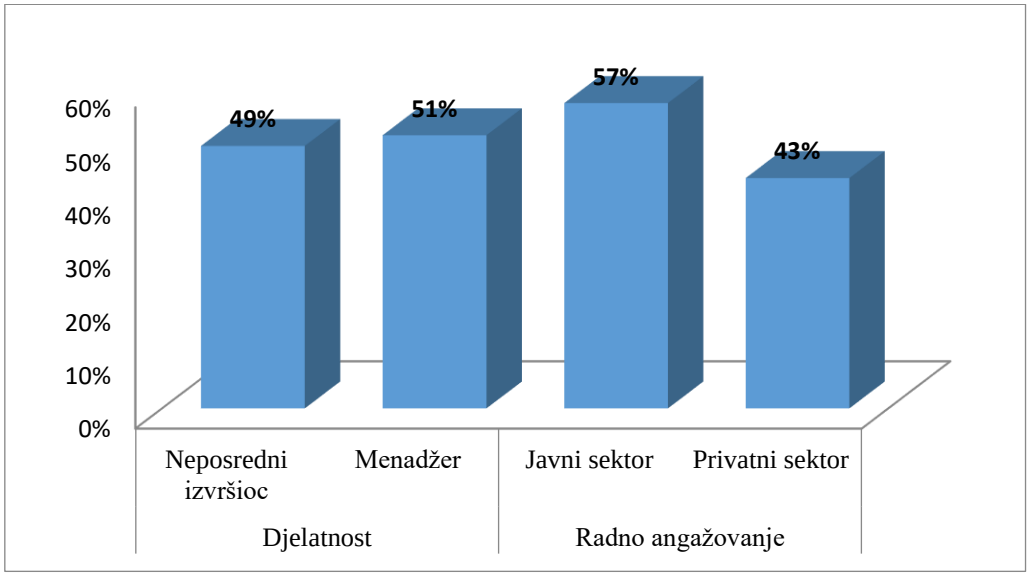
Na osnovu rezultata istraživanja evidentno je da postojeća zakonska regulativa u oblasti javno-privatnog partnerstva treba da pretrpi određene izmjene. To je opšti zaključak ispitanika od 36 do 45

godina muške populacije, sa završenom najmanje visokom stručnom spremom. I u ovom segmentu imamo korelaciju sa strukturom ispitanika koji su dali slične odgovore i na prethodna pitanja.

STAROSNA STRUKTURA			POL		ŠKOLSKA SPREMA			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
32%	49%	19%	52%	48%	12%	24%	31%	33%

Tabela br. 24.: Opšti podaci o ispitanicima koji smatraju da postojeća zakonska regulativa djelimično uređuje oblast javno-privatnog partnerstva u Crnoj Gori

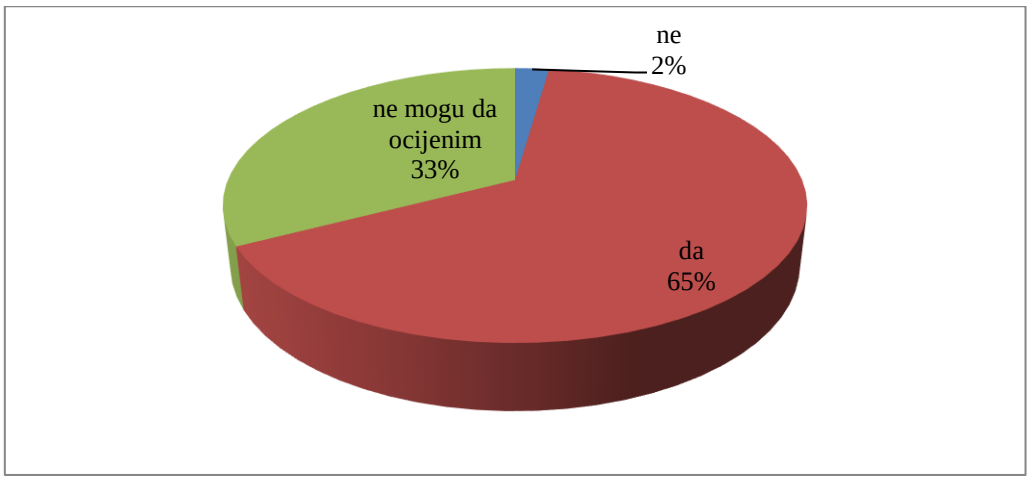
Djelatnost ispitanika ne pokazuje značajnu razliku između neposrednih izvršilaca i menadžera, s obzirom da je neznatna razlika između navedenih kriterijuma podjele anketiranih lica. Drugim riječima, i jedni i drugi smatraju da postojeća zakonska regulativa samo djelimično uređuje oblast javno-privatnog partnerstva u Crnoj Gori. Pored navedenog, posebno je važno da anketirani pripadnici javnog sektora u znatno većem broju percipiraju da postojeću zakonsku regulativu treba prilagoditi aktuelnim potrebama u izgradnji javno-privatnog partnerstva u Crnoj Gori.



Grafikon br. 28.: Djelatnost i radno angažovanje ispitanika koji smatraju da postojeća zakonska regulativa djelimično uređuje oblast javno-privatnog partnerstva u Crnoj Gori

17. Da li je u Crnoj Gori potrebno donošenje posebnog zakona o javno-privatnom partnerstvu ?

Prema dobijenim rezultatima, učesnici ankete su se ubjedljivom većinom (65%) izjasnili za zakonsko uređenje javno-privatnog partnerstva kroz donošenje posebnog zakona, dok samo 2% ispitanika zastupa stav da za to nema potrebe. Visok je, međutim, i procenat onih koji o tom pitanju nisu mogli da se izjasne (33%). Treba napomenuti da je u periodu nakon sprovođenja ankete Predlog zakona o javno-privatnom partnerstvu Crne Gore upućen u skupštinsku proceduru.

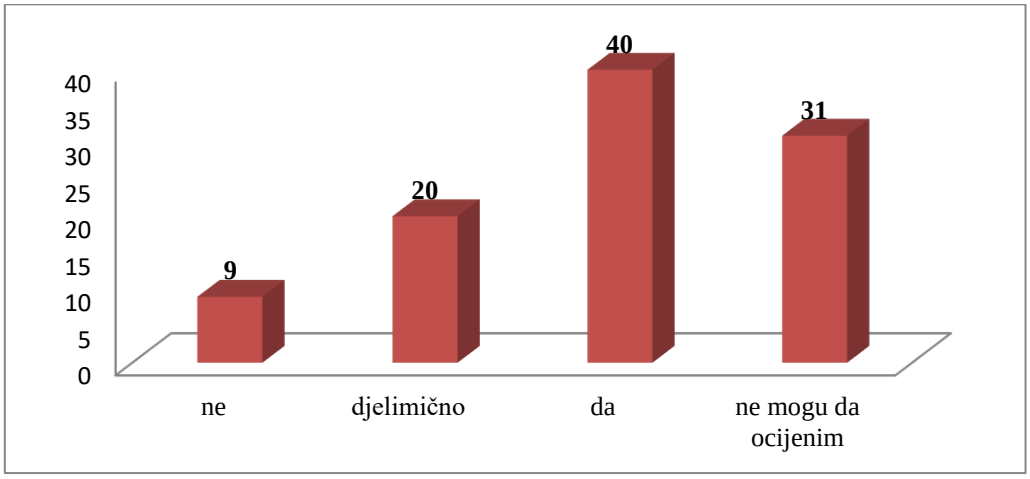


Grafikon br. 29.: Da li je potrebno donošenje novog zakona o javno-privatnom partnerstvu

S obzirom na korelaciju sa prethodnim pitanjem, u odgovorima imamo istu strukturu ispitanika koji smatraju da je potrebno donošenje novog zakona kojim bi se u potpunosti uredila oblast javno-privatnog partnerstva u Crnoj Gori. Naime, i u ovom slučaju najveći broj ispitanika koji su se za to izjasnili je srednje starosne dobi, muškog pola i sa najmanje visokom stručnom spremom. Pored toga, identična je i zastupljenost neposrednih izvršilaca i menadžera u organizacijama iz koje dolaze. S druge strane, evidentno je da je javni sektor posebno zainteresovan za donošenje zakona kojim bi država uredila ovu oblast.

18. Da li je model javno-privatnog partnerstva primjenljiv u zaštiti kritične infrastrukture Crne Gore?

Na veoma važno pitanje o primjenljivosti modela javno-privatnog partnerstva u području zaštite kritične infrastrukture u Crnoj Gori tek je relativna većina od 40% ispitanika dala nedvosmisleno potvrdan odgovor, a još 20% anketiranih smatra da je taj model djelimično primjenljiv. S druge strane, negativan stav o tome ima svega 9% ispitanika, uz značajan postotak (31%) onih koji o tom pitanju nisu mogli da se izjasne.



Grafikon br. 30.: Da li je model javno-privatnog partnerstva primjenljiv u zaštiti kritične infrastrukture Crne Gore

Prema starosnoj dobi, najveći broj ispitanika koji model javno-privatnog partnerstva u području zaštite kritične infrastrukture u Crnoj Gori smatraju primjenljivim je do 35 godina (48%) a najmanji preko 45 godine sa 18%. To se može smatrati očekivanim, s obzirom na činjenicu da starije generacije i dalje imaju povjerenje prvenstveno u državne organe i njihove kapacitete. Za promjenu ovog stereotipa neophodan je duži vremenski period ali i veća transparentnost funkcionisanja privatnog sektora bezbjednosti.

Analiza školske spreme anketiranih lica ukazuje da visoko obrazovani ispitanici (54%) u odnosu na ostale imaju veće povjerenje u privatni sektor i mogućnost stvaranja javno-privatnog partnerstva u zaštiti kritične infrastrukture. Sigurno je na navedene rezultate uticala i percepcija dosadašnjih stečenih iskustava u radu sa privatnim sektorom.

STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
48%	34%	18%	63%	37%	5%	6%	54%	35%

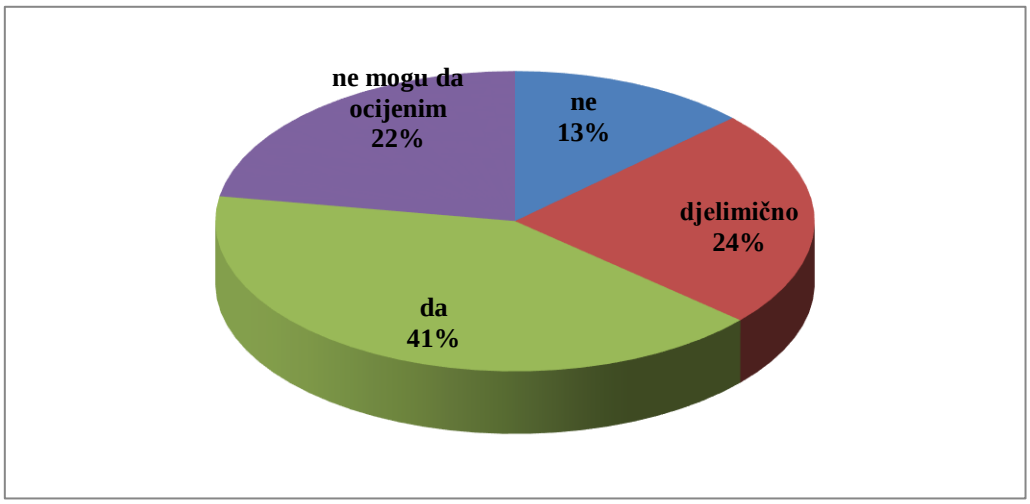
Tabela br.25.: Podaci o ispitanicima koji su saglasni sa mogućnošću javno-privatnog partnerstva u zaštiti kritične infrastrukture

Kada je riječ o djelatnostima ispitanika i njihovom radnom angažovanju, evidentno je da rukovodeći kadar (menadžeri) ima u znatno većoj mjeri pozitivan odnos prema predmetnom partnerstvu (66%) za razliku od neposrednih izvršilaca.

Kada se razmatra radno angažovanje ispitanika, evidentan je stav pripadnika privatnog sektora da taj sektor posjeduje kapacitete za stvaranje javno-privatnog partnerstva i da može da uspješno učestvuje u zaštiti kritične infrastrukture. Pored toga, analiza odgovora ukazuje i da javni sektor izražava vjerovanje u mogućnosti privatnog sektora. To ukazuje da državni sektor ne posmatra privatni sektor isključivo kao suparnički, već i kao način da u konkurenciji unapređuje sopstvene usluge. Navedeno potvrđuje da prema privatnom sektoru ispitanici imaju pretežno pozitivan stav, po kome isti ima kapacitete da zajednički djeluje sa javnim sektorom u zaštiti kritične infrastrukture.

19. Da li je model javno-privatnog partnerstva primenljiv u vašoj organizaciji ?

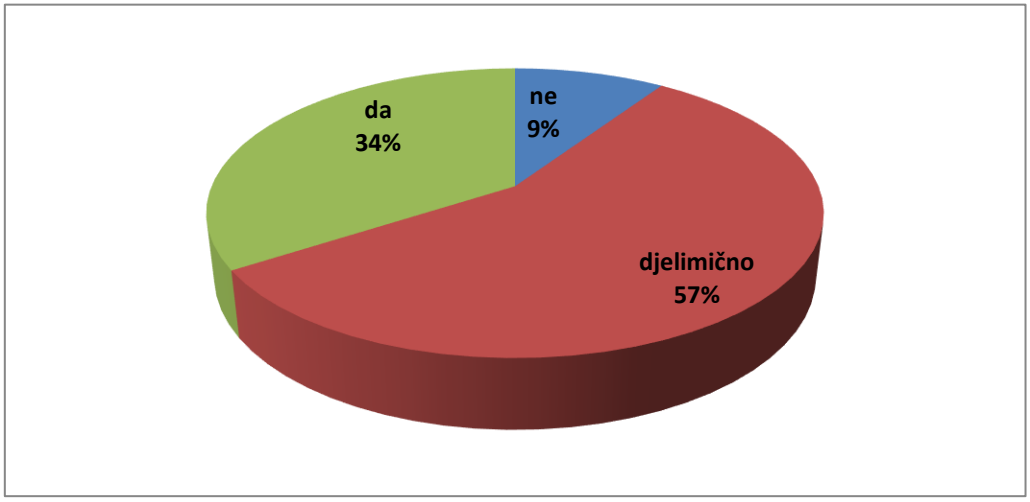
Pitanje se po svojoj suštini nadovezalo na prethodno, te su se mogli i očekivati slični rezultati ankete. Naime, relativna većina od 41% ispitanika smatra da se model javno-privatnog partnerstva može primijeniti u organizaciji u kojoj su zaposleni, uz još 24% anketiranih čiji je stav da je taj model djelimično primjenljiv u njihovoj sredini. O toj mogućnosti se negativno izjasnilo 13% ispitanika, uz relativno visok procenat (22%) anketiranih koji o tom pitanju nisu imali stav.



Grafikon br. 31.: Da li je model javno-privatnog partnerstva primjenljiv u vašoj organizaciji

20. Da li privatnom sektoru bezbjednosti treba zakonom omogućiti investiranje u zaštitu kritične infrastrukture u Crnoj Gori ?

Dobijeni rezultati ukazuju da velika većina ispitanika u osnovi podržava zakonsku mogućnost investiranja privatnog sektora bezbjednosti u zaštitu kritične infrastrukture u Crnoj Gori, ali da o tome zadržava i određene rezerve. Naime, apsolutna većina anketiranih (57%) zastupa stav da to treba djelimično omogućiti, dok 34% ispitanika bezrezervno podržava takvu opciju. Negativnu percepciju privatnih ulaganja u bezbjednost i zaštitu kritične infrastrukture ima svega 9% učesnika ankete.



Grafikon br.32.: Da li privatnom sektoru bezbjednosti treba zakonom omogućiti investiranje u zaštitu kritične infrastrukture

Analizirajući starosnu strukturu ispitanika koji smatraju da privatnom sektoru treba djelimično omogućiti investiranje u zaštiti kritične infrastrukture, možemo uočiti sličnosti kao i kod prethodnih odgovora jer se i u ovom slučaju radi o mlađoj populaciji koja očito ima pozitivan odnos prema

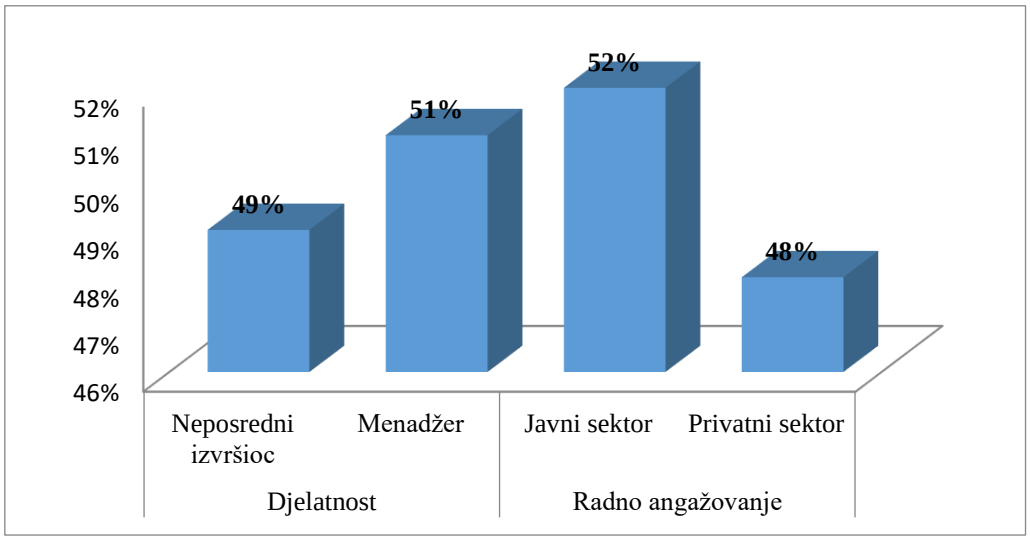
privatnom sektoru. U vezi sa tim su i njihova pozitivna iskustva koja su stekli u kontaktima sa privatnim sektorom bezbjednosti što je sigurno doprinijelo izgradnji njihove pozitivne percepcije.

Polna pripadnost ispitanika nije od značaja u odgovoru na ovo pitanje, s obzirom na ravnomjernu zastupljenost polova. Kada se radi o školskoj spremi, najveći broj ispitanika koji su dali potvrdan odgovor pripada grupi sa najvećim stepenom obrazovanja, što je u korelaciji sa prethodnim pitanjima, u vezi kojih su ispitanici iz ove grupe imali pozitivan odnos prema privatnom sektoru kao i mogućnostima stvaranja javno-privatnog partnerstva i slično.

STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
48%	34%	18%	52%	48%	5%	6%	54%	35%

Tabela br. 26.: Opšti podaci o ispitanicima koji smatraju da privatnom sektoru bezbjednosti treba omogućiti djelimično investiranje u zaštitu kritične infrastrukture

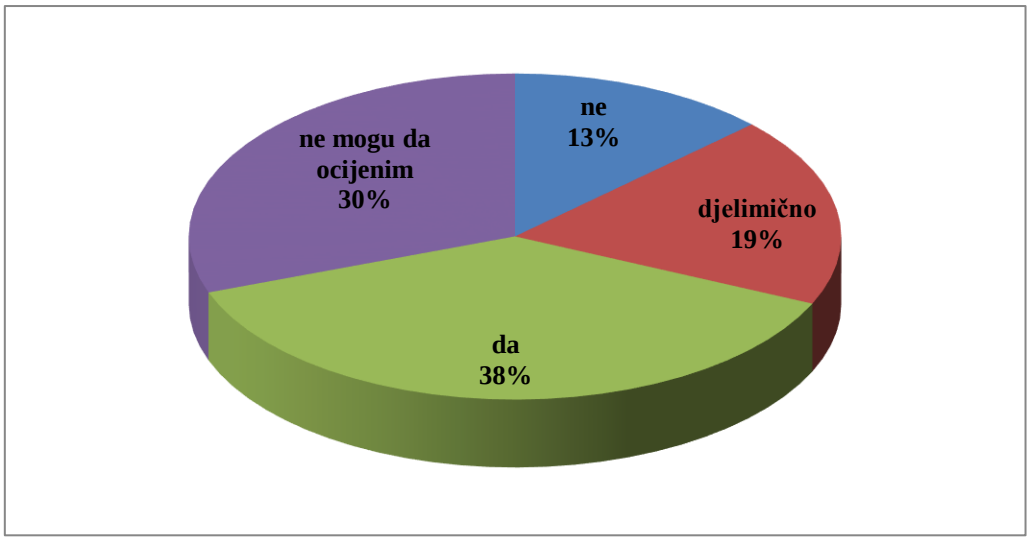
Analizirajući djelatnost i radno angažovanje ispitanika koji su prihvatili navedenu opciju uočavamo nepostojanje suštinskih razlika iz ova dva kriterijuma. Naime, i za neposredne izvršioce kao i za one ispitanike koji se svrstavaju u upravljački dio svojih organizacija je moguće da privatni sektor bezbjednosti u određenim okvirima učestvuje u zaštiti kritične infrastrukture. Posebno je važno i da pripadnici javnog sektora pozitivno percipiraju mogućnost angažovanja privatnog sektora u zaštiti kritične infrastrukture. Uključivanje subjekata privatnog sektora u to područje djelovanja, se od strane javnog sektora posmatra i kao rasterećenje sopstvenih obaveza, odnosno kao mogućnost da kapacitete usmjere na prioritetnija polja djelovanja.



Grafikon br. 33.: Djelatnost i radno angažovanje ispitanika koji smatraju da privatnom sektoru bezbjednosti treba omogućiti djelimično investiranje u zaštitu kritične infrastrukture

21. Da li postojeći subjekti privatnog sektora bezbjednosti u Crnoj Gori posjeduju kapacitete za zaštitu kritične infrastrukture?

Analiza dobijenih rezultata ukazuje na značajnu podijeljenost stavova ispitanika o kapacitetima privatnog sektora bezbjednosti u domenu zaštite kritične infrastrukture u Crnoj Gori. Najzastupljeniji, ali tek relativno većinski stav anketiranih (38%) je da postoje adekvatni kapaciteti privatnog sektora, dok još 19% ispitanika te kapacitete percipira kao djelimične. Negativno mišljenje o aktuelnim sposobnostima privatnog sektora bezbjednosti da adekvatno štiti kritičnu infrastrukturu ima 13% anketiranih, dok je ponovo visok postotak (30%) ispitanika koji o tom pitanju nisu mogli da daju svoju ocjenu.



Grafikon br. 34.: Da li postojeći subjekti privatnog sektora bezbjednosti u Crnoj Gori posjeduju kapacitete za zaštitu kritične infrastrukture

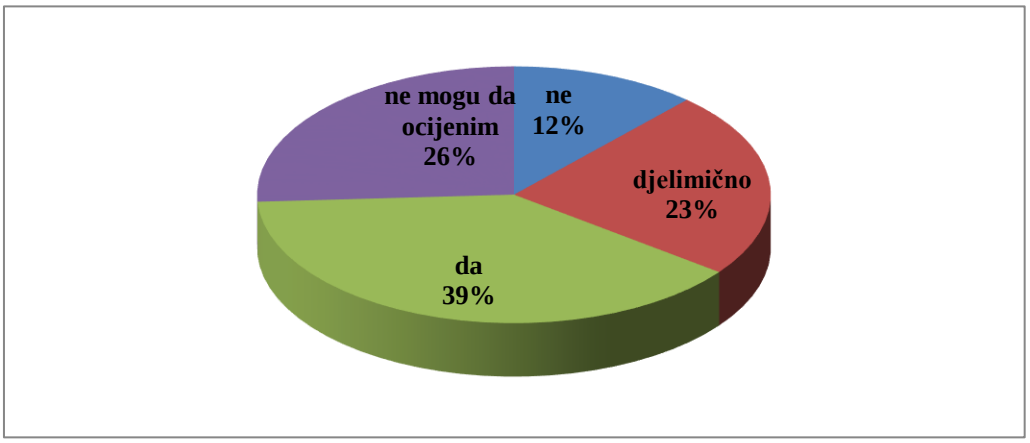
I u ovom slučaju kao i u prethodnim evidentno je da mlađi ispitanici u relativnoj većini smatraju da privatni sektor ima adekvatne kapacitete i da može da zadovolji potrebama tržišta pa tako i domenu zaštite kritične infrastrukture. S druge strane stariji ispitanici pokazuju određen stepen sumnjičavosti kada je u pitanju privatni sektor. Razlog navedenom treba tražiti u dugoj istoriji javnog sektora Crne Gore, za razliku od privatnog koji je tek u nastajanju. To je ujedno i veća obaveza privatnog sektora da kroz profesionalni i odgovoran rad stekne veće povjerenje i starijih generacija.

Polna zastupljenost je relativno ravnopravna. Kod školske spreme ispitanici visoke spreme smatraju da postoje djelimični kapaciteti, dok kod više i srednje ima značajan procenat neopredijeljenih.

22. Da li postojeći subjekti privatnog sektora bezbjednosti u Crnoj Gori posjeduju kapacitete za zaštitu vaše organizacije ?

S obzirom da se ovo pitanje po svojoj suštini nadovezalo na prethodno, bilo je realno očekivati i slične rezultate ankete. U tom smislu je relativna većina od 39% ispitanika zauzela stav da postojeći

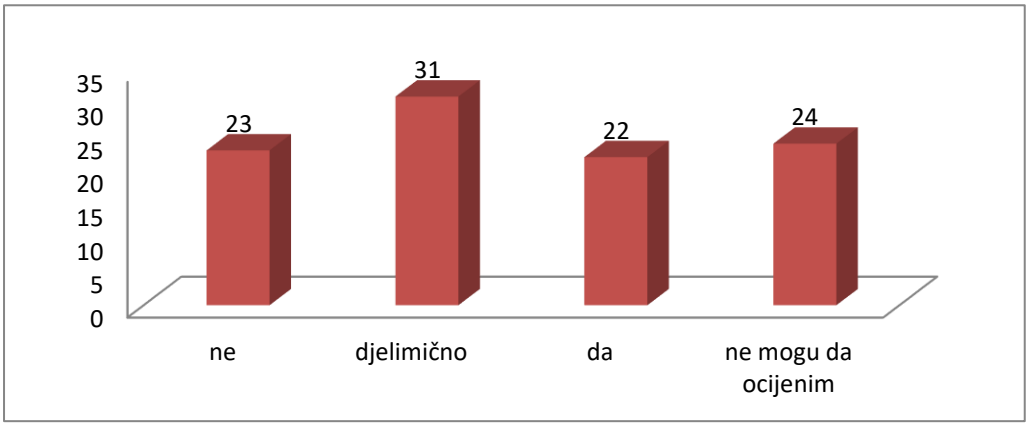
subjekti privatnog sektora bezbjednosti u Crnoj Gori posjeduju kapacitete za zaštitu organizacije u kojoj su zaposleni, uz još 23% anketiranih koji smatraju da su ti kapaciteti djelimični. Negativno mišljenje o aktuelnim kapacitetima privatnog sektora bezbjednosti je izrazilo 12% ispitanika, uz relativno visok procenat (26%) anketiranih koji o tom pitanju nisu imali stav.



Grafikon br. 35.: Da li postojeći subjekti privatnog sektora bezbjednosti u Crnoj Gori posjeduju kapacitete za zaštitu organizacije iz koje dolaze ispitanici ?

23. Da li je Zakon o zaštiti lica i imovine dovoljan normativni okvir za angažovanje privatnog sektora bezbjednosti u zaštiti kritične infrastrukture u Crnoj Gori?

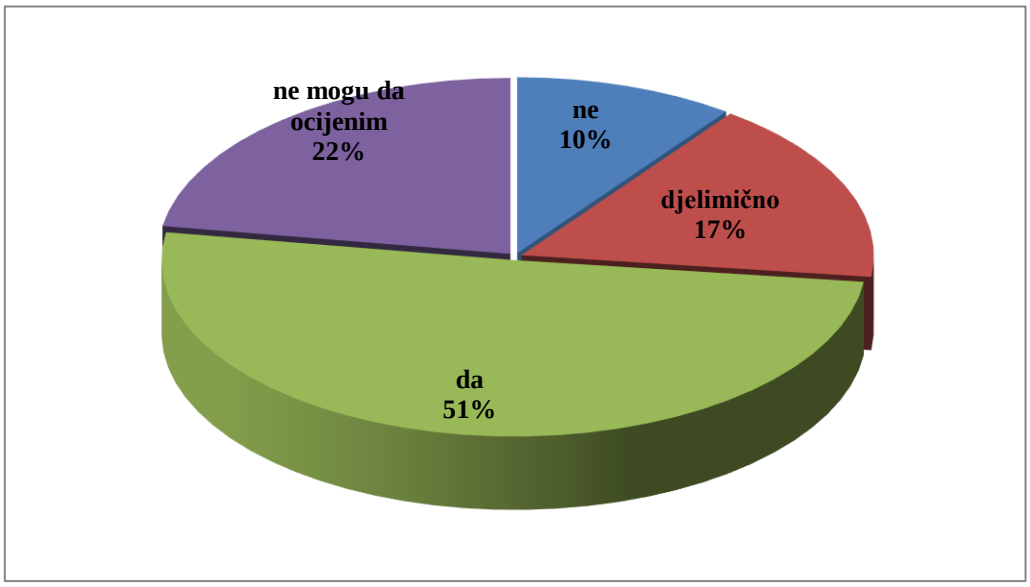
Analiza dobijenih rezultata ukazuje na značajnu podijeljenost stavova ispitanika u pogledu primenljivosti Zakona o zaštiti lica i imovine kao normativnog okvira za angažovanje privatnog sektora bezbjednosti u zaštiti kritične infrastrukture u Crnoj Gori. S jedne strane, 23% ispitanika smatra da predmetni zakon ne daje mogućnost angažovanja privatnog sektora u toj oblasti, dok suprotnu percepciju ima 22% anketiranih. Uz 24% ispitanika koji nijesu mogli da se izjasne o tom pitanju, relativno najveći postotak (31%) učesnika ankete je zauzeo stav da navedeni zakon samo djelimično može predstavljati osnov za angažovanje privatnog sektora u zaštiti kritične infrastrukture.



Grafikon br. 36.: Da li je Zakon o zaštiti lica i imovine dovoljan normativni okvir za angažovanje privatnog sekotora bezbjednosti u zaštiti kritične infrastrukture?

24. Da li privatni sektor bezbjednosti u Crnoj Gori doprinosi povećanju opšte bezbjednosti?

Odgovori na relativno opštije pitanje o doprinosu privatnog sektora povećanju opšte bezbjednosti u Crnoj Gori ukazuju na afirmativnu percepciju ispitanika, od kojih je 51% dalo pozitivan odgovor, uz još 17% anketiranih koji su se sa tim djelimično složili. Ulogu privatnog sektora bezbjednosti u ovom domenu je negativno percipiralo 10% anketiranih lica, dok 22% učesnika ankete nije moglo da ocijeni tu ulogu.



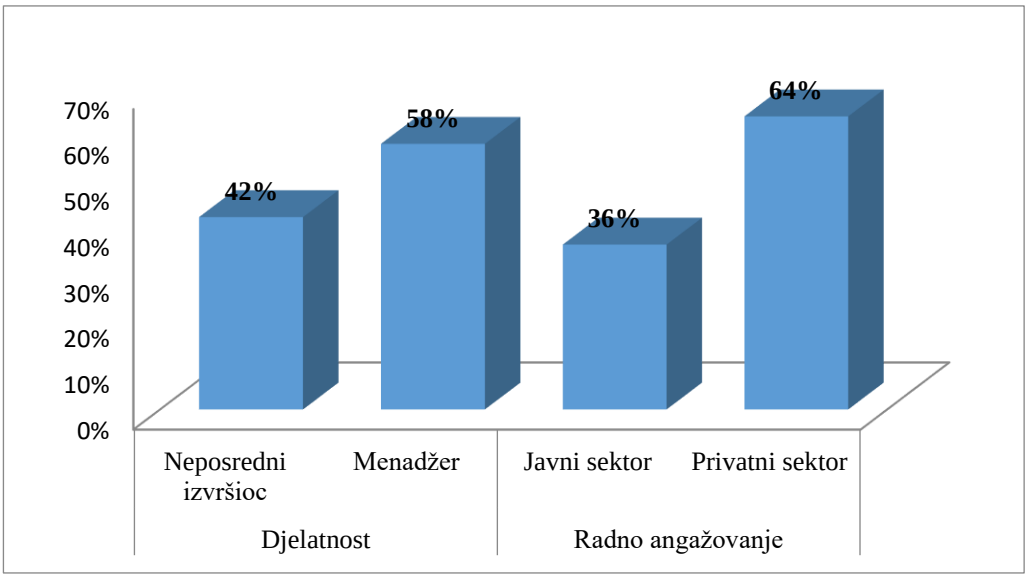
Grafikon br. 37.: Da li privatni sektor bezbjednosti doprinosi povećanju opšte bezbjednosti u Crnoj Gori

Posebnu pažnju zavređuje pitanje da li privatni sektor bezbjednosti u Crnoj Gori doprinosi povećanju opšte bezbjednosti, na koje je 51% ispitanika potvrdno odgovorilo. Takav odgovor se može smatrati veoma pozitivnim s obzirom da Crna Gora nema dugu tradiciju privatnog sektora bezbjednosti.

STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
45%	37%	18%	59%	41%	7%	9%	51%	33%

Tabela br.27.: Podaci o ispitanicima koji su potvrdno odgovorili da privatni sektor bezbjednosti doprinosi povećanju opšte bezbjednosti Crne Gore

Odgovor na predmetno pitanje ima posebnu važnost jer odražava opšti stav ispitanika prema privatnom bezbjednosnom sektoru. Analiza odgovora potvrđuje i prisutnost aktuelnog trenda većeg povjerenja i pozitivnije percepcije ispitanika prema privatnom sektoru bezbjednosti. To je posebno značajno jer je povjerenje osnova za stvaranje javno-privatnog partnerstva ne samo u zaštiti kritične infrastrukture već i šire. Na osnovu odgovora indirektno možemo zaključiti da građani Crne Gore imaju relativno pozitivna iskustva kada se radi o privatnom sektoru bezbjednosti. Kao i kod prethodnog pitanja u starosnoj strukturi onih koji su dali potvrdan odgovor dominiraju mlađi ispitanici kao i oni sa visokom školskom spremom.

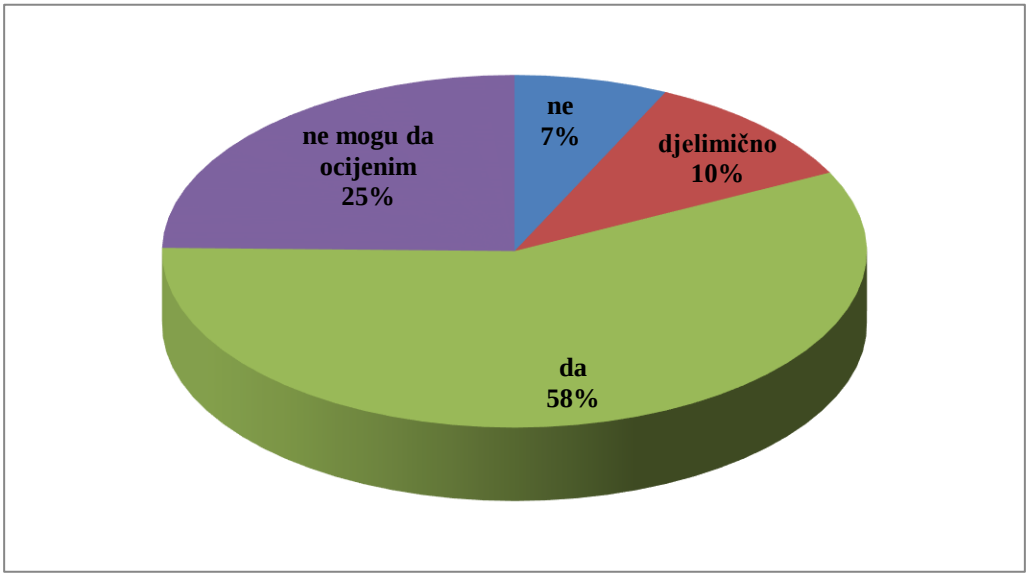


Grafikon br.38.: Podaci o ispitanicima koji su potvrdno odgovorili da privatni sektor bezbjednosti doprinosi povećanju opšte bezbjednosti Crne Gore

Ukoliko analiziramo djelatnost i radno angažovanje, možemo uočiti određene promjene u odnosu na prethodno pitanje. Naime, prisutan je povećani broj neposrednih izvršilaca koji smatraju da privatni sektor bezbjednosti pozitivno utiče na povećanje opšte bezbjednosti. Pored toga, evidentno je i povećanje učešća javnog sektora u potvrdnom odgovoru na navedeno pitanje. Rezultati ovog pitanja nesumnjivo ukazuju na ispravnost sadašnjeg pravca razvoja privatnog sektora u Crnoj Gori, koji u sve većoj mjeri stiče povjerenje građana svojim profesionalnim radom, što upućuje i na mogućnost uspješnog stvaranja predmetnog partnerstva u području bezbjednosti.

25. Da li bi angažovanjem privatnog sektora bezbjednosti bio povećan stepen zaštite kritične infrastrukture u Crnoj Gori ?

Analiza dobijenih rezultata ukazuje da značajna većina ispitanika (58%) ima pozitivnu percepciju uloge privatnog sektora bezbjednosti u zaštiti kritične infrastrukture u Crnoj Gori u smislu doprinosa povećanju stepena te zaštite. S druge strane, negativan stav o tome ima samo 7% anketiranih, uz standardno visok procenat ispitanika (25%) koji o tome nijesu u stanju da daju ocjenu.



Grafikon br. 39.: Da li bi angažovanjem privatnog sektora bezbjednosti bio povećan stepen zaštite kritične infrastrukture

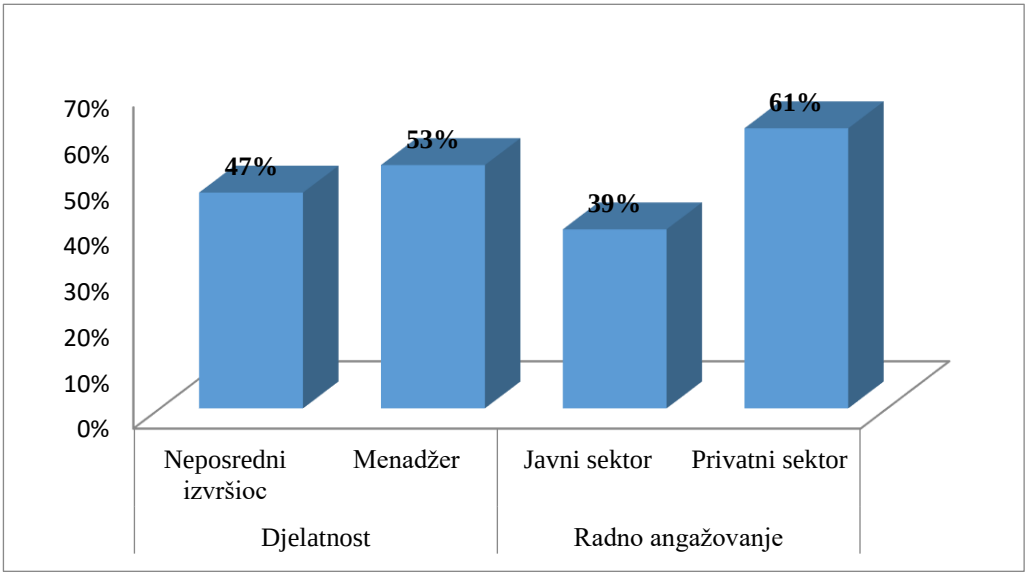
Za predmet ovog rada posebno je značajno pitanje da li bi angažovanje privatnog sektora bezbjednosti predstavljalo povećan stepen zaštite kritične infrastrukture. Na navedeno pitanje čak 58% ispitanika je potvrdno odgovorilo, što je u skladu sa trendovima u odgovorima na prethodna pitanja.

Kao i kod prethodnih pitanja, najveći broj ispitanika koji su se opredijelili za ovu opciju bio je starosti do 35 godina (43%), a znatno manje (18%) su zastupljena lica sa preko 45 godina života. S druge strane, polna struktura je bez bitnih promena u odnosu na prethodna pitanja. Kada se posmatra školska sprema, i u ovom slučaju je najveći broj ispitanika koji su dali potvrdan odgovor (50%) sa visokom stručnom spremom, dok je s druge strane najmanje učešće anketiranih lica sa višom (7%) i srednjom stručnom spremom (7%).

STAROSNA STRUKTURA			**POL**		**ŠKOLSKA SPREMA**			
do 35 godina	od 36 do 45 g.	preko 45g.	muški	ženski	srednja stručna sprema	viša stručna sprema	visoka stručna sprema	master i doktorat
43%	39%	18%	58%	42%	8%	7%	50%	34%

Tabela br. 28.: Podaci o ispitanicima koji su potvrdno odgovorili da bi angažovanje privatnog sektora bezbjednosti predstavljalo povećan stepen zaštite kritične infrastrukture

Kada se posmatra djelatnost i radno angažovanje ispitanika uočavamo donekle ujednačen odnos neposrednih izvršilaca i upravnih djelatnosti, dok je s druge strane dominiraju pripadnici privatnog sektora koji su se u najvećem broju (61%) složili sa stavom da angažovanje privatnog sektora doprinosi povećanom stepenu bezbjednosti i zaštite kritične infrastrukture.



Grafikon br.40.: Podaci o ispitanicima koji su potvrdno odgovorili da bi angažovanje privatnog sektora bezbjednosti predstavljalo povećan stepen zaštite kritične infrastrukture

Analizom odgovora na ostala pitanja koja su u direktnom odnosu sa predmetom istraživanja možemo doći do sličnih zaključaka koji ukazuju da privatni sektor bezbjednosti doprinosi povećanju opšte bezbjednosti, što ga ujedno preporučuje za ravnopravnog aktera javno-privatnog partnerstva u zaštiti kritične infrastrukture. Drugim riječima, ispitanici smatraju da privatni sektor ima dovoljne kapacitete i resurse i da može doprinijeti uspostavljanju adekvatnog načina zaštite kritične infrastrukture Crne Gore.

Pored navedenog, ovo istraživanje je pokazalo da u Crnoj Gori ne postoji izraziti polaritet između javnog i privatnog sektora, što umnogome olakšava uspostavljanje adekvatnog javno-privatnog partnerstva u području zaštite kritične infrastrukture. Uspostavljanju saradnje može doprinijeti i činjenica da i javni i privatni sektor imaju sličnu percepciju ključnih oblika ugrožavanja što pozitivno utiče na njihovo približavanje i mogućnosti uspostavljanja dugoročne saradnje. Međutim, za tako nešto je potrebna i jasna i potpuna zakonska regulativa koja bi predstavljala normativni osnov takvog partnerstva. U vezi sa tim, od ključnog značaja je zakon koji bi preciznije regulisao materiju javno-privatnog partnerstva i koji bi otvorio prostor za efikasniju zajedničku saradnju dva sektora u ovoj oblasti.

ŠESTI DIO

MODEL JAVNO-PRIVATNOG PARTNERSTVA U ZAŠTITI KRITIČNE INFRASTRUKTURE CRNE GORE

6.1. Bezbjednosni kontekst – pokazatelji stanja mira i sigurnosti na globalnom nivou i pozicija Crne Gore u odnosu na druge države

Global Peace Index (GPI)[512] mjeri stanje mira na globalnom nivou uz korišćenje 23 kvalitativna i kvantitativna pokazatelja iz relevantnih izvora, pri čemu pokriva 99,7% svjetske populacije. Rezultati za svaki pojedinačni indikator se kvantifikuju na skali od 1-5, pri čemu su kvalitativni indikatori grupisani u pet cjelina i kvantitativno se ocjenjuju od 1 do 5 (na treću decimalu). Global Peace Index mjeri nivo negativnog mira koji se definiše kao odsustvo nasilja ili straha od nasilja, što omogućava da se mir lakše posmatra. U kvantifikativnom izražavanju globalnog mira primjenjuju se ukupno 23 indikatora koji su podijeljeni u tri domena. Prvi od njih su aktuelni unutrašnji i međunarodni sukobi, koji se prate u cilju istraživanja u kojoj su mjeri države uključene u unutrašnje i međunarodne sukobe, kao i utvrđivanja njihove uloge i trajanja umiješanosti u sukobe. Posebno se analiziraju broj i trajanje unutrašnjih sukoba, broj smrtnih slučajeva kao posledica spoljnog i unutrašnjeg oružanog sukoba, učestalost miješanja i trajanje umiješanosti države u spoljne sukobe, te intenzitet unutrašnjeg sukoba i odnosi sa susjednim državama.

Rang	Država	Unutrašnji i međunarodni konflikti
1.	Bocvana	**1,000**
2.	Čile	**1,000**
3.	Mauricijus	**1,000**
29.	Albanija	**1,225**
56.	**Crna Gora**	**1,426**
84.	Srbija	**1,604**
88.	Sjeverna Makedonija	**1,628**
112.	Bosna i Hercegovina	**1,876**
160.	Jemen	**3,670**
161.	Avganistan	**3,674**
162.	**Sirija**	**3,828**

Tabela br. 29: Domen unutrašnjih i međunarodnih konflikata za pojedine države u svijetu

Unutrašnji i međunarodni konflikti bili su jedini indikatori koji su se na globalnom nivou pogoršali u sadašnjem periodu, uprkos pozitivnih pokazatelja kao što su smanjenje intenziteta sukoba

[512] U ovom delu rad korišćeni su podaci Global Peace Index, The Institute for Economics & Peace, 2019, dostupno na: http://visionofhumanity.org/app/uploads/2019/06/GPI-2019-web003.pdf

i poraz Islamske države (ISIL). Do navedenog pogoršanja je došlo zbog uključenja pojedinih država u manje sukobe širom svijeta. Sve u svemu, mir se 2018. godine poboljšao u 86, a pogoršao u 76 analiziranih država.

Uopšteno posmatrano, globalni mir se pogoršao u okviru dva od tri domena tokom poslednje decenije. Broj aktuelnih sukoba se povećao za 6%, dok je indikator bezbjednosti pogoršan za 3%. Terorizam i unutrašnji sukobi su indikatori koji su najviše doprinijeli globalnom pogoršanju mira tokom decenije. U istom periodu, 100 zemalja je doživjelo povećanu terorističku aktivnost, sa samo 38 slučajeva poboljšanja, dok se ukupan broj sukoba povećao nekoliko puta u periodu od 2006. do 2016. godine.

Istraživanja pokazuju različite rezultate u području međunarodnih odnosa na evropskom prostoru tokom 2018. godine. U pogledu odnosa sa susjednim zemljama i širih integracija, prisutni su neujednačeni trendovi. Na primjer, Sjeverna Makedonija je započela proces ubrzanog priključivanja NATO-u, dok Velika Britanija nastoji da sprovede svoj plan za izlazak iz Evropske unije. U istom periodu, kod 19 evropskih zemalja došlo je do pogoršanja rezultata u pogledu broja, trajanja i uloge u spoljnim sukobima, pri čemu je Turska zabilježila i porast broja smrtnih slučajeva koji su posledica ovih sukoba. Suprotno tome, Rumunija, Njemačka i Velika Britanija registrovale su pad broja smrtnih slučajeva od spoljnih sukoba.

Drugi domen mjerenja stanja mira procjenjuje nivo harmonije ili neslaganja u državi. Na tom planu 10 indikatora u širokom zahvatu procjenjuje ono što bi se moglo opisati kao društvena sigurnost i bezbjednost. Ocjenjuje se da niska stopa kriminala, minimalna teroristička aktivnost i zanemarljiva prisutnost nasilnih demonstracija, harmonični odnosi sa susjednim državama, stabilna politička scena i mali dio stanovništva koji je interno raseljen ili se nalazi u izbjeglištvu, predstavljaju doprinos miru. Konkretnije, u ovom domenu se posebno procjenjuju uticaj terorizma, nivo percepcije kriminala u društvu, politička (ne)stabilnost, broj ubistava, nivo nasilnog kriminala, vjerovatnoća nasilnih demonstracija, broj lica koja izdržavaju zatvorske kazne, broj službenika unutrašnje bezbjednosti i policije. U cilju objektivnog vrednovanja i realnih poređenja među državama pojedini parametri (npr. broj ubistava i slično) se brojčano izražavaju u odnosu na 100.000 ljudi.

Rang	Država	Društvena sigurnost i bezbjednost
1.	Island	1,131
2.	Singapur	1,233
3.	Norveška	1,243
43.	Srbija	2,086
62.	Severna Makedonija	2,332
68.	Albanija	2,392
71.	Bosna i Hercegovina	2,420
97.	**Crna Gora**	2,574
160.	Centralna Afrička Republika	4,061
161.	Južni Sudan	4,090
162.	Avganistan	4,198

Tabela br. 30: Domen društvene sigurnosti i bezbjednosti pojedinih država

U toku 2018. godine poboljšana je većina aspekata iz domena sigurnosti i zaštite, što se posebno odnosi na politički terorizam i uticaj terorizma uopšte. Većina država u Evropi, osim Turske, registruje nizak nivo političkog terora, koji uključuje politička hapšenja, nestanke i mučenja. Rezultati po ovom pokazatelju su pogoršani u samo četiri zemlje, dok su u devet država poboljšani.

Raseljavanje stanovništva u Evropi takođe je opalo u analiziranom periodu. Najuočljivije poboljšanje se tiče učešća izbjeglica i interno raseljenih lica prema broju stanovništva na Kipru, jer je taj procenat smanjen sa 23% na 18%. U toku 2018. godine opao je i procenat raseljenih Turaka, iako je Turska i dalje glavna zemlja primalac azilanata, posebno sa Bliskog Istoka i Severne Afrike. Srbija je u tom domenu takođe zabilježila pad, iako tačne brojke variraju u zavisnosti od izvora podataka.

Tokom 2018. godine su 92 države poboljšale svoje rezultate u odnosu na terorizam, nastavljajući petogodišnji trend koji je započeo nakon dostizanja negativnog vrhunca 2014. Godine. Međutim, prosječna globalna ocjena terorizma je zapravo pogoršana, zbog velikog porasta uticaja terorizma u pojedinim državama.

Rang	Država	Militarizacija
1.	Island	1,032
2.	Mađarska	1,151
3.	Slovenija	1, 179
20.	Bosna i Hercegovina	1,499
27.	**Crna Gora**	1,547
46.	Srbija	1,630
50.	Albanija	1,656
61	Severna Makedonija	1,707
160.	SAD	3,073
161.	Rusija	3,252
162.	Izrael	3,880

Tabele br. 31: Domen militarizacije za pojedine države u svijetu

Poseban domen je militarizacija, koja odražava vezu između nivoa vojne izgradnje jedne države i pristupa oružju i nivo mira, kako u zemlji, tako i u okruženju. Ovaj domen sadrži sedam indikatora kao što su podaci o vojnim troškovima (u procentu BDP-a), broj pripadnika oružanih snaga, finansijski doprinosi mirovnim misijama UN-a, uvoz i izvoz naoružanja, kapaciteti nuklearnog i teškog naoružanja, dostupnost malokalibarskog i lakog naoružanja.

Najizraženije poboljšanje u 2018. godini zabilježeno je u domenu militarizacije, što znači da je nastavljen dugoročni trend pada militarizacije. To je izraženo smanjenjem procenta vojnih izdataka u procentu BDP-a, kao i veličine oružanih snaga u državama širom svijeta. Međutim, navedena poboljšanja umanjena su pogoršanjem percepcije kriminala. Kod najvećeg broja država koje su imale

pogoršanje po bilo kom pokazatelju, negativni trendovi su bili vezani za indikatore nuklearnog i teškog naoružanja, što je registrovano u 76 država. Inače, najveće prosječno pogoršanje dogodilo se na pokazatelju borbe protiv spoljašnjih sukoba, iza koga slijede pogoršana percepcija kriminaliteta i unutrašnji sukobi. Međutim, iako se broj država koje imaju problema sa unutrašnjim sukobima ukupno povećao, broj smrtnih slučajeva je smanjen, prvenstveno zbog nižeg intenziteta sukoba u Siriji, Ukrajini i Nigeriji.

Rang	Država	Ekonomska cijena nasilja (%BDP)
1.	Sirija	28, 942.8 (67%)
2.	Avganistan	32,815.3 (47%)
3.	Centralna Afrička Republika	1,408.9 (42%)
46.	Bosna i Hercegovina	4,010.0 (9%)
53.	**Crna Gora**	973.8 (8%)
59.	Srbija	8,156.3 (8%)
68.	Severna Makedonija	2,180.7 (7%)
94.	Albanija	2,100.9 (6%)
160.	Indonezija	74, 591.6 (2%)
161.	Ekvatorijalna Gvineja	700.2 (2%)
162.	Malavi	503.0 (2%)

Tabela br. 32: Domen ekonomske cijene nasilja za pojedine države

U 2018. godini se na globalnom nivou domen ekonomskog uticaja nasilja prvi put poboljšao od 2012. godine (smanjenje za 3,3% ili 475 milijardi američkih dolara), što se pozitivno odrazilo na ukupno stanje svjetskog mira. Navedeno smanjenje je prije svega posledica pada troškova povezanih sa oružanim sukobima, do čega je došlo zbog nižih nivoa oružanih sukoba u Siriji, Kolumbiji i Ukrajini. To je takođe rezultiralo i pozitivnim učinkom na pokazatelje vezane za izbjeglice, interno raseljena lica i terorizam, što je izraženo kroz smanjenje troškova za iste. Zemlje zahvaćene sukobima - Sirija, Avganistan, Irak, Centralnoafrička Republika, Somalija i Kolumbija – imale su veće troškove i ukupne negativne posljedice zbog smrtnih slučajeva i povreda uzrokovanih sukobima i terorizmom, povećanja broja izbjeglica i interno raseljenih lica i gubitaka BDP-a kao rezultata sukoba. Izdaci za unutrašnju bezbjednost bili su u 2018. godini druga najveća komponenta, koja je činila 32% globalnog ekonomskog uticaja nasilja, odnosno 4,5 milijardi USD. Ipak, taj pokazatelj na globalnom nivou bilježi smanjenje za jedan procenat u odnosu na prethodnu godinu. Pod troškovima za unutrašnju bezbjednost se ovdje podrazumijevaju sredstva koja se izdvajaju za policijske i pravosudne sisteme, kao i troškovi povezani sa zatvorskim kaznama.

Posmatrajući navedene podatke, možemo zaključiti da je Evropa i dalje relativno najmirniji i najstabilniji region u svijetu, pri čemu pokazatelji za 2018. godinu pokazuju i neznatno poboljšanje stanja mira nakon nekoliko godina negativnijih trendova. U istom periodu, poboljšanja su zabilježile 22 od 36 evropskih zemalja. Poboljšanja se odnose na indikatore političkog terora, uticaja terorizma,

izbjeglica i interno raseljenih lica i na pokazatelje stope ubistava. Međutim, i pored ovih poboljšanja, šire političko okruženje u Evropi ostaje neizvjesno, a rastući nacionalizam i međunarodni terorizam ostaju značajne prijetnje miru.

Generalno uzev, u 2018. godini se Globalni indeks mira poboljšao u 86 država, dok se u 76 zemalja pogoršalo, pri čemu se globalni prosječni GPI rezultat poboljšao za 0,09%. To je ujedno i najveće poboljšanje indeksa zabilježeno od 2013. godine. Najveće poboljšanje zabilježeno je za oblast Militarizacija, gdje je taj trend prisutan u 98 zemalja. Ipak, Evropa je bila jedina od četiri regije u razvoju koje se nijesu poboljšale u svim domenima GPI-a. Naime, napredak u Evropi je zabilježen u domenima sigurnosti i smanjenja militarizacije, ali je negativni trend registrovan kod tekućih sukoba.

Crna Gora je po većini indikatora vezanih za Globalni indeks mira relativno visoko rangirana, sa izuzetkom domena društvene sigurnosti i bezbjednosti pojedinih zemalja, gdje je u 2018. godini zauzela 97. mjesto od 162 analizirane države.

6.2. Sajber bezbjednost Crne Gore-kvantitativni pristup

U cilju potpunijeg prikaza aktuelnog stanja sajber bezbjednosti Crne Gore i njenog poređenja sa drugim državama iskoristićemo jednu od dostupnih baza podataka koje izrađuju različite međunarodne i nacionalne organizacije. Treba napomenuti da jedan broj pomenutih baza podataka sadrži samo završne rezultate, što znači da nema mogućnosti uvida u primijenjenu metodologiju ocjenjivanja. To je ujedno i razlog i opredjeljenje za korišćenje National Cyber Security Index[513] u radu.

Nacionalni indeks sajber-bezbjednosti (NCSI) je globalni indeks, koji mjeri spremnost država da spriječe sajber prijetnje i da upravljaju sajber incidentima. NCSI ujedno predstavlja i bazu podataka koja je javno dostupna i koja je kao takva sredstvo za izgradnju kapaciteta u području nacionalne kibernetičke bezbjednosti. Predmetni indeks je razvijen u pet faza:

- identifikacija osnovnih sajber prijetnji na nacionalnom nivou,
- identifikacija sajber sigurnosti na nacionalnom nivou (mjere i kapaciteti),
- izbor važnih i mjerljivih aspekata,
- razvoj pokazatelja sajber sigurnosti i
- grupisanje indikatora sajber bezbjednosti.

Posebna karakteristika Nacionalnog indeksa sajber-bezbjednosti jeste fokusiranost na mjerljive aspekte sajber bezbjednosti koju sprovode nadležni državni organi, i to:

- važeći zakonski okvir (zakonski akti, podzakonski propisi, službeni nalozi i slično)
- uspostavljene jedinice (postojeća organizaciona struktura, odjeljenja, grupe i slično)
- formati saradnje (savjet, odbor, oficijelna radna grupa i slično) i
- ishodi/proizvodi (politike, vježbe, edukacija, upotreba tehnologija, veb stranice, programi i slično).

[513] U ovom dijelu rada korišćeni su podaci *National Cyber Security Index*, Ministry of Foreign Afairs within Estonian Development Cooperation, 2018, dostupno na: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

U cilju objektivnog ocjenjivanja sajber sposobnosti država korišćeni su javno dostupni podaci sadržani u pravnim aktima i službenim dokumentima, kao i zvanične veb stranice. Nacionalni indeks sajber-bezbjednosti ima tri kategorije, 12 svojstva (sposobnosti) i 46 indikatora. Svaki indikator ima vrijednost, koja pokazuje relativnu važnost indikatora u indeksu. Vrijednosti daju ekspertske grupe prema definisanim kriterijumima (1 bod-pravni akt koji reguliše određenu oblast; 2-3 boda - jedinica koja ima posebnu odgovornost za sajber bezbjednost; 2 boda-oblik uspostavljene službene saradnje i 1-3 boda proizvod sajber bezbjednosti države kao što su dokumenta, vježbe, upotreba tehnologija i slično).

Ocjena iz Indeksa ukazuje na procenat koji je država dobila od maksimalne vrijednosti pokazatelja, pri čemu je maksimalni rezultat indeksa uvijek 100 (100%). Pored Indeksa sajber-bezbjednosti utvrđuje se i nivo digitalnog razvoja (DDL), koji se izračunava prema indeksu razvoja informaciono-komunikacionih tehnologija i indeksu mrežne spremnosti (NRI). Nivo digitalnog razvoja je prosječni procenat koji je država dobila od maksimalne vrijednosti oba indeksa. Kada je riječ o razlici, ista prikazuje odnos između nacionalnog indeksa sajber-bezbjednosti i nivoa digitalnog razvoja. Pozitivan rezultat pokazuje da je razvoj kibernetičke sigurnosti zemlje u skladu ili ispred njenog digitalnog razvoja. Negativni rezultat pokazuje da je digitalno društvo u zemlji naprednije od nacionalnog područja sajber bezbjednosti.

Rang	Država	NCSI	Nivo digitalnog razvoja	Razlika
1.	Francuska	83,12	79,06	4,06
2.	Njemačka	83,12	81,95	1,17
3.	Estonija	81,12	79,27	2,55
16.	Srbija	66,23	61,62	4,61
29.	Hrvatska	57,14	66,91	-9,77
46.	Slovenija	44,16	70,47	-26,31
47.	Albanija	42,86	53,56	-10,70
60.	**Crna Gora**	33,77	62,91	-29.14
99.	Madagaskar	2,60	26,97	-24,37
100.	Karibati	1, 30	21, 70	-20,40

Tabela br. 33: Sajber bezbjednost Crne Gore i pojedinih država

Prema bazi podataka National Cyber Security Index za 2018. godinu, Crna Gora se nalazi na šezdesetom mjestu od sto analiziranih država svijeta. Najveći indeks sajber bezbjednosti imaju Francuska, Njemačka i Estonija. Od država regiona najbolje je rangirana Srbija, a nakon toga Hrvatska. Za Crnu Goru je posebno karakteristično da je razlika ocijenjena negativno, što ukazuje da je digitalno društvo Crne Gore znatno naprednije od nacionalnog područja sajber bezbjednosti.

Drugim riječima, za unapređenje sajber bezbjednosti potrebna je bolja reakcija države od njenog aktuelnog djelovanja. Ipak, značajno je da je nivo digitalnog razvoja znatno bolji u odnosu na pojedine države u regionu, što znači da Crna Gora u ovom domenu ne zaostaje kao što je to slučaj u segmentu kojim je određen indeks nacionalne sajber bezbjednosti. U vezi sa tim, značajno je osvrnuti se na definisane elemente predmetnog Indeksa, jer se može uočiti zajednički element koji se odnosi i na nivo digitalnog razvoja. Naime, evidentno je da je potrebno unaprijediti važeće zakonske propise, kao i postojeće organizacione strukture u cilju adekvatnog odgovora na prijetnje u sajber prostoru. Pri tome ne treba zaboraviti ni dalji razvoj politike sajber bezbjednosti, kao i vježbe i edukaciju subjekata javnog i privatnog sektora u zaštiti informacione infrastrukture. Međutim, treba napomenuti da digitalni razvoj podrazumijeva kontinuirani proces i da ujedno predstavlja presudni faktor održivosti i u budućem periodu, što upućuje na potrebu stalnog razmatranja tog pitanja i iz ugla bezbjednosti i zahtijeva stalnu uključenost državnih organa u iznalaženju optimalnog modela.

DRŽAVA (RANG)	**Razvoj politike sajber bezbjednosti**	**Analize i informacije sajber prijetnji**	**Obrazovanje i profesionalni razvoj**	**Doprinos globalnoj sajber bezbjednosti**	**Zaštita digitalnih usluga**	**Zaštita osnovnih usluga**	**E-identifikacija i povjerenje u usluge**	**Zaštita ličnih podataka**	**Odgovor na sajber incidente 24/7**	**Upravljanje sajber krizama**	**Borba protiv sajber kriminala**	**Vojne sajber operacije**
Srbija (16)	6%	0%	4%	3%	0%	00%	00%	00%	7%	0%	00%	**3%**
Hrvatska (29)	1%	0%	6%	3%	0%	%	9%	00%	0%	0%	00%	**0%**
Slovenija (46)	4%	0%	3%	3%	%	7%	9%	00%	3%	0%	7%	**7%**
Albanija (47)	7%	0%	1%	7%	%	3%	9%	00%	7%	0%	7%	**7%**
Crna Gora (60)	**7%**	**%**	**2%**	**0%**	**0%**	**%**	**2%**	**100%**	**0%**	**0%**	**7%**	**%**

Tabela br. 34: Nacionalni indeks sajber bezbjednosti pojedinih država

Upoređujući nacionalni indeks sajber bezbjednosti prema navedenim elementima uočavaju se tri parametra prema kojima je Crna Gora najslabije ocijenjena i zbog kojih zaostaje u odnosu na države u okruženju.

Prvi parametar je nedostatak potpunijih analiza i informacija o sajber prijetnjama, što je od posebnog značaja za razmjenu podataka i definisanje procjene prijetnji u sajber prostoru. Neophodno je i postojanje centralnog državnog organa (jedinice) koja bi bila specijalizovana za analizu stanja strateške sajber bezbjednosti na nacionalnom nivou. Pored toga, nužno je i da javni dio nacionalne analize sajber prijetnji bude objavljivan najmanje jednom godišnje, uz dostupnost najmanje jednog veb sajta za bezbjednost i za profesionalce u sajber području. Drugi parametar je nedostatak zaštite osnovnih usluga koje se ostvaruju u sajber prostoru. Naime, operatori osnovnih usluga moraju redovno (najmanje jednom u tri godine) da pružaju dokaze o efikasnoj primjeni politika za sajber bezbjednost (npr. rezultat revizije, dokumentacija, poseban izveštaj). Treći parametar je nedostatak posebne organizacione cjeline u okviru oružanih snaga Crne Gore za planiranje i sprovođenje sajber operacija. Prema ostalim parametrima Crne Gora ne zaostaje za navedenim državama. Riječ je, između ostalog, o zaštiti ličnih podataka i borbi protiv sajber kriminala, pri čemu je posebno vrednovan doprinos Crne Gore globalnoj sajber bezbjednosti i slično.

6.3. Javno-privatno partnerstvo u zaštiti kritične infrastrukture Crne Gore

Kao samostalna država, Crna Gora se opredijelila za proces pristupanja evroatlanskim integracijama i dostizanja punopravnog članstva u EU i NATO. U vezi sa tim, Crna Gora je potpisala Sporazum o stabilizaciji i pridruživanju sa EU u oktobru 2007. godine, kao i bilateralni sporazum sa Svetskom trgovinskom organizacijom (STO) u aprilu 2008. godine. Na samitu NATO u Bukureštu u aprilu iste godine, Crna Gora je pozvana da se pridruži intenzivnom političkom dijalogu sa tom organizacijom. Ministri spoljnih poslova NATO-a su pozvali Crnu Goru da učestvuje u Akcionom planu za članstvo u Alijansi (MAP) 4. decembra 2009. godine. Evropska komisija je 9. novembra 2010. godine preporučila status kandidata Crnoj Gori, pod uslovom da pregovori o pristupanju započnu nakon završetka sedam „ključnih prioriteta“. Ovu odluku je ratifikovalo Evropsko vijeće i EU je odobrila status kandidata 17. decembra 2010. godine[514].

Za dalje integracije Crne Gore u evroatlantske tokove značajan datum je 5. jun 2017. godine, kada je ratifikovan Vašingtonski ugovor, čime je Crna Gora postala 29-ta članica NATO-a. Na taj način je Crna Gora zaokružila višegodišnji proces reformi i ispunila jedan od najvažnijih spoljnopolitičkih ciljeva zemlje[515].

Uzimajući u obzir uspješne rezultate javno-privatnih partnerskih projekata u državama članicama EU, kao i nedostatak budžetskih sredstava za razvoj infrastrukture, Vlada Crne Gore je odlučila da intenzivnije koristi predmetni model kroz proces privatizacije. U obrazloženju pomenute odluke crnogorske vlade je istaknuto da kada postoje oblasti (resursi) u kojima država ne djeluje dovoljno efikasno i pri čemu se za revitalizaciju određenog sektora ne izdvajaju značajnija budžetska

[514] Keković Zoran, Kentera Savo: Montenegrin Police: Current Profile and Future Trends, in: Meško G. et al. (eds.): *Handbook on Policing in Central and Eastern Europe*, Springer, New York, 2013, pp. 169-170

[515] *Komunikaciona strategija – CrnaGora članica NATO-aza period do 2020. godine*, Vlada Crne Gore, Podgorica, 2018, str. 3

sredstva, pogodnije je „delegirati“ određeno područje (resurs) kompanijama koje su spremne da ulože neophodna finansijska sredstva za ostvarivanje određenog cilja. S druge strane, zakonske odredbe štite nacionalne interese i sprečavaju trajno dodjeljivanje takvih resursa i infrastrukture privatnim kompanijama. U praksi je u poslednjih nekoliko godina evidentan rast broja zaključenih ugovora javno-privatnog partnerstva. Nesumnjivo je da ovakva saradnja donosi višestruku dobit za obije strane. Država dugoročno zadržava infrastrukturu, dok privatna kompanija prima materijalnu naknadu kroz korišćenje resursa. Međutim, postoje određeni rizici koji se mogu ogledati kroz potencijalno nisku profitnu stopu od povjerenih resursa za privatnu kompaniju, ili značajne gubitke za državu, ako kompanija dobije one segmente infrastrukture koji imaju monopolski položaj.[516]

U Crnoj Gori postoje brojni zainteresovani akteri koji sa svojim kapacitetima mogu imati značajnu ulogu u pružanju sveobuhvatnih i strukturalnih odgovora na aktuelne bezbjednosne prijetnje. Naime, ekonomski razlozi i dinamika društvenih promjena uzrokovali su i smanjenje državnog monopola u oblasti bezbjednosti. Iako je industrija privatne bezbjednosti u Crnoj Gori počela da funkcioniše 1992. godine, što je relativno rano u poređenju sa državama u okruženju, potpuni razvoj tog sektora započet je krajem devedesetih godina[517]. U nizu izveštaja i drugih dokumenata EU postoje preporuke da se: uspostavi jasniji odnos između privatnih kompanija za obezbjeđenje i policije, osigura veća transparentnost u regulaciji privatnog sektora bezbjednosti, sprovedu rigorozni programi obuke, prvenstveno vezane za primjenu sile, i druga pitanja iz te oblasti[518].

6.3.1. Normativni okvir

Spoljnopolitičko opredjeljenje Crne Gore za članstvo u EU, između ostalog, zahtijeva i usklađivanje nacionalnog zakonodavstva sa evropskim pravnim tekovinama u procesu priključenja. To je ujedno i jedan od razloga aktuelnih ažuriranja, izmjena i dopuna brojnih zakonskih akata. Iz prethodnih djelova rada nesumnjivo se može uočiti složenost koncepta javno-privatnog partnerstva i neophodnost proučavanja različitih zakonskih odredbi koje regulišu predmetnu oblast. Uzimajući u obzir navedeno, u narednom dijelu disertacije biće dat osvrt na najvažnije akte iz domena nacionalne legislative u cilju njene dogradnje i potrebnih izmjena kako bi se obezbijedio adekvatan normativni okvir javno-privatnog partnerstva u zaštiti kritične infrastrukture Crne Gore. S obzirom na činjenicu da je proces izgradnje zakonodavstva složen i da podrazumijeva angažovanje stručnjaka različitog profila, ukazaćemo samo na najvažnija aktuelna zakonska rešenja.

[516] *Public-private partnerships in Montenegro*, Institute Alternative,2010, dostupno na: http://www.institut-alternativa.org/wp-content/uploads/2009/05/jpp-eng.pdf

[517] Keković Zoran, Kentera Savo: Montenegrin Police: Current Profile and Future Trends, in: Meško G. et al. (eds.): *Handbook on Policing in Central and Eastern Europe*, Springer, New York, 2013, pp. 182-183

[518] South Eastern Europe Clearinghouse for the Control of SmallArms and Light Weapons. SALW and privatesecurity companies in South Eastern Europe: A cause oreffect of insecurity? 2005 dostupno na:http://www.seesac.org/uploads/studyrep/SALW_i_firme_za_privatno_obezbedjenje_u_jugoistocnoj_Evropi.pdf

6.3.2. Strategija nacionalne bezbjednosti Crne Gore

U cilju potpunije analize normativnog okvira javno-privatnog partnerstva u Crnoj Gori neophodno je sagledati širi kontekst s obzirom na složenost predmeta istraživanja. Analizu normativnog okvira započinjemo odredbama strategije nacionalne bezbjednosti, zbog činjenice da su najvažnija strateška opredeljenja u domenu bezbjednosti iskazana kroz Strategiju nacionalne bezbjednosti Crne Gore. Pored toga, Strategijom se utvrđuju i mehanizmi zaštite nacionalnih interesa, a sama Strategija predstavlja osnov za ostala strategijska dokumenta i planove u oblasti bezbjednosti. Uopšteno posmatrano, Strategija nacionalne bezbjednosti je koncipirana prema savremenim shvatanjima nacionalne bezbjednosti. Posebno je značajna činjenica da dokument strategije započinje nacionalnim interesima i ciljevima kao osnovama za uspostavljanje strateškog pristupa u oblasti nacionalne bezbjednosti.

Kada se analiziraju strategijski interesi Crne Gore, posebno su značajne odredbe koje se odnose na „zaštitu prirodnih i svih drugih resursa i potencijala Crne Gore". Iako je navedena odredba po svom obimu i sadržaju dosta široka, tako da može da obuhvati i kritičnu infrastrukturu, posmatranu kao skup nacionalnih resursa koji su od značaja ne samo za funkcionisanje države i društva, već ujedno predstavljaju i nacionalne resurse. Kao važan nacionalni interes, Strategija prepoznaje zaštitu kritične infrastrukture prvenstveno iz ugla „podsticanja saradnje državnih institucija, civilnog i privatnog sektora, u cilju jačanja civilne spremnosti za odgovore na bezbjednosne izazove, rizike i prijetnje". Na taj način, strategija u cilju jačanja kapaciteta u zaštiti kritične infrastrukture u prvi plan stavlja partnerstvo različitih struktura. Pored navedenog, Strategija nacionalne bezbjednosti poseban akcenat stavlja i na zaštitu informacione infrastrukture države i sistema bezbjednosti[519].

U okviru posebne cjeline koja se bavi bezbjednosnim izazovima, rizicima i prijetnjama, Strategija jasno naglašava, između ostalog, ugrožavanje energetske bezbjednosti, kao i činjenicu da je za funkcionisanje države i društva od posebnog značaja pružanje ključnih usluga koje direktno zavise od funkcionisanja kritične infrastrukture. Pored navedenog, Strategija nacionalne bezbjednosti ukazuje i na značaj pojedinih industrijskih sistema, naročito ako se isti zloupotrijebe, kao i na informaciono-komunikacionu infrastrukturu i njenu povezanost i izvan granica države[520]. Nesumnjivo je da Strategija punu pažnju posvećuje kritičnoj infrastrukturi kao nacionalnom interesu Crne Gore.

Strategija nacionalne bezbjednosti ima indirektan pristup problematici javno-privatnog partnerstva. To se manifestuje u djelovima teksta koji se odnose na jedinstvo akcije u odgovoru na savremene izazove, rizike i prijetnje, što između ostalog podrazumijeva saradnju državnih i civilnih organa, institucija i organizacija. Pored navedenog, Strategija definiše i koncept civilne spremnosti koja treba da omogući saradnju državnih institucija i privatnog sektora s obzirom da savremeni bezbjednosni izazovi zahtijevaju odgovor cjelokupnog društva[521].

U posebnoj cjelini Strategije koja se odnosi na sistem nacionalne bezbjednosti u okviru posebnih elemenata sistema, između ostalog su svrstane i agencije za privatno obezbjeđenje i

[519]Strategija nacionalne bezbjednosti Crne Gore, „*Službeni list Crne Gore"*, br. 085/18, str. 2
[520]Ibid, str. 5
[521] Ibid, str. 6

zaštitarske službe[522]. To je ujedno i uobičajen način na koji se u Strategiji privatni sektor bezbjednosti najčešće navodi kao element strukture nacionalne bezbjednosti.

Iz svega navedenog može se zaključiti da po pitanju javno-privatnog partnerstva u zaštiti kritične infrastrukture, Strategija nacionalne bezbjednosti Crne Gore pruža solidnu osnovu za primjenu navedenog koncepta. Iako ne sadrži eksplicitne odredbe kojima bi se nedvosmisleno apostrofirao predmetni koncept, Strategija otvara mogućnost da se kroz zakone ili strategije niže opštosti, implementira predmetno partnerstvo. U okolnostima budućih izmjena ili ažuriranja predmetne strategije, na planu jasnijih određenja postoji mogućnost da se posebno naglasi značaj koordinisanog zajedničkog nastupa javnog i privatnog sektora bezbjednosti u zaštiti kritične infrastrukture. Ovakva rešenja se inače mogu naći u strategijama bezbjednosti mnogih država[523].

6.3.3. Zakon o zaštiti lica i imovine

Zakon o zaštiti lica i imovine je ključan u implementaciji koncepta javno-privatnog partnerstva u zaštiti kritične infrastrukture, s obzirom da se istim regulišu pitanja od značaja za vršenje poslova njene zaštite. S druge strane, u cilju primjene navedenog koncepta, predmetni zakon bi trebao da pretrpi veći broj izmjena u okviru nacionalne legislative, što implicira da bi najcjelishodnije rešenje bilo pravljenje novog Zakona o zaštiti lica i imovine. Naime, poseban član postojećeg zakona se odnosi na obavezno štićene objekte, a Crna Gora je u međuvremenu pristupila procesu usvajanja Zakona o kritičnoj infrastrukturi. Na taj način se stvara neusklađenost između navedenih zakona, što se može negativno odraziti na funkcionisanje privatnog sektora u zaštiti kritične infrastrukture. Slično važi i za većinu članova Zakona o zaštiti lica i imovine koji regulišu djelatnost zaštite, značenje osnovnih pojmova i slično, a koji bi morali da sadrže pojam kritične infrastrukture usklađen sa novim posebnim zakonom. Pored toga, u Zakonu o zaštiti lica i imovine potrebno je predvidjeti i postupanje sa naoružanjem u zaštiti kritične infrastrukture, s obzirom da je predmetnim zakonom definisana njihova upotreba samo u poslovima fizičke zaštite i poslova zaštite stvari u transportu[524].

Od značaja je i usklađivanje Zakona o zaštiti lica i imovine sa Zakonom o oružju kojim je uređena oblast vatrenog oružja između ostalog u domenu nabavke, držanja, nošenja, sakupljanja i prenošenja. Zakonom o oružju, zakonodavac je oružje razvrstao u četiri kategorije, pri čemu je za sve kategorija definisao nabavku, držanje, nošenje i prenošenje. Za oružje A kategorije u koje spada između ostalog automatsko vatreno oružje, vojno oružje, kao i posebna municija nije dozvoljena nabavka, držanje i nošenje oružja i municije kao i nošenje na javnom mestu[525], što je od značaja za eventualnu upotrebu od strane privatnog sektora u obezbjeđenju kritične infrastrukture. I pored navedenih zakonskih rešenja, predmetni zakon bi i u dijelu uslova za nabavku i korišćenje oružja, trebao da pretrpi određene izmjene u cilju prilagođavanja potrebama bezbjednosti kritične infrastrukture. Evidentno je da Zakon na znatno uži način razmatra problematiku oružja na prostoru

[522] Ibid, str. 9
[523]Strategija nacionalne sigurnosti Republike Hrvatske, „*Narodne novine*“, br.73/2017, str. 8; *Austrian Security Strategy, Security in a new decade— Shaping security*, Vienna, 2013, p. 18;
[524] Zakon o zaštiti lica i imovine, „*Službeni list Crne Gore*“, br. 43/2018, čl. 13, 16
[525] Zakon o oružju, *„Službeni list Crne Gore“*, br. 10/2015, čl. 5

Crne Gore, bez ulaženja u specifičnost kao što je mogućnost korišćenja privatnog sektora u zaštiti kritične infrastrukture.

S obzirom da smo u prethodnim djelovima rada nedvosmisleno zaključili da kritična infrastruktura ima poseban značaj za funkcionisanje države i društva, neophodno je obezbijediti mogućnost korišćenja odgovarajućeg vatrenog oružja u njenoj zaštiti. Zbog toga je posebno značajno odrediti vrstu oružja koje se može koristiti u skladu sa specifičnostima kritične infrastrukture. Prilikom predviđanja upotrebe naoružanja u zaštiti kritične infrastrukture bitno je uzeti u obzir da se radi o specifičnim objektima koji mogu obuhvatiti između ostalog i veliko područje koje zahvata i javne površine (na primjer energetska postrojenja), ali i znatno manji prostor, zbog čega je potrebno precizno definisati vrstu i uslove nošenja naoružanja u skladu sa posebnostima objekata kritične infrastrukture. Treba imati u vidu da upotreba oružja u zaštiti kritične infrastrukture posebno dolazi do izražaja u okolnostima koje su definisane strategijom nacionalne bezbjednosti Crne Gore[526]- vanrednom i ratnom stanju.

Pored navedenog, aktuelni Zakon o zaštiti lica i imovine sadrži odredbe koje su posebno značajne iz ugla implementacije predmetnog koncepta, jer otvara mogućnost uspostavljanja operativnog centra za potrebe obavljanja poslova zaštite. To je posebno važno za adekvatnu razmjenu informacija u realnom vremenu između lica angažovanih na poslovima obezbjeđenja kritične infrastrukture i nadležnih državnih organa. Na taj način se otvara mogućnost stalne koordinacije ne samo po pitanju zaštite kritične infrastrukture već i znatno šire, što može pozitivno uticati na stvaranje povjerenja između javnog i privatnog sektora. S obzirom na činjenicu da je iz ugla obezbjeđenja, kritična infrastruktura veoma raznolika, uspostavljanje i funkcionisanje operativnog centra se ne može zakonskim odredbama uopštavati, već treba dati mogućnost da se u svakom konkretnom slučaju ispolji kreativnost u njegovom funkcionisanju, a sve u cilju povećanja bezbjednosti kritične infrastrukture[527].

Iako navedene odredbe Zakona imaju svoju opštu opravdanost, za primjenu koncepta javno-privatnog partnerstva posebno je značajno uspostavljanje uslova za vršenje poslova obezbjeđenja kritične infrastrukture od strane privatnog sektora. Navedeno proizilazi i iz opšteg značaja kritične infrastrukture, zbog čega se poslovi obezbjeđenja ne mogu prepustiti akterima privatnog sektora koji nemaju adekvatne kapacitete i resurse. Kako bi se to postiglo, jedna od mogućnosti je da posebna odredba zakona sadrži posebne kriterijume koje mora ispuniti privatni sektor bezbjednosti za učešće u zaštiti kritične infrastrukture. U aktuelnim odredbama Zakona o zaštiti lica i imovine dati su opšti uslovi[528], međutim nedostaju oni koji se odnose na detaljniju razradu mogućnosti (sposobnosti) privatnog sektora da učestvuje u ostvarivanju zaštite kritične infrastrukture. To se prvenstveno odnosi na propisane stroge zahtjeve za obavljanje takve djelatnosti sa stanovišta finansija i resursa: osnovni kapital, osoblje, sredstva, garancije i slično. Osim toga treba da posjeduje potvrdu izdatu od ovlašćenog sertifikacionog subjekta, koja garantuje njihovu osnovnu usklađenost sa relevantnim administrativnim, radnim, socijalnim i poreskim propisima. Zbog svega navedenog neophodno je uspostaviti odgovarajuće standarde koje privatni sektor treba da ispuni da bi učestvovao u zaštiti kritične infrastrukture. Na taj način bi Crna Gora jasno zakonski uredila predmetnu oblast, što bi

[526] Strategija nacionalne bezbjednosti Crne Gore, „*Službeni list Crne Gore*“, br. 085/18, str. 10
[527] Zakon o zaštiti lica i imovine, *„Službeni list Crne Gore“*, br. 43/2018, čl. 17
[528] Ibid, čl. 18-20

ujedno predstavljalo primjer precizno definisanih standarda u zakonodavnom okviru. S druge strane, može se ocijeniti da postojeća zakonska rešenja u domenu ovlašćenja u vršenju poslova zaštite, kao i dozvola za lica koja vrše poslove zaštite, zadovoljavaju potrebe koje se odnose na zaštitu kritične infrastrukture.

Poseban značaj normativnog uređenja imaju kaznene odredbe, kojima se stimuliše profesionalni i odgovorni rad privatnog sektora u zaštiti kritične infrastrukture, ali i adekvatno sankcionišu propusti. To proizilazi i iz značaja štićene vrijednosti (kritične infrastrukture) za državu i društvo, kao i iz već navedene činjenice da se ovim poslovima mogu baviti samo subjekti privatnog sektora koji imaju adekvatne kompetencije. Zbog toga je sasvim opravdano da kaznene odredbe budu jasnije definisane u domenu kritične infrastrukture.

6.3.4. Zakon o kritičnoj infrastrukturi

Sa aspekta primjene navedenog koncepta poseban značaj ima zakon kojim se reguliše oblast kritične infrastrukture, kroz proces identifikacije, određivanja i zaštite kritične infrastrukture kao i utvrđivanja nadležnosti i uređivanja ostalih pitanja od značaja za kritičnu infrastrukturu. U periodu izrade ovog rada, aktuelan je Nacrt zakona o određivanju i zaštiti kritične infrastrukture Crne Gore, koji je sačinjen u duhu Evropske regulative u ovoj oblasti.

Iz analize Nacrta zakona uočava se da se zakonodavac opredijelio za sektorski pristup u identifikaciji kritične infrastrukture. Definisano je osam sektora kritične infrastrukture, uz otvorenu mogućnost daljeg proširivanja. Jedna od osnovnih primjedbi na predložena zakonska rešenja je uvrštavanje zaštite životne sredine kao sektora kritične infrastrukture. U tom kontekstu, nema dileme da je životna sredina od velikog značaja za funkcionisanje države i društva. Međutim, ista se štiti znatno šire i na posredan način kroz ostale djelatnosti društva i države. Zato se čini nepotrebnim definisanje zaštite životne sredine kao kritične infrastrukture. S druge strane, potpuno je neopravdano izostavljanje proizvodnje i distribucije hrane kao sektora kritične infrastrukture u pomenutom nacrtu zakona. Zaštita lanaca snabdevanja hranom se naziva i „odbrana hrane“, a poljoprivreda i hrana prepoznati su kao kritični nacionalni sektori u mnogim zemljama, kao što su na primjer SAD, Holandija, Švedska i druge države. Pored toga, treba imati u vidu da su česti slučajevi kontaminacije hrane, što nerijetko ima za posledice epidemije, pa i smrtne slučajeve[529]. Hrana posle vode predstavlja najvažniju ljudsku potrebu, a ekonomska stabilnost skoro svih država u svijetu zavisi od stabilnosti ovog sektora. (Tabela br. 17).

[529] Boddie W., Kun L.: Health care, public health and the food and agriculture critical infrastructures, *IEEE Engineering in Medicine and Biology*, vol. 27(6), 2008, pp. 54–58, dostupno na: https://www.researchgate.net/publication/23469138_Health_care_public_health_and_the_food_and_agriculture_critical_infrastructures

SEKTOR	PODSEKTORI
ENERGETIKA	- proizvodnja i distibucija električne energije - prerada, skladištenje i distribucija nafte - skladištenje i distibucija gasa
SAOBRAĆAJ	- drumski saobraćaj - željeznički saobraćaj - vazdušni saobračaj - pomorski saobraćaj
SNABDIJEVANJE VODOM	- snabdijevanje vodom za piće - kontrola kvaliteta vode - kontrola zaliha vode
ZDRAVSTVO	- medicinske službe hitne pomoći - medicinska njega - proizvodnja i distribucija ljekova
FINANSIJE	- finansijska sredstva
INFORMACIONA I KOMUNIKACIONA TEHNOLOGIJE	- IKT softver - IKT komunikacije i hardver
HRANA	- proizvodnja i distribucija hrane - bezbjednost hrane - robne zalihe hrane
FUNKCIONISANJE DRŽAVNIH ORGANA	- sistem državne uprave i sprovođenje zakona - hitne službe - vojna infrastruktura

Tabela br. 35: Predlog sektora i podsektora kritične infrastrukture Crne Gore

Rukovodeći se primjerom Holandije, Crna Gora ima mogućnost da navedene sektore definiše prema prioritetima. Na taj način bi se omogućilo jasno određenje prioriteta djelovanja u zaštiti kritične infrastrukture. Pri tome od posebne važnosti je analiziranje međusobne povezanosti navedenih sektora i uočavanja prednosti pojedinih sektora. Uvođenjem koordinatora za zaštitu kritične infrastrukture, bezbjednosnog plana i drugog Crna Gora je uskladila nacionalno zakonodavstvo u ovoj oblasti sa evropskim standardima, a posebno sa Direktivom 2008/114/EZ. Međutim, osnovni nedostatak na koji se zakonodavcu može prigovoriti je neodređivanjenje ministarstva kome je dato u nadležnost problematika kritične infrastrukture. Naime u početnim odredbama nije naznačeno koje je Ministarstvo odgovorno za zaštitu nacionalne infrastrukture. Kao jedno od mogućih rešenja je Ministarstvo unutrašnjih poslova. S druge strane znatno veći propust je napravljen kod Koordinacionog tijela za zaštitu kritične infrastrukture. Iz zakonskih odredbi se može zaključiti da se radi o ad hoc tijelu koje se uspostavlja u okolnostima nastupanja ugrožavanja, ometanja ili uništenja kritične infrastrukture. Predmetno rešenje nije adekvatno naročito ako se uzme u obzir da se Crna Gora nalazi u procesu uspostavljanja nacionalne kritične infrastrukture. Zato je od posebnog značaja formiranje stalnog tijela koje bi imalo u nadležnost cjelokupne poslove uspostavljanja i funkcionisanja kritične infrastrukture. O potrebi uspostavljanja stalnog Koordinacionog tijela za

zaštitu kritične infrastrukture biće više riječi u dijelu koji se odnosi na organizacioni aspekt zaštite kritične infrastrukture Crne Gore.

6.3.5. Zakon o javno-privatnom partnerstvu

Pored navedene legislative od značaja su i odredbe Zakona o javno-privatnom partnerstvu kojim se uređuje predmetna oblast, i koji se nalazi u proceduri razmatranja i usvajanja u Skupštini Crne Gore. Predloženim rešenjima novog zakona se, između ostalog, na sistematski način uređuju pitanja koja se odnose na ugovorno ulaganje između privatnog i javnog partnera. Na taj način se postiže sinergija autoriteta javnih institucija i ekspertiza i znanja privatnog sektora, a u cilju izgradnje i rekonstrukcije javne infrastrukture, te izvođenja javnih radova i realizovanja javnih usluga. U ovom zakonskom tekstu se kao osnovni cilj javno-privatnog partnerstva ističe povećanje kvaliteta usluga za krajnjeg korisnika, jer bez tog segmenta javno-privatno partnerstvo nema elemente kvalitetnog ugovora i projekta. Novi zakon detaljno razrađuje proceduru zaključivanja ugovora o javno-privatnom partnerstvu - od ideje do realizacije projekta koji se završava ugovorom. U vezi sa tim, prema odredbama Predloga Zakona ugovori javno-privatnog partnerstva se zaključuju na rok od tri godine do 30 godina.

Pomenuti zakonski predlog donosi novine i u institucionalnom okviru u cjelokupnoj politici Crne Gore u području investicionih ulaganja. To se prvenstveno odnosi na formiranje novog tijela - Agencije za investicije Crne Gore, koja je u sistemu pozicionirana u skladu sa Zakonom o državnoj upravi i koja kao takva predstavlja dalji korak u reformi državne uprave i objedinjavanju organa koji se bave različitim segmentima politike u toj oblasti. Naime, pored propisanog djelokruga rada koji se odnosi na javno-privatno partnerstvo, Agencija će objediniti i postojeća tijela iz oblasti investicione politike. Značaj novog zakona je i u tome što precizno definiše pitanja koja se odnose na izradu tenderske dokumentacije i analizu opravdanosti, i što razrađuje cjelokupnu proceduru kroz koju predlog jednog projekta prolazi do konačnog usvajanja. Pritom je značajno i to što je zakonodavac posebno apostrofirao značaj javnog interesa, budući da je analiza opravdanosti koju prati svaki projekat javno-privatnog partnerstva njegov važan segment.

6.3.6. Zakon o javnim nabavkama

S obzirom na određena negativna iskustva u domenu javno-privatnog partnerstva kao što je to slučaj u primjeru Bugarske, za implementaciju predmetnog koncepta posebno su značajne zakonske odredbe o javnim nabavkama. Pored toga, u radu je navedeno da se predmetno partnerstvo realizuje kroz proces javnih nabavki. Crna Gora ima zakonodavni okvir[530] sa razrađenim mehanizmima u području javnih nabavki. Zbog toga je od ključne važnosti dosledno sprovođenje važećeg zakonodavstva i sprečavanje pojava korupcije. Posebne odredbe Zakona o javnim nabavkama sadrže antikorupcijsko pravilo[531], kojim se utvrđuju obaveze naručioca u slučaju preduzetih koruptivnih radnji. Pored navedenog, taj zakon predviđa opšte preventivne mjere za

[530] Zakon o javnim nabavkama, *" Službeni list Crne Gore*", br. 042/11, 057/14, 028/15, 042/17
[531] Ibid, čl. 16

sprečavanje korupcije, uključujući i obavezu naručioca da preduzme sve neophodne mjere u cilju sprečavanja korupcije u bilo kojoj fazi javne nabavke. Naručilac ima obavezu da sve faze postupka oblikuje na način kojim se osigurava da se na vrijeme spriječi pojava korupcije ili da se obezbijede dokazi za radnje korupcije[532].

Za proces javnih nabavki je od posebne važnosti da se osigura što veća konkurencija. To je ujedno i obaveza naručioca, koji je dužan da u okviru svojih objektivnih potreba predmet nabavke odredi tako da omogući što je moguće veću konkurentnost[533]. Drugim riječima, specifikacija javne nabavke ne može biti usmjerena ka izboru određenog ponuđača, već potrebe naručioca moraju biti opisane na način koji je objektivan i pored ostalog usklađen sa ponudom na tržištu. Pored navedenog, bitno je da je naručilac obavezan da osigura da se postupak javnih nabavki sprovodi i dodijeljeni ugovor realizuje u datim rokovima i na način koji je propisan zakonom, ali i uz što manje troškova vezanih za izvršenje javne nabavke[534].

6.4. Organizacioni aspekt

Organizacijom se projektuju i uspostavljaju odnosi među aktivnostima i ljudima koji su uključeni u organizacione resurse. Organizacija započinje određivanjem ciljeva, te nastojanjima da se obezbijedi organizacija kao efikasna struktura autoriteta, kao i uspostavljanjem odgovornosti i stvaranjem komunikacionih kanala neophodnih za realizaciju organizacionih ciljeva, planova i procedura. U vezi sa tim, treba imati u vidu da se javne organizacije osnivaju zakonom, dok sa druge strane privatne bezbjednosne kompanije osnivaju zainteresovana fizička ili pravna lica svojom voljom i u skladu sa zakonom[535].

U praksi svaka organizacija ima svoju organizacionu strukturu kojom ostvaruje postavljene ciljeve u određenom organizacionom okruženju. Zbog toga je od posebnog značaja projektovanje organizacije. Sa aspekta zaštite kritične infrastrukture, organizaciju čine različiti subjekti koji su uključeni u ovaj proces. To umnogome određuje složenost i nameće potrebu stalnog usklađivanja aktivnosti. U radu smo napomenuli da u komparativnoj praksi države obično dodjeljuju odgovornost za određeni sektor nadležnim ministarstvima koja su kompetentna za određenu oblast, što nedvosmisleno upućuje i na kompleksan pristup zaštiti kritične infrastrukture.

Poseban izazov je izbor najboljeg modela zaštite koji odgovara nacionalnim potrebama. Uz to, prilikom uspostavljanja modela ne treba isključiti mogućnost da se isti u praksi pokaže kao neodgovarajući ili neadekvatan. Zato, države često uspostavljaju mehanizme kojima se osigurava da se politika u ovoj oblasti periodično preispituje u cilju otklanjanja uočenih propusta i slabosti. Takođe, uočavaju se i različiti pristupi država organizaciji zaštite kritične infrastrukture s obzirom da se predmetna djelatnost može naći u djelokrugu nadležnosti ministarstava za unutrašnje poslove ili odbrane.

[532] Ibid, čl. 15
[533] Ibid, čl. 25
[534] Ibid, čl. 87-91
[535] Stevanović O.: *Bezbednosni menađment*, Kriminalističko-policijska akademija, Beograd, 2012, str. 23

Sa aspekta predmeta ovog rada, u Crnoj Gori poseban značaj imaju Koordinaciono tijelo za zaštitu kritične infrastrukture, ali kao stalni organ, kao i privatni sektor bezbjednosti angažovan na poslovima zaštite kritične infrastrukture.

6.4.1. Koordinaciono tijelo za zaštitu kritične infrastrukture

Iako postoje različiti modaliteti, mnoge savremene države su formirale vladinu agenciju koja se nalazi u centru zaštite nacionalne kritične infrastrukture. Najvažniji zadatak takve agencije je uloga koordinatora u određenju i sprovođenju nacionalnog pristupa zaštiti kritične infrastrukture. Nacrtom zakona o određivanju i zaštiti kritične infrastrukture Crne Gore je predviđeno Koordinaciono tijelo za zaštitu kritične infrastrukture. S obzirom da smo u prethodnom dijelu rada definisali određene zakonodavne izmjene u toj oblasti, u ovom dijelu navedeno tijelo posmatraćemo kao stalni organ zadužen za poslove zaštite kritične infrastrukture.

Iako je obim i sadržaj poslova Koordinacionog tijela raznovrstan, iste možemo uslovno svrstati u nekoliko osnovnih funkcija:

Planiranje predstavlja osnov za ostale djelatnosti i aktivnosti Koordinacionog tijela za zaštitu kritične infrastrukture. S obzirom na misiju koja je dodijeljena Koordinacionom tijelu, planiranje koje se u okviru njega sprovodi je vezano za problematiku kritične infrastrukture. S druge strane, samo planiranje zahtijeva jasno definisane ciljeve kao i utvrđivanje svih mogućih puteva postizanja tih ciljeva. Za Koordinaciono tijelo je značajno strateško planiranje kojim se ostvaruju definisane misije, kao i operativno planiranje kojim se ostvaruju postavljeni zadaci u kraćem vremenskom periodu. U praksi se proces planiranja uobličava kroz izradu planova sadržanih u više planskih dokumenata. Ti planovi moraju da sadrže, između ostalog, i ciljeve koji se žele postići, zadatke, snage i sredstva angažovana na ostvarivanju zadataka, rokove, koordinaciju i saradnju između različitih subjekata.

Koordinacija je funkcija Koordinacionog tijela kojom se dovode elementi strukture u skladan odnos i usklađuju aktivnosti više učesnika u jednom procesu, što je slučaj i sa kritičnom infrastrukturom. Ostvarivanjem koordinacije sa različitim subjektima omogućava se racionalno korišćenje ograničenih resursa. U tom smislu, Koordinaciono tijelo treba da ostvaruje koordinaciju sa nadležnim ministarstvima u skladu sa sektorskim principom definisanja kritične infrastrukture. S druge strane, nadležna ministarstva posjeduju kapacitete i stručnost od značaja za funkcionisanje kritične infrastrukture. Uspostavljanje adekvatne eksterne povezanosti nije vezano samo za nadležna ministarstva već i za cjelokupan obavještajno-bezbjednosni sektor Crne Gore. To je ujedno i odraz potrebe koordinacije u razmjeni informacija koje su od značaja za funkcionisanje sistema bezbjednosti kritičnih infrastrukturnih objekata. S druge strane, neposredna koordinacija se ostvaruje sa koordinatorima za zaštitu kritične infrastrukture i u okolnostima angažovanja privatnog sektora koordinacija se ostvaruje sa privatnim sektorom u segmentu zaštite kritične infrastrukture. Pored navedenog, koordinacija se mora ostvarivati i sa nadležnim policijskim službama, što je od posebnog značaja u okolnostima ugrožavanja imovine i lica u većem obimu i težeg narušavanja javnog reda i mira.

Kontrola je značajna funkcija koja ima za cilj da otkrije eventualna odstupanja od planiranih aktivnosti i sadržaja i da ukaže na postupak korekcije u zaštiti kritične infrastrukture. Pored toga, kontrolom se provjerava i funkcija planiranja na način da se utvrđuje da li je postavljene ciljeve i

zadatke moguće ostvariti u realnim uslovima. U cilju uspostavljanja realne kontrole Koordinaciono tijelo mora definisati objektivne parametre na osnovu kojih realizuje kontrolnu funkciju. Na taj način se ostvaruje mogućnost upoređivanja ostvarenih rezultata sa planiranim ciljevima i zadacima. Takođe, kontrolom treba da se otkriju odstupanja od plana, ali i da se predloži preduzimanje korektivne akcije kako bi se plan ostvario. U procesu kontrole se provjerava i sam proces planiranja, tako što se preispituje mogućnost izvršenja postavljenih ciljeva i zadataka u realnim uslovima. Iako su planiranje i kontrola faktički povezane aktivnosti, njihovo odvajanje povećava značaj svake od tih funkcija i ohrabruje zaposlene da pažljivije obavljaju kontrolu kako bi bili sigurni da određene aktivnosti nijesu zapostavljene ili loše obavljene. S obzirom na složenost sistema zaštite kritične infrastrukture, potreba za kontrolom kao posebnom funkcijom se povećava.

Izvještavanje i informisanje je posebna funkcija Koordinacionog tijela koja se može ostvariti na različite načine. Na primjer, izvještavanje o izvršavanju poslova ostvaruje se putem uobičajenih oblika službenog komuniciranja, prije svega dostavljanjem informacija, izvještaja, analiza i drugih analitičko-informativnih materijala. Izvještaji predstavljaju kompleksno izlaganje i prikaz rezultata i informacija analitičkog sagledavanja stanja bezbjednosti, pojava i događaja, preduzetih mjera i radnji, odnosno stepena realizacije programskih i planskih dokumenata u vezi s radom pojedinih subjekata angažovanih na poslovima kritične infrastrukture. Izvještavanje se vrši po pravilu u pisanoj formi. Samo izuzetno, iz razloga hitnosti ili pogodnosti usmenog komuniciranja, odnosno kada se izvještavanje ne može izvršiti u pisanoj formi, ono se sprovodi usmeno, neposredno ili preko tehničkih sredstva veze. U toj funkciji, Koordinaciono tijelo treba da ima ulogu organa koji prima izvještaje od subjekata kritične infrastrukture, uz obavezu dostavljanja periodičnih izvještaja Skupštini Crne Gore i to Odboru za bezbjednost i odbranu, a preko Ministarstva unutrašnjih poslova. Navedenom odboru bi se dostavljali godišnji izveštaji o zaštiti i funkcionisanju kritične infrastrukture Crne Gore, realizovanim zadacima kao i o eventualnim problemima.

S druge strane, informisanje se ostvaruje razmjenom podataka i saznanja između svih subjekta u okviru kritične infrastrukture, kao i između njih i najšire (opšte) javnosti. Informisanje javnosti o stanju kritične infrastrukture omogućava da se unapređuje bezbjednosna kultura građana kao i da se otklone eventualni nesporazumi i međusobno nepovjerenje, te da se javnost pridobije kao saradnik i partner u ostvarivanju što povoljnijeg stanja zaštićenosti kritične infrastrukture, u okvirima poštovanja povjerljivih podataka.

Iz svega navedenog možemo zaključiti da Koordinaciono tijelo mora imati dovoljan kapacitet da bi ostvarilo postavljene ciljeve. Njegova organizaciona struktura mora biti uspostavljena na osnovu podjele rada, grupisanja poslova, delegiranja autoriteta i odgovornosti i odgovarajućim mehanizmima koordinacije i kontrole. Zbog svega toga mora imati strukturu koju bi činile organizacione jedinice zadužene za ostvarivanje određenih funkcija.

6.4.2. Privatni sektor bezbjednosti u zaštiti kritične infrastrukture

Privatni sektor bezbjednosti u zaštiti kritične infrastrukture u Crnoj Gori je povezan sa Koordinacionim tijelom i Ministarstvom unutrašnjih poslova. U pogledu zakonskih ovlašćenja, proces dobijanja sertifikata za vršenje poslova obezbjeđenja kritične infrastrukture, kao i gubljenja prava za bavljenje tim poslovima, u nadležnosti je Ministarstva unutrašnjih poslova. Kada je riječ o

nadležnostima Koordinacionog tijela, njegova uloga u ovom domenu je prije svega da razmjenjuje informacije koje su od značaja za obezbjeđenje kritične infrastrukture sa privatnim sektorom.

Zbog međusobne povezanosti Koordinacionog tijela i privatnog sektora bezbjednosti od značaja je razvijanje partnerskog odnosa. Kao jedna od mogućnosti unapređenje odnosa je i učešće predstavnika privatnog sektora u radu Koordinacionog tijela. Pored jačanja partnerskih odnosa to je od izuzetnog značaja i za povećanje efikasnosti i koordinacije između javnog i privatnog sektora, što posebno dolazi do izražaja u vanrednim situacijama i okolnostima kada je potrebno brzo donošenje odluka i reagovanje na novonastale okolnosti. Učešće predstavnika privatnog sektora je od značaja za rad Koordinacionog tijela kroz sve njegove navedene funkcije, kao stručnog organa koji poznaje djelatnost privatnog sektora bezbjednosti. I bez daljeg navođenja opredeljenja kojima bi bilo podržano navedeno rešenje, u mnogome bi se unaprijedio i učinio efikasnijim rad Koordinacionog tijela. Međutim, prilikom određivanja predstavnika privatnog sektora, treba uzeti u obzir činjenicu da Koordinaciono tijelo razmjenjuje podatke koji po svojoj prirodi mogu sadržati određen stepen tajnosti. Zbog toga je važno izvršiti bezbjednosnu provjeru predstavnika privatnog bezbjednosnog sektora. U vezi sa tim neophodno je pridržavati se Zakona o tajnosti podataka[536] kojim je zakonodavac definisao pristup tajnim podacima.

Za privatni sektor je od značaja da se normativno preciznije urede obaveze u izradi planova neophodnih za zaštitu kritične infrastrukture. Drugim riječima, potrebno je odgovarajućim izmjenama Zakona o zaštiti lica i imovine detaljnije urediti organizacione aspekte djelovanja privatnog sektora bezbjednosti u zaštiti kritične infrastrukture, definisati minimalne kapacitete i resurse, kao i odnose aktera privatnog sektora sa drugim subjektima u toj oblasti. Na taj način će se stvoriti uslovi za efikasnije funkcionisanje privatnog sektora bezbjednosti, ali i obezbijediti adekvatnije vršenje kontrole u području zaštite kritične infrastrukture. Privatni sektor bezbjednosti u Crnoj Gori je u obavezi da svoje planove rada i postupanja usklađuje i sa Strategijom nacionalne bezbjednosti Crne Gore. To se prvenstveno odnosi na definisane izazove, rizike i prijetnje sa aspekta kritične infrastrukture u svakom konkretnom slučaju obezbjeđenja i zaštite. Pored toga, privatni sektor bezbjednosti mora da ima pripremljene planove rada u slučaju redovnog stanja, vanrednog stanja i ratnog stanja, kako je to određeno Strategijom nacionalne bezbjednosti, i moraju postojati mjere koje treba preduzimati u svakom od navedenih slučajeva.

Za organizaciju i djelatnost privatnog sektora bezbjednosti od posebnog je značaja ugovor o javno-privatnom partnerstvu. Ugovorom se određuju, između ostalog, obaveze privatnog sektora angažovanog u zaštiti kritične infrastrukture. U vezi sa tim, uputno je da se tim ugovorom regulišu i obaveze propisane Bezbjednosnim planom operatora (Operator security plans) kritične infrastrukture. Pri tome, predmetni plan mora biti usklađen sa nacionalnim zakonodavstvom. Ovako definisane ugovorne obaveze su važne i sa aspekta ostvarivanja kontrole privatnog sektora bezbjednosti i stvaranja odgovornog odnosa subjekata tog sektora u pogledu preuzetih obaveza.

[536] Zakon o tajnosti podataka, *„Službeni list Crne Gore“*, br. 14/08, 76/09, 41/10, 40/11, 38/12, 44/12, 14/13, 18/14 i 48/15, čl. 25-54

Z A K LJ U Č A K

Iako predstavlja trend koncept kritične infrastrukture u savremenom dobu dobija posebnu dimenziju. To je ujedno i posledica međuzavisnosti različitih infrastrukturnih elemenata države, kao i promjene percepcije bezbjednosti. Zbog značaja koji ima, kritična infrastruktura se nalazi u vrhu agende nacionalne bezbjednosti mnogih država, što potvrđuje činjenica da se na potencijalne prijetnje njenog ugrožavanja gleda kao na problem od najvećeg značaja za nacionalnu bezbjednost. S druge strane, savremene države imaju različite pristupe kako u određenju kritične infrastrukture, tako i u njenoj bezbjednosti, što je između ostalog posledica njihovog različitog geopolitičkog, geostrateškog i geografskog položaja. Neosporno je da se u današnjem vremenu kritična infrastruktura proširuje i na virtuelni (sajber) prostor, te da je prisutna sve veća povezanost različitih sektora infrastrukture, uz zahtjeve za koordinisanim pristupom u njenoj zaštiti. S obzirom na složenost kritične infrastrukture i njena zaštita predstavlja kompleksan proces koji obuhvata različite aktivnosti i djelatnosti usmjerene na sprečavanju fizičkih i drugih napada. U vezi sa tim, težište je na aktivnostima koje su usmjerene na odvraćanje od napada, što ukazuje da preventivni pristup zaštiti kritične infrastrukture ima dominantan značaj.

Nesumnjivo je da efikasan sistem zaštite kritične infrastrukture stvara preduslove za normalno i nesmetano funkcionisanje šireg društvenog sistema. U skladu sa tom činjenicom, u Crnoj Gori se ulažu veliki napori u cilju utvrđivanja i implementacije adekvatnih mehanizama zaštite kritične infrastrukture. Otežavajući činioci na tom planu su prije svega vezani za širok spektar vitalnih sektora koje kritična infrastruktura obuhvata, poput saobraćaja, transporta, proizvodnje i distribucije energije, informacionih i komunikacionih sistema, zdravstvenih službi, sistema za snabdijevanje vodom i hranom i slično. S druge strane, politika zaštite kritične infrastrukture predstavlja jedan veoma složen sklop različitih strategija, metodologija i planova usmjerenih ka prevenciji rizika i prijetnji kao i sprečavanju većih posledica koje mogu nastati usled kriznih situacija. Kompleksnost te problematike zahtijeva jedan krajnje multidisciplinarni pristup i primjenu namjenski izrađenih alata u zaštiti kritične infrastrukture.

Evropska unija pridaje veliki značaj normativi, standardima i politikama u području zaštite kritične infrastrukture, i danas u toj oblasti predstavlja jednog od ključnih aktera na međunarodnom planu. EU i njene države članice su od 2004. godine pokrenule niz inicijativa i istraživačkih programa kako bi se ispitali različiti aspekti zaštite i prijetnji po kritičnu infrastrukturu, kao i uticaji koji ugrožavanje i oštećenje kritičnih infrastruktura mogu imati na privredu, zdravstvo, sistem komunikacija, obrazovanje i druge segmente ljudske djelatnosti i društvenog života. Pitanja funkcionisanja i koordinacije između država članica Evropske unije u tom domenu regulisani su Direktivom EU o zaštiti kritičnih infrastruktura iz 2008. godine. Direktiva se može posmatrati i kao odgovarajući model koji pruža mogućnosti za preuzimanje određenih rešenja u zaštiti i funkcionisanju kritične infrastrukture u Crnoj Gori.

U pogledu utvrđivanja i primjene mjera zaštite kritične infrastrukture, sve savremene države, uključujući i Crnu Goru, moraju da utvrde i redosled postupaka. To se prvenstveno odnosi na identifikaciju kritične infrastrukture, izradu kataloga kritične infrastrukture, osposobljavanje osoblja angažovanog na poslovima i zadacima u sistemima kritične infrastrukture, razmjenu informacija kao

i na uvježbavanje reagovanja osoblja i sistema za zaštitu kritične infrastrukture u različitim situacijama.

Zaštita kritične infrastrukture se može posmatrati i iz ugla procesa prevencije i odgovora na vanredne situacije. Zadaci organizacije su uspostavljanje, primjena i održavanje procedura za identifikovanje potencijalnih incidenata koji mogu negativno uticati na određenu organizaciju, njene aktivnosti, funkcije, usluge, zainteresovane strane i okruženje. Procedure su u funkciji prvenstveno zaštite života i imovine, kao i sprečavanje prerastanja incidenta u vanrednu situaciju ili katastrofu, smanjenje perioda prekida operacija ili djelatnosti organizacije, oporavak najvažnijih djelatnosti, povratak na redovne aktivnosti, zaštita reputacije organizacije i slično.

Javno-privatno partnerstvo između državnog i privatnog sektora postoji vjekovima, ali su motivi i interesi bili različiti. Vremenom se predmetni koncept proširio i na zajedničke tehnologije, ekološke projekte, kao i na javno-privatna partnerstva u oblasti obrazovanja, zdravstvene zaštite i izvršenja zatvorskih kazni. Značajna karakteristika je i da svaki od učesnika ulaže nešto u partnerstvo, da bi partnerstvo bilo uspješno, svaki od partnera ulaže materijalni ili nematerijalni resurs i na taj način se ostvaruje sinergijski efekt za sve učesnike u projektu. Pored navedenog, velika pažnja je usmjerena na prednosti javno-privatnog partnerstva u zaštiti kritične infrastrukture.

Postavljene hipoteze u radu su verifikovane odgovarajućim metodološkim pristupom istraživanju, što je podrazumijevalo analizu različitih izvora podataka, kao i komplementarno korišćenje različitih istraživačkih metoda, uključujući analizu naučne i stručne literature, analizu pravnih dokumenata, metod sekundarne analize, metod analize sadržaja, statistički metod, metode modelovanja i komparativne metode. Pored toga, teorijska razmatranja su potkrijepljena i empirijskim istraživanjem, kojim su potvrđeni polazni hipotetički stavovi i rezultati teorijskog istraživanja.

Za potrebe izrade doktorske disertacije sprovedeno je empirijsko istraživanje u formi anketnog upitnika, kojim su anketirana lica koja se neposredno bave poslovima vezanim za zaštitu i funkcionisanje kritične infrastrukture Crne Gore. Prikupljeni su podaci po unaprijed pripremljenim i formulisanim pitanjima. Rezultati empirijskog istraživanja su nedvosmisleno ukazali na probleme vezane za normativni okvir zaštite kritične infrastrukture. Na osnovu analizirane normativno-pravne i zakonske regulative, istraživanje je ukazalo na potrebu usvajanja novih zakonskih rešenja u ovoj oblasti. U vezi sa tim, identifikovani su problemi vezani za uspostavljanje koncepta javno-privatnog partnerstva u zaštiti kritične infrastrukture Crne Gore. Pored toga, sublimirane su i brojne iznijete sugestije u vezi sa zaštitom kritične infrastrukture.

Sprovedeno teorijsko i empirijsko istraživanje je potvrdilo generalnu hipotezu da uvođenje koncepta javno privatnog partnerstva u zaštiti kritične infrastrukture Crne Gore podrazumijeva prilagođavanje postojeće zakonske regulative. Aktuelne odredbe nacionalnog zakonodavstva ukazuju na potrebu dogradnje pojedinih zakona. U toku izrade ovog rada u procesu je usvajanje Zakona o javno-privatnom partnerstvu kao i Zakona o kritičnoj infrastrukturi koji i pored toga mora da pretrpi određene izmjene. S druge strane neophodno je prilagoditi zakon koji se odnosi na privatni sektor bezbjednosti. To je ujedno i ključni zakon koji treba da prepozna angažovanje privatnog sektora u zaštiti kritične infrastrukture. Pored toga Crna Gora kao i države u okruženju nema dugu tradiciju privatnog sektora bezbjednosti što zahtijeva posebnu pažnju i jasno definisanje zakonskih odredbi koje se odnose i na ovaj segment.

Na osnovu obavljenog istraživanja potvrđena je prva posebna hipoteza da u Crnoj Gori oblast kritične infrastrukture nije zakonom uređena. Uz sprovedenu teorijsku analizu aktuelnog zakonodavnog okvira, i rezultati empirijskog istraživanja su pokazali da većina ispitanika zastupa stav o nužnosti donošenja posebnog zakona kojim bi se uredila oblast zaštite kritične infrastrukture. S druge strane, pokazalo se da značajan procenat ispitanika smatra da je aktuelna regulativa samo djelimično usklađena sa savremenim oblicima ugrožavanja. Treba imati u vidu da se u periodu izrade ovog rada na javnoj raspravi nalazio Nacrt Zakona o kritičnoj infrastrukturi, koji je krajem marta 2019. godine, saglasno Programu rada Vlade Crne Gore, pripremila međuresorska grupa u Ministarstvu unutrašnjih poslova. Ponuđena rješenja u predmetnom Nacrtu zakona se mogu posmatrati iz različitih uglova, ali je značajno da se Crna Gora, u okviru obaveza koje proističu iz pristupnih pregovora za članstvo u EU, opredijelila za novi koncept, različit od postojećeg koji podrazumijeva obavezno štićene objekte. Nesumnjivo je da je zatečeni koncept zaštite prvenstveno bio posledica dominacije vojnog faktora u području nacionalne bezbjednosti što je uslovilo da se područje kritične infrastrukture prevashodno posmatra iz ugla vojnih priprema za odbranu zemlje.

Istraživanje je pokazalo i da su na izmjenu tog pristupa uticali i uvođenje sekuritizacije u teoriju bezbjednosti kao i činjenica da bezbjednost i odbranu države ne čine samo oružane snage već i drugi sektori. Novi koncept zaštite kritične infrastrukture je i odraz potrebe usklađivanja nacionalnog zakonodavstva u ovoj oblasti u procesu priključenja Crne Gore Evropskoj uniji. Istraživanje je pokazalo i da predmetni Nacrt sadrži određene nedostatke, koji se prvenstveno odnose na ne uvođenje stalnog nacionalnog organa zaduženog za poslove zaštite kritične infrastrukture, koji bi koordinirao svim poslovima uspostavljanja novog sistema kritične infrastrukture. Na taj način bi se stvorile osnove za jedinstven i sinhronizovan pristup ovako značajnoj oblasti. S druge strane, uvrštavanje životne sredine u kritičnu infrastrukturu u Nacrtu zakona se ocjenjuje nepotrebnim, jer se ista štiti posredno kroz ostale djelatnosti države i društva. Pored toga, činjenica je da se uvođenjem životne sredine u zakonski tekst znatno proširuje obim i sadržaj kritične infrastrukture Crne Gore.

Sprovedeno istraživanje je potvrdilo i drugu posebnu hipotezu, po kojoj aktuelni zakonski okvir nije adekvatan modelu javno privatnog partnerstva u zaštiti kritične infrastrukture kojim Crna Gora teži. Navedena konstatacija je ujedno i odraz duge istorije u kome je javni sektor Crne Gore imao dominantan uticaj u mnogim sferama društvenog života. Međutim, proces transformacije države i društva uticao je da postepeno i privatni sektor dobije značajni prostor za ispoljavanje svog djelovanja. U konkretnom slučaju, zakonodavstvo Crne Gore nije u dovoljnoj mjeri prepoznalo mogućnost uključivanja privatnog sektora bezbjednosti u zaštiti kritične infrastrukture. S druge strane, rezultati sprovedenog empirijskog istraživanja ukazuju da zakonodavni okvir djelimično može da zadovolji potrebe javno-privatnog partnerstva u Crnoj Gori. Ipak, značajna većina ispitanika se založila za donošenje posebnog zakona o javno-privatnom partnerstvu. Prema rezultatima istraživanja, privatni sektor bezbjednosti bi trebalo da ima veću ulogu u zaštiti kritične infrastrukture, s obzirom da je relativno većinski stav ispitanika da taj sektor posjeduje potrebne kapacitet za zaštitu kritične infrastrukture.

I pored rezultata istraživanja koji ukazuju na veće mogućnosti učešća privatnog sektora u zaštiti kritične infrastrukture, ograničavajući činilac je u tome što Crna Gora nema zakonski okvir koji bi podržao implementaciju navedenog koncepta. Donošenje Zakona o kritičnoj infrastrukturi bi u tom smislu morale pratiti i izmjene aktuelnog zakona koji se odnosi na privatnu bezbjednost. Jedan

od razloga je neusklađenost pojmovnog aparata između dva navedena zakonska akta što može imati negativne posledice u njihovoj primjeni. Zato je važno usvajanje novog zakona o privatnom obezbjeđenju koji bi sadržao mogućnosti uključivanja privatnog sektora bezbjednosti u zaštiti kritične infrastrukture. S obzirom da Crna Gora nema dugu istoriju privatnog sektora bezbjednosti, ne može se doslovno rukovoditi iskustvima pojedinih država koje su umjesto posebnog zakona uspostavile samo standarde za djelatnost privatnog sektora. Iz tih razloga je znatno uputnije predmetnu oblast regulisati novim zakonom koji bi, između ostalog, sadržao razrađene odredbe koje se odnose na angažovanje privatnog sektora u zaštiti kritične infrastrukture.

Na osnovu obavljenog teorijskog istraživanja potvrđena je i treća posebna hipoteza da model učešća javno-privatnog partnerstva u zaštiti kritične infrastrukture podrazumijeva i implementaciju primjera dobre prakse kakva postoji u razvijenim državama. S obzirom da Crna Gora nema tradiciju primjene koncepta javno-privatnog partnerstva, od značaja je sprovedena analiza dosadašnjih iskustava drugih država, kao što su SAD i Velika Britanija, koje imaju viševjekovnu tradiciju u ovoj oblasti. Naročito su značajna iskustva ovih zemalja u poslednjim decenijama, posebno nakon terorističkog napada u SAD 2001. godine, koji se smatra ključnim događajem na planu pojačanog angažovanja privatnog sektora u zaštiti kritične infrastrukture. Istraživanje je ukazalo i da je primjer navedenih država posebno značajan u segmentu koji se odnosi na razmjenu informacija, kao i na stvaranje povjerenja i partnerskih odnosa između javnog i privatnog sektora. Naime, u ovim državama a naročito u SAD-u privatni sektor je nezamjenljiv u obezbjeđenju kritične infrastrukture, pri čemu su partnerski odnosi i povjerenje između javnog i privatnog sektora bezbjednosti stvarani postupno i kroz dugogodišnju praksu. S druge strane, rezultati istraživanja su pokazali da evropske države predmetni koncept razvijaju u skladu sa preporukama EU, uz uvažavanje nacionalnih specifičnosti.

Posebno su značajna iskustva država koja ukazuju na uočene propuste i slabosti u primjeni ovog koncepta. To se između ostalog odnosi na proces realizacije javnih nabavki kroz koje se ostvaruje primjena ovog koncepta. Naime, proces javnih nabavki je često predstavljao problem i u mnogim drugim djelatnosti naročito za države u okruženju. Samo jasan zakonski okvir, dosledna primjena zakonski odredbi kao i izgrađen sistem integriteta u procesu javnih nabavki može predstavljati uspjeh.

LITERATURA

1. Alós R., Urbano X.: *Report on the Trade Unions and Employers Organisations in the Sector of Private Security in Spain*, QUIT, Universitat Autònoma de Barcelona, Barcelona 2003
2. ASIS International, ASIS International Joins Department of Homeland Security and FBI on Information-Sharing Project, ASIS International Press Release, June 23, 2004, dostupno na: https://www.businesswire.com/news/home/20040623005739/en/ASIS-International-Joins-Department-Homeland-Security-FBI
3. Anson County (NC) Sheriff's Office, „History—The Middle Ages", dostupno na: http://www.ansonsheriff.com/TheOffice/History.aspx
4. A World bank Resource for PPP in Infrastructures, dostupno na: https://ppp.worldbank.org/public-private-partnership/
5. Agence nationale de la sécurité des systèmes d'information, dostupno na: https://www.ssi.gouv.fr/en/
6. Akintoye A., Beck M., Hardcastle C.: *Public-Private Partnerships Managing Risk and Opportunities*, Blackwell, Science, Oxford, 2006
7. Austrian Cyber Security Strategy, Vienna, 2013, dostupno na: https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf
8. *Austrian Security Strategy, Security in a new decade— Shaping security*, Vienna, 2013
9. Bada M., at all: *Computer Security Incident Response Teams(CSIRTs), An Overview*, Global Cyber Security Capacity Centre, University of Oxford, 2014
10. Barbaro M., Gillis J.:Wal-Mart at forefront of hurricane relief, *The Washington Post*, September 6, 2005, dostupno na: https://www.washingtonpost.com/archive/business/2005/09/06/wal-mart-at-forefront-of-hurricane-relief/6cc3a4d2-d4f7-4da4-861f-933eee4d288a/?noredirect=on
11. Bastin J.: *Public-Private Partnerships: A Review of International and Austrian Experience*, Public Private Partnership, Studiengesellschaft für Wirtschaft und Recht, Wirtschaftsuniversität Wien, Wienna, 2003
12. Bettignies J-E, Ross T.W. :The Economics of Public-Private Partnerships, Sauder School of Business, *Canadian Public Policy*, vol.XXX, (2), University of British Columbia, 2004
13. Bing L., Akintoye A.: An overview of public–private partnership, in: Akintoye A., Beck M., Hardcastle C. (eds): *Public–Private Partnerships: Managing Risks and Opportunities*, Blackwell Oxford, 2003
14. Blaton A., Vliegher De D.: An update on the use of public private partnerships (PPPs) in Belgium, dostupno na: https://www.lexology.com/library/detail.aspx?g=917445f5-4c66-42f2-a55a-c9b29425e418
15. Boddie W., Kun L.: Health care, public health and the food and agriculture critical infrastructures, *IEEE Engineering in Medicine and Biology*, vol. 27(6), 2008, dostupno na: https://www.researchgate.net/publication/23469138_Health_care_public_health_and_the_food_and_agriculture_critical_infrastructures

16. Boin A.; Smith D.: Terrorism and Critical Infrastructures: Implications for Public–Private Crisis Management, *Public Money & Management*, Volume 26, Issue 5, Taylor & Francis, 2006
17. Boin R.A.: From Crisis to Disaster: Toward an Integrative Perspective, in: Perry R., Quarantelli E.L.(eds): *What is a Disaster? New Answers to Old Questions*, Xlibris Press, Philadelphia 2005
18. Brøgger T., Kristiansen F.Ø.: Denmark, In: Çakmak Z., Çağdaş E. E.: *Global Public-Private partnership (PPP) guide*, Çakmak Yayınevi ve Medya Limited Şirketi, Ankara, 2016
19. Brenner J.F.: Eyes wide shut: The growing threat of cyber attacks on industrial control systems. Bulletin of the Atomic Scientists., 69 (3), 2013, pp. 15–20, dostupno na: https://journals.sagepub.com/doi/pdf/10.1177/0096340213501372
20. Brooks C: Public Private Partnerships And The Cybersecurity Challenge Of Protecting Critical Infrastructure, Forbes, May 6, 2019, dostupno na: https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/#7f93f8fc5a57
21. Bruijne De M., Eeten Van M.: Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment, *Journal Contingency Crisis Management*, Volume 15, Issue 1 ,2007
22. Brunner E. M., Suter M.: *International CIIP handbook 2008/2009*, Center for Security Studies, Zurich, 2008
23. Brussels Summit Declaration, dostupno na: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=uk
24. Ukraine – EU – NATO Cooperationfor Countering Hybrid Threats in the Cyber Sphere, Centre for Global Studies "Strategy XXI" Kyiv, 2019
25. Bult-Spiering M., Dewulf G.: *Strategic issues in public–private partnerships: an international perspective*, Blackwell Publishing, Oxford, 2006
26. Bundesministerium des Innern Nationale Strategie zum Schutz Kritischer Infrastrukturen, Bundesministerium des Innern. Berlin, 2009
27. Bush V.: *Science: The Endless Frontier, 1945*, dostupno na: http://www.nsf.gov/about/history/vbush1945.html
28. Busch E. N., Givens D. A: Public-Private Partnerships in Homeland Security: Opportunities and Challenges, *Homeland Security Affairs*, Volume 8, article 18, 2012, dostupno na: https://www.hsaj.org/articles/233
29. Bush G.: *Homeland Security Presidential Directive 7*: Critical Infrastructure Identification, Prioritization and Protection, Washington, DC 2008, dostupno na: https://www.hsdl.org/?abstract&did=441950
30. Van Den Hurk M., Van Garsse S., Verhoest K.:*Ten years of PPP in Belgium: an overview*, Federale Overheidsdienst Financiën – België, 2013
31. Vaughan R., Pollard, R.: *Rebuilding America VOL1, Planning and Managing Public Works*, Council of State Planning Agencies,1984

32. Velde van de D., Veeneman W.,Schipholt L. L. : Competitive tendering in The Netherlands: central planning vs. functional specifications,Transportation Research Part A: *Policy and Practice*, 42, (9), 2008
33. Vidriková D., Boc K., Dvořák Z., Řehák D.:*Critical Infrastructure and Integrated Protection*, The Association of Fire and Safety Engineering, Ostrava, Czech Republic, 2017
34. Vitel P., Bliddal H.: French Cyber Security and Defence: an overview, *Information & Security: An International Journal*, vol. 32, 2015, dostupno na: https://it4sec.org/system/files/3209_france.pdf
35. Vujačić S.: Montenegro, In Çakmak Z., Ergün E. C.*: Global public-private partnership (PPP) guide*, Çakmak Yayınevi ve Medya Limited Şirketi, 2016
36. García Z. A., Jeun I.: *Best practices for Critical Information Infrastructure Protection (CIIP): experiences from Latin America and the Caribbean and selected countries*, Inter-American Development Bank, Washington, D.C., 2016
37. Get Safe Online Free expert advice, доступно на:https://www.getsafeonline.org
38. Gillet E.: Belgium, In*: PPP in Europe, CMS Legal Services* -European Economic Interest Grouping, 2009, p. 11-12, доступно на: https://cms.law/en/CHE/Publication/PPP-in-Europe
39. Giménez-Salinas A: New approaches regarding private/public security, *Policing and Society*, vol. 14, No. 2 2004
40. Glass T.A., Schoch-Spana, M.: Bioterrorism and the People: How to Vaccinate a City against Panic, *Clinical Infectious Diseases*, Volume 34, Issue 2. Oxford academic, 2002
41. *Global Guide toPublic-PrivatePartnerships*, Allen & Overy LLP, UK, 2010
42. *Good practices manual for CIP policies, For policy makers in Europe*, European Commission-Directorate-General Home Affairs, 2011
43. Gordon K., Dion M.: Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security", OECD, France, 2008
44. Graeme A. H. Carsten G., Anthony E. B. : *International Handbook onPublic–Private Partnerships*, Edward Elgar Publishing, UK, 2010
45. Graeme H., Carsten G.: *The Challenge of Public–Private Partnerships, Learning from International Experience*, Books Ltd, Bodmin, Cornwall, 2005
46. *Green Paper on PPP and Community law on public contracts and concessions*, 2004, COM(2004)327,
47. Greve C., Mörth U.: Public–private partnerships: the Scandinavian experience, in Graeme A. H., Greve C., Boardman E. A.: *International Handbook on Public–Private Partnerships*, Edward Elgar Publishing, 2010
48. Grenda B., Ślachcińska E.: Terrorist Threats for the Critical Infrastructure of the State, Advances in Economics, *Business and Management Research*, volume 31, Atlantis Press, 2017
49. Grimsey D., Lewis K. M.: *Public private partnerships-the world wide revolution in Infrastructure Provision and project finance*, Edward Elgar Publishing Limited, UK, 2007
50. Grimsey D., Lewis M.: PPP- *The worldwide revolution in infrastructure provision and project finance*, Edvard Elgar Publishing Limited, 2004

51. Grimsey D., Lewis M.K.:*Public Private Partnerships - the world wide revolution in Infrastructure Provision and Project Finance,* Edward Elgar Publishing limited, UK, 2004
52. Gritzalis D., Stergiopoulos G., Kotzanikolaou P., Magos E., Lykou G.: Critical infrastructure protection: a holistic methodology for Greece,*Conference on security of industrial control and cyber physical systems (CyberICPS)*, Springer, 2016
53. Gritzalis D., Theocharidou M., Stergiopoulos G.: *Critical InfrastructureSecurity and ResilienceTheories, Methods, Tools and Technologies*, Springer, Switzerland, 2019
54. Guidelines for Successful Public – Private Partnerships, European commission, March 2003, dostupno na: http://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf
55. Davidovic D., Kesetovic Z., Pavicevic O.: National Critical Infrastructure Protection in Serbia: The Role of Private Security, *Journal of Physical Security* 6(1), 2012, dostupno na: http://rbsekurity.com/JPS%20Archives/JPS%206(1).pdf
56. Дамјановић Д., Павловић-Крижанић Т., Петри Г.: *Партнерство јавног и приватног сектора-Добра и лоша искуства*, ПАЛГО центар, Београд, 2010
57. *Data Protection Act 1998,* dostupno na: http://www.legislation.gov.uk/ukpga/1998/29/contents
58. De Bettignies J. E., Ross T. W.: The economics of public–private partnerships: some theoretical contributions, *International Handbook on Public–Private Partnerships*, Cheltenham, Northampton, UK, 2010
59. *Dedicated Public-Private Partnership Units A Survey of Institutional and Governance Structures*, OECD Publishing, 2010
60. Dempsey S. J.:*Introduction to Private Security, Second Edition*, Wadsworth, Cengage Learning, 2011
61. Denver Board of Water Commissioners, Agreement for Armed Security Guard Services at Denver Water Facilities (April 9, 2014), dostupno na: http://www.denverwater.org/docs/assets/CF9D67A3-AAE5-1B28-92C82953B0D8C0A5/IIc.pdf
62. Department of Homeland Security, Critical Infrastructure Partnership Advisory Council, dostupno na: https://www.dhs.gov/critical-infrastructure-partnership-advisory-council
63. Department of Homeland Security, Private Sector Resources Catalog, dostupno na: https://www.dhs.gov/private-sector-resources-catalog
64. *Directive 2004/17/EC* of the European Parliament and of the Council of 31 March 2004 relating to the coordination of procedures for the award of contracts in the water, energy, transport and postal services sectors
65. *Directive 2004/l8/EC* of the European Parliament and of Council of 31 March 2004 relating to the coordination of procedures for the award of public works, supply and services contracts
66. Dzhekova R., Kojouharov A.: Mission Critical, Mission Impossible – The Role of PSCs in Protecting Critical Infrastructure in Bulgaria, In: Klopfer F., and Amstel van N.(eds.): *Private Security in Practice: Case studies from Southeast Europe*, DCAF, 2016
67. Dzhekova R., Rusev A.: Bulgaria, In: Franziska K.,, Amstel van N. (eds), *A Force for Good? Mapping the private security landscape in Southeast Europe*, DCAF Geneva 2015

68. Dunn-Cavelty M., Suter M.: Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection, *International Journal of Critical Infrastructure Protection*, 2, 2009
69. *Electronic Communications Act 2000*, dostupno na: http://www.legislation.gov.uk/ukpga/2000/7/contents
70. Eismann C.: Trends in critical infrastructure protection in Germany, *Safety Engineering Series,* Vol. IX, No. 2, Technical university of Ostrava, 2014
71. Engel E., Fischer R., Galetovic A.: Publice-private partnerships: when and how, Department of Economics, Yale University, 2008, dostupno na: http://www.econ.uchile.cl/uploads/publicacion/c9b9ea69d84d4c93714c2d3b2d5982a5ca0a67d7.pdf
72. EU SolidarityProgramme on the consequences of terrorism dostupno na: http://www.consilium.europa.eu/uedocs/cmsUpload/15480EU_Solidarity_Programme.pdf
73. *EU Cybersecurity Initiatives-Working Towards a more Secure OnlineEnvironment. Factsheet*, European Commission. 2017, dostupno na: http://ec.europa.eu/information_society/newsroom/image/document/20173/factsheet_cybersecurity_update_january_2017_41543.pdf
74. *PPP Guide,* European PPP Expertise Centre(EPEC), dostupno na: http://www.eib.org/epec/g2g/intro2-ppp.html
75. European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI)), dostupno na: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167
76. *Council Directive 2008/114/EC of 8 December 2008* on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection
77. Communication from the Commission to the Council, theEuropean Parliament, the Economic and Social Committee and the Committee of the Regions, *The European Security Agenda,* COM(2015)185 final, European Commission, 2015,
78. *Eurostat Treatment of Public-Private Partnerships, Purposes, Methodology and Recent Trends*, European PPP Expertise Centre, 2010
79. Executive Order 13010 - Critical Infrastructure Protection, *Federal Register*, Vol. 61, No. 138, dostupno na: https://www.hsdl.org/?abstract&did=1613
80. *Executive summary of barriers to PPP in municipal and regional public works contracts*, Danish Competition and Consumer Authority, 2013, dostupno na: https://www.en.kfst.dk/media/3304/20131209-executive-summary-of-barriers-to-ppp-in-municipal-and-regional-public-works-contracts.pdf
81. Eckert S.: Protecting Critical Infrastructure: The Role of the Private Sector, dostupno na: https://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf
82. Zalud B.: Transition Times for Bank and Financial Services, *Security Magazin*, June 2015, dostupno na: https://www.securitymagazine.com/articles/86405-transition-times-for-bank-and-financial-services-security

83. Zakon o informacionoj bezbjednosti, "*Službeni list Crne Gore*", br. 014/10, 040/16
84. Zakon o koncesijama „Službeni list Crne Gore", 08/09
85. Zakon o učešću privatnog sektora u obavljanju javnih usluga „Službeni list Crne Gore, br. 30/02 i 73/10
86. Zakon o stranim investicijama *„Službeni list Crne Gore"*, br. 8/11
87. Zakon o javnim nabavkama *„Službeni list Crne Gore"*, br042/11, 057/14, 028/15, 042/17
88. Zakon o prostornom razvoju i izgradnja objekata *„Službeni list Crne Gore"*, br 51/08 i 33/14
89. Zakon o državnoj upravi *„Službeni list Crne Gore"* br. 38/03 i 42/11
90. Zakon o zaštiti lica i imovine, *„Službeni list Crne Gore"*, br. 43/2018
91. Zákon o kritickej infraštruktúre, Zbierka zákonov č. 45/2011, dostupno na: https://www.zakonypreludi.sk/zz/2011-45
92. Zakon o kritičnim infrastrukturama, „Narodne novine" br. 56/13
93. Zakon o kritični infrastrukturi (ZKI), Uradni list RS, št. 75/2017
94. *Public-private partnerships*, International Monetary Fund, 2004
95. InfraGard, доступно на: https://www.infragard.org
96. ISAF's Mission, NATO and Afghanistan, North Atlantic Treaty Organization, dostupno na: www.globalresearch.ca/rendition-and-the-global-war-on-terrorism-28-nations-have-supported-theus-in-the-detention-and-torture-of-suspects/18419
97. Јаковљевић В.: Ресурси критичне инфраструктуре и њихов значај за управљање ванредним ситуацијама, *Зборник радова ФЦО*, Београд, 2010
98. Jomo KS, Chowdhury A., Krishnan S., Platz D.: *Public-Private Partnerships and the 2030 Agenda for Sustainable Development: Fit for purpose?*, Department of Economic & Social Affairs, DESA Working Paper No. 148, 2016
99. Johnson B.R., Ortmeier P. J.: *Introduction to security: operations and management*, Pearson, 2018
100. Joseph J.: Resilience as embedded neoliberalism: A governmentality approach. Resilience, *International Policies, Practices and Discourses*, 1(1), 2013
101. Kaska K.: *National Cyber Security Organisation: the Netherlands*, NATO Cooperative Cyber Defence Centre of Excellence Tallinn, 2015
102. Kačer H., Kružić D., Perković A.: Javno-privatno partnerstvo: atraktivnost DBFOOT modela, *Zbornik radova*, br.3, Pravni fakultet, Split, 2008
103. Кековић З., Савић С., Комазец Н., Милошевић М., Јовановић Д.: *Процена ризика у заштити лица, имовине и пословања*, Центар за анализу ризика и управљање кризама, Београд, 2011
104. Keković Zoran, Kentera Savo: Montenegrin Police: Current Profile and Future Trends, in: Meško G. et al. (eds.): *Handbook on Policing in Central and Eastern Europe*, Springer, New York, 2013
105. Kelley A., Pesch-Cronin N., Marion E.: *Critical infrastructure protection, risk management, and resilience: a policy perspective*, Taylor & Francis Group, 2016
106. Kernaghan K.: Partnerships and public administration: conceptual and practical considerations, *Canadian Public Administration*, Vol. 36, Issue 1, Institute of Public Administration of Canada,1993

107. Klaver M.:*Good practices manual for CIP policies, for policy makers in Europe*, Brussels, 2011, dostupno na: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/FINAL_RECIPE_manual.pdf
108. Klijn H. E., Koppenjan J.: The impact of contract characteristicon the performance of public–private partnerships (PPPs), *Public Money & Management*, 36(6), 2016
109. Kovacich G.L., Halibozek E. P.: *The manager's handbook for corporate security: establishing and managing a successful assets protection program*, Elsevier Science,USA, 2003
110. Komunikaciona strategija – Crna Gora članica NATO-a za period do 2020. godine, Vlada Crne Gore, Podgorica, 2018
111. Konrad S. T.: *Management Control in Public-Private Partnerships, Between International Governmental Actors and the Private Sector*, Springer, 2018
112. Koppenjan J. F. M.: The formation of public–private partnerships: lessons from nine transport infrastructure projects in The Netherlands, *Public Administration,* 83, (1), Blackwell Publishing, Oxford 2005
113. Koselleck et al.: Krise und Kritik. In: Geschichtliche Grundbegriffe, *Historisches Lexikon zur politisch-sozialen Sprache in Deutschland (Vol. 3)*, Klett-Cotta, Stuttgart, 1982
114. Koubatis A., Schönberger J.Y.: *Risk management of complex critical systems', Journal of Critical Infrastructures,* Vol. 1, Nos. 2/3, 2001
115. Khairallah M.: Identifying Control Perimeters, Security Magazin, 2007, dostupno na:https://www.securitymagazine.com/articles/78267-identifying-control-perimeters-1
116. Lazari A.: *European Critical Infrastructure Protection*, Springer, 2014
117. Leese M.: Governing airport security between the market and the public good, *Criminology & Criminal Justice* 16(2), 2016
118. Leese M., Wildi L.: Security Measures at Zurich Airport, *Analyses in Security Policy No 208*, Center for Security Studies, Zurich, 2017
119. Лековић В, Ивановић В.: *Јавно-приватно партнерство у функцији обезбеђења квалитетније инфраструктуре*, Фестивал квалитета, Крагујевац, 2009
120. Lehtinen R., Russell D., Gangemi Sr G.T.: *Computer Security Basics, 2nd Edition*, O'Reilly Media, California, 2006
121. Lewis T.: I*nfrastructure Protection in Homeland Security, Defending a Networked Nation*, Wiley Interscience, 2006
122. Lewis T.: *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation,* Wiley Interscience,New Jersey, 2014
123. Lindemans J..: Vandeburie and Maeyaert, Belgium, The Government Procurement Review, Law Business Research, London, 2016, dostupno na:https://thelawreviews.co.uk//digital_assets/c9be8045-55f1-4902-b275-d2871ba8f8cc/The-Government-Procurement-Review---Edition-7.pdf
124. Link N.A.: *Public/Private Partnerships Innovation Strategies and Policy Alternatives*, Springer, 2006

125. Lopez J., Setola R., Wolthusen D. S.: *Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense,* Springer-Verlag Berlin Heidelberg 2012
126. Lukitsch K., Müller M., Stahlhut C. Criticality in: Engels I., J. (ed.): *Key Concepts for Critical Infrastructure Research,* Springer, Wiesbaden, Germany, 2018
127. Luiijf E., Burger H., Klaver M., Marieke H.:*Critical infrastructure protection in the Netherlands: a Quick-scan,* EICAR Denmark, Copenhagen, 2003
128. Maiolo M., Pantusa D.: Infrastructure Vulnerability Index of drinking water systems to terrorist attacks,Cogent Engineering, Volume 5, Issue 1 2018,pp. 2–3, dostupno na: https://www.cogentoa.com/article/10.1080/23311916.2018.1456710.pdf
129. Marboe J P., Lassner N.: Austria, In: Davey J., Gatenby A.: *The Government Procurement Review*, Law Business Research Ltd, London, 2015
130. Marjanović M., Nađ I.: Assessment of threats to critical infrastructure facilities from serious and organized crime, in: Keković Z., Čaleta D., Kešetović Ž., Jeftić Z.: *National critical infrastructure protection regional perspective*, Faculty of Security Studies, Belgrade, 2013
131. Марјановић М.: Партнерство између приватног и јавног сектора безбедности, у:*Супротстављање савременим облицима криминалитета –анализа стања, европски стандарди и мере за унапређење,Зборник радова*, Криминалистичко-полицијска академија, Београд, 2015
132. *Методологија избора критичне инфраструктуре*, Министарство за информационо друштво и телекомуникације, Подгорица, 2014
133. Meyer C.: Compounding Technologies for More Accurate Intruder Detection, Security Magazin, February 2015, dostupno na:http://digital.bnpmedia.com/publication/?i=244485&article_id=1920048&view=articleBrowser&ver=html5#{%22issue_id%22:244485,%22view%22:%22articleBrowser%22,%22article_id%22:%221920048%22}
134. Mitchell B.: Protecting Your People, Property and Posterior: The Top 11 Errors in Emergency Planning, *Security Magazin*, May 2013, dostupno na: https://www.securitymagazine.com/articles/84368-protecting-your-people-property-and-posterior-the-top-11-errors-in-emergency-planning
135. Milošević M., Petrović P.: Privatising the Security of Critical Infrastructure in Serbia – The Case of Private Security at the Hydropower Plant Djerdap, In: Klopfer F., Nelleke van A: (eds.): *Private Security in Practice: Case studies from Southeast Europe,* DCAF, 2016
136. Мићовић М.: Безбедносни аспекти функционисања критичне инфраструктуре у ванредним ситуацијама, *докторска дисертација*, Факултет безбедности, Београд, 2016
137. *Montenegro-PPP Units and Related Institutional Framework,* European PPP Expertise Centre, 2014
138. Moteff J.,Copeland C.,Fischer J.: *Critical Infrastructures: What Makes an Infrastructure Critical?,*The Library of Congress, Washington, 2003, dostupno na: https://fas.org/irp/crs/RL31556.pdf

139. McConnell A.: Post-Crisis Reform and Learning in the Aftermath of the 1998 Sydney Water Crisis, Report Number: GOV2005-4, School of Economics and Political Science, Sydney University, 2005, dostupno na: http://www.econ.usyd.edu.au/13602.html
140. Nadav M.: *Comparative homeland security : global lessons*, John Wiley & Sons, 2011
141. Nádai L., Padányi J.: *Critical Infrastructure Protection Research*, Springer International Publishing Switzerland 2016
142. Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, Ministerstvo financií, 2008, dostupno na:www.informatizacia.sk/ext_dok-narodna_strategia_pre.../6167c
143. *National Monuments and Icons Sector – Specific Plan: An Annex to the National Infrstructure Protection Plan*, U.S. Department of Homeland Security, 2010, dostupno na: https://www.hsdl.org/?abstract&did=691293
144. *National Risk Profile 2016, An All Hazard overview of potential disasters and threats in the Netherlands, The National Network of Safety and Security Analysts*, National Institute for Public Health and the Environment The Netherlands, 2016
145. National Security Strategy and Strategic Defence and Security Review, UK Government, 2015, dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
146. National strategy for the protection of Switzerland against cyber risks 2018-2022
147. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Ministry of the Interior, Federal Republic of Germany, 2009
148. *National Emergency Plan for the Telecommunications Sector*, доступно на:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61807/emergency-plan-telecomms-sector.pdf
149. *National Maritime Security Strategy, 2013*, dostupno na: https://www.lamoncloa.gob.es/documents/20131333estrategiadeseguridadmartima_ingls.pdf
150. Nacional Cyber Security Centre, *What is a WARP*, доступно на:https://www.ncsc.gov.uk/information/what-warp
151. Недељковић С., Форца Б.: Европска стратегија безбедности и сајбер претње-значај за Србију, *Војно дело, бр. 3*, МЦ Одбрана, Београд, 2015
152. Nemeth C.P. : *Private Security and the Law*, Elsevier, USA, 2012
153. Nemeth P. C.: *Private Security An Introduction to Principles and Practice*, Boca Raton, 2017
154. Nemeth P. C.: *Private Security, An Introduction to Principles and Practice, CRC Press*, Taylor & Francis Group, 2018
155. New Zealand's Cyber Security Strategy, Department of the Prime Minister and Cabinet, 2019, dostupno na: https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf
156. Niskanen A. W.: The soft infrastructure of a Market, CATO Journal, In: Gotbaum R: The Difference Between Soft And Hard Infrastructure, And Why It Matters, *State Impact Magazine*, New Hampshire, 2011

157. No free Lunch: Agribusiness and Risks to Food Security, dostupno na: http://www.preventionweb.net/english/hyogo/gar/2013/en/gar-pdf/chap10.pdf
158. Kešetović Ž.*: Krizni menadžment*, Fakultet bezbjednosti, Beograd, 2008
159. Odluka o obrazovanju savjeta za informacionu bezbjednost, „Službeni list Crne Gore“, br. 48/17
160. Odluka o određivanju velikih tehničkih sistema od značaja za odbranu, „*Službeni list Crne Gore*“, br. 15/08
161. *Online Etymology Dictionary, Douglas Harper, Historian*, The Etymology of Infrastructure: http://dictionary.reference.com/browse/infrastructure
162. *Optimization of Resourcesfor Mitigating Infrastructure Disruptions Study, Final Report and Recommendations by the Council*, National Infrastructure Advisory Council, 2010, dostupno na: https://www.dhs.gov/sites/default/files/publications/niac-optimization-resources-final-report-10-19-10-508.pdf
163. *Operational Requirements, Principles of assessing and implementing effective protective security*, Centre for the Protection of National Infrastructures, 2018
164. Oregon Health Authority, *Physical Security for Drinking Water Facilities*, 2009, dostupno na: https://public.health.oregon.gov/HealthyEnvironments/DrinkingWater/Preparedness/Documents/PhysicalSecurity-Oregon.pdf
165. Ortmeier J. P.:*Introduction to Security, 3rd ed*., Prentice Hall, 2009
166. Ouyang M.: Review on modeling and simulation of interdependent critical infrastructure systems,*Reliability Engineering & System Safety*, Volume 121, 2014
167. *Federal Emergency Management Agency, Critical Asset Risk Management, Participant Guide*, Office of Homeland Security, 2014
168. Pagano A., Pluchinotta I., Giordano R., Fratino U.: Integrating “Hard” and “Soft” Infrastructural Resilience, Assessment for Water Distribution Systems, Complexity, vol. 2018, Article ID 3074791, dostupno na: https://www.hindawi.com/journals/complexity/2018/3074791/
169. Paolino R.C.: All Aboard: Making the Case for a Comprehensive Rerouting Policy to Reduce the Vulnerability of Hazardous Rail-Cargoes to Terrorist Attack, *Military Law Review, Volume 193,* Department of Army Pamphlet, 2007
170. *Partners for Amtrak Safety and Security*, Protecting America's Railroad, доступно на: https://pass.amtrak.com/resources.html
171. Pekich J.:What How to Plan for Post-Incident “Golden Minutes”, *Security Magazin,* November 2013, доступно на:https://www.securitymagazine.com/articles/84887-how-to-plan-for-post-incident-golden-minutes
172. Persoli M.A.: Javno-privatno partnerstvo u funkciji zadovoljavanja javnih potreba, *Hrvatska javna uprava*, br.4, Pravni fakultet, Zagreb, 2010
173. Pesch-Cronin A. K., Marion E. N.: *Critical infrastructure protection, risk management, and resilience: a policy perspective*, Taylor & Francis Group, 2016
174. Petersen H.O.: Regulation of public–private, partnerships: the Danish case, Public Money & Management, Vol. 30, Issue.3, 2010

175. Petrakos N., Kotzanikolaoup P.:Methodologies and Strategies for Critical Infrastructure Protection In: Gritzalis D., Theocharidou M., StergiopoulosG. (ed): *Critical Infrastructure Security and Resilience, Theories, Methods, Tools and Technologies*, Springer, Switzerland, 2019
176. Plumer J.:*Focusing Partnership: A Sourcebook. for Municipal Capacity Building in Public - Private Partnership*, Earthscan, London, 2002
177. *PPPs financed by the European Investment Bank from 1990 to 2018*, European Investment Bank, 2019
178. *Port Authority Warns TSA It Will Be Replaced By Private Security Force Over Long Lines At Airports*, New York CBS, dostupno na: http://newyork.cbslocal.com/2016/05/09/tsa-port-authority-airports/
179. *Police and Justice Act 2006*, dostupno na: http://www.legislation.gov.uk/ukpga/2006/48/contents
180. Pravilnik o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave, dostupno na: http://www.mju.gov.me/organizacija
181. Predlog Zakona o javno-privatnom partnerstvu, dostupno na: https://www.paragraf.me/nacrti_i_predlozi/predlog-zakona-o-javno-privatnom-partnerstvu.pdf
182. Prenzler T., Sarre, R. Public-private crime prevention partnerships. In: Prenzler T.: *Policing and security in practice: challenges and achievements*, Palgrave Macmillan UK, 2012
183. Project Argus, City of London Police, dostupno na: https://www.cityoflondon.police.uk/advice-and-support/countering-terrorism/Pages/project-argus.aspx
184. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILconcerning measures to ensure a high common level of network and information security across the Union, Brussels, 7.2.2013COM(2013) 48 final, dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN
185. *Public-private partnership analysis, Network for Affirmation of NGO Sector*, Balkan monitoring public finances, 2017
186. *Public-Private Partnerships A Basic Introduction for Non-Specialists*, Economics and Private Sector Professional Evidence and Applied Knowledge Services UK, 2017
187. *Public-Private Partnerships*, Prepared by the Fiscal Affairs Department International monetary fund, 2014, dostupno na: https://www.imf.org/external/np/fad/2004/pifp/eng/031204.pdf
188. *Public Private Partnerships in the EU: Widespread shortcomings and limited benefits*, European court of auditors, 2018
189. Public-private partnerships in Montenegro, Institute Alternative, 2010, dostupno na: http://www.institut-alternativa.org/wp-content/uploads/2009/05/jpp-eng.pdf
190. Purser S.: Standards for Cyber Security, In: Hathaway E. M. (ed.*): Best Practices in Computer Network Defense: Incident Detection and Response*, IOS Press, 2014

191. Pursiainen C., Gattinesi P.: Towards Testing Critical Infrastructure Resilience, Publications Office of the European Union, JRC Scientific and Policy Reports, Luxembourg, 2014, dostupno na:https://core.ac.uk/download/pdf/38627770.pdf
192. Radvanovsky R., McDougall A.:*Critical Infrastructure*, Boca Raton, FL: CRC Press, 2013
193. Review the Sector Coordinating Council for Energy, dostupno na: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf
194. *Report: Maintenance of Prison Facilities in Public-Private Partnership - Monitoring by the Public Building Authority (Régie des bâtiments) and the Ministry of Justice'* (21 November, 2018), dostupno na: https://www.ccrek.be/EN/Publications/Fiche.html?id=2847611e-cb6b-4b04-b897-136cfe1baf48
195. Republic of Slovenia's, Ministry of defence, dostupno na: http://www.mo.gov.si/en/areas_of_work/critical_infrastructure/
196. Resilient critical infrastructure, National Coordinator for Security and Counterterrorism Ministry of Justice and Security, dostupno na:https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf
197. Rendiero J.: Threat Analysis and Ratings for Overseas Security, *Security Magazin*, January 2013, dostupno na:https://www.securitymagazine.com/articles/83892-threat-analysis-and-ratings-for-overseas-security
198. Rehak D., Markuci J., Hromada M., Barcova K.: Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system, *International Journal of Critical Infrastructure Protection*, 14, 2016
199. *Rządowego Centrum Bezpieczeństwa*, Warszawa, dostupno na: https://rcb.gov.pl/en/critical-infrastructure/
200. Ridley G.: National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience, *Journal of Business Ethics*, vol. 103, no. 1, 2011
201. Rinaldi S.M.: Modeling and simulating critical infrastructures and their interdependencies, *37th Hawaii International Conference on System Sciences*, 2004. dostupno na: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.1206&rep=rep1&type=pdf
202. Rinaldi S. M., Peerenboom J. P., Kelly T. K.: Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems Magazine*, 21(6), 2001, dostupno na: https://pdfs.semanticscholar.org/b1b7/d1e0bb39badc3592373427840a4039d9717d.pdf
203. Roberts M.: Keeping Mass Transit Ahead of the Curve, *Security Management, ASIS International*, November 2005
204. Role of Critical Infrastructure in National Prosperity, Shared Narrative, Government of Canada, 2015, dostupno на: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-rl-crtclnfrstrctr-ntnlprsprty/index-en.aspx

205. Rudy J.: Fire Protection: A Complete Approach, *Occupational Healt & Safety*, December 2012, dostupno na: http://ohsonline.com/Articles/2012/12/01/Fire-Protection-A-Complete-Approach.aspx
206. Sarsengali A. et all: Development of Public-Private Partnership in the Republic of Kazakhstan, *IEJME—Mathematics education* , Vol. 11, No. 5, 2016
207. Sventekova E., Leiitner B., Dvorak Z.: Transport Critical Infrastructure in Slovak Republic, Proceedings of The 8th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2017), dostupno na :http://www.iiis.org/CDs2017/CD2017Spring/papers/ZA357XP.pdf
208. Setola R., Luiijf E., Theocharidou M.: Critical Infrastructures, Protection and Resilience, in: Setola R., Rosato V., Kyriakides E., Rome E. (ed): *Managing the Complexity of Critical Infrastructures, A Modelling and Simulation Approach*, Springer, Switzerland, 2016
209. Sector Coordinating Councils, Department of Homeland Security, dostupno na:https://www.dhs.gov/cisa/sector-coordinating-councils
210. Securitas International, Case Study: Sound Transit, Western Washington State, dostupno na:http://www.securitasinc.com/globalassets/us/files/casestudies/updated-case-studies/case-study---sound-transit.pdf
211. *Sklep o določitvi nosilcev sektorjev kritične infrastrukture Republike Slovenije in z njimi sodelujočih državnih organov*, Vlada Republike Slovrenije, št. 80200-1/2018/, dostupno na: http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/zki/SprejetoBesediloAkta_Nosilci_sektorjev_KI.pdf
212. Smedts B.: *NATO's Critical Infrastructure Protection and Cyber Defense*, Royal High Institutefor Defense Center for Security and Defense Studies, Brussels, 2010
213. Smith A.: *Privatized Infrastructure: The Role of Government*, Thomas Telford, 1999
214. Smith F. C., Schmalleger F.,Siegel J. L.: *Private Security Today*, Pearson Education, 2017
215. Solms von R., Niekerk van J.: From information security to cyber security, *Computers & Security,Vol 38*, International Federation for Information Processing, 2013
216. *South Eastern Europe Disaster Risk Mitigation and Adaptation Initiative, Risk Assessment for South Eastern Europe Desk Study Review*, United Nations, Geneva, 2008
217. South Eastern Europe Clearinghouse for the Control of SmallArms and Light Weapons. SALW and privatesecurity companies in South Eastern Europe: A cause oreffect of insecurity? 2005, dostupno na: http://www.seesac.org/uploads/studyrep/SALW_i_firme_za_privatno_obezbedjenje_u_jugoistocnoj_Evropi.pdf
218. Spanish Ministry of the Interior, The National Center for Infrastructure Protection and Cybersecurity (CNPIC), dostupno na: http://www.cnpic.es/en/Preguntas_Frecuentes/Que_es_una_Infraestructura_Critica/index.html

219. Spencer I.: *Mass Transit Security Market on Track for Big Growth*, Security Systems News January 2015
220. Средојевић С.: *Јавно-приватно партнерство*, Архипелаг & Институт економских наука, Београд, 2010
221. Стакић Б., Васић Д., Ћурковић В.: *Улагање капитала путем јавно-приватног партнерства и концесија*, Факултет за пословне студије и право, Београд, 2015
222. Staković Lj., Cvetanović S.: Javno privatna partnerstva – faktor unapređenja konkurentske prednosti, *Ekonomika preduzeća*, br. 3-4, Savez ekonomista Srbije, Beograd, 2011
223. *State Regulation concerningCivilian Private Security Servicesand their Contribution to Crime Preventionand Community Safety*, United Nations Office on Drugs and Crime (UNODC), Vienna, 2014
224. Stevanović O.: *Bezbednosni menađment*, Kriminalističko-policijska akademija, Beograd, 2012
225. Stevens G. M., Tatelman, T. B.: Protection of Security-Related Information, *Congressional Research Service*, September 27, 2006, dostupno na :http://fas.org/sgp/crs/secrecy/RL33670.pdf
226. Stanghellini S., Copiello S.: Urban Models in Italy: Partnership Forms, Territorial Contexts, Tools, Results, in: Dalla Longa R.(ed.): *Urban Models and Public-Private Partnership,* Springer, Heidelberg-Dordrecht-London-New York, 2011
227. Strategija nacionalne bezbjednosti Crne Gore, „*Službeni list Crne Gore*“, br. 085/18
228. Strategija nacionalne sigurnosti Republike Hrvatske, „*Narodne novine*“, br.73/2017
229. *Study on the development of statistical data on the European security technological andindustrial base*, Security Sector Survey Analysis: Spain, Ecorys, The Netherlands, 2015, dostupno na: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/reference-documents/docs/final_security_survey_descriptive_analysis_es_en.pdf
230. Sullivant J.: *Strategies for Protecting National Critical Infrastructure Assets A Focus on Problem-Solving*, John Wiley & Sons, Inc., Publication, New Jersey, 2007
231. Schaap L., Leenknegt G.J.: *Decentralised autonomy?, Report in preparation for the study by the Council of Europe into the state of sub-national selfgovernment in the Netherlands*, DEMOS – Centre for Better Governance and Citizenship, University of Tilburg, Tilburg, 2014
232. Schallbruch M., Skierka I.: *Cybersecurity in Germany*, Springer Briefs, 2018
233. Schaffhauser-Linzatti M.: Risk menagement in an Austrian standardised public-private partnership model, in: Akintoye A., Beck M., Hardcastle C.: *Public-private partnerships, managing risk and opportunities*, Blackwell Science, 2003
234. Schneider J.: *Public Private Partnerships for Urban Rail Transit*, Deutscher Universitats-Verlag, Wiesbaden 2004
235. Swapnil G., Sachin G.: Rethinking Public-private Partnerships: An Unbundling Approach, *Transportation Research Procedia 25*, 2017

236. Taylor A.B.: *The Evolution of Airline Security Since 9/11*, dostupno na:http://www.ifpo.org/resource-links/articles-and-reports/protection-of-specific-environments/the-evolution-of-airline-security-since-911/
237. Tvarnø D. C.: Legal, Financial and Governmental PPP Initiatives, *Fifth International PPP conference in Antwerp*, 2016, dostupno na: https://openarchive.cbs.dk/bitstream/handle/10398/9387/2016%20tvarno%20legal%20financiel%20and%20governmental%20PPP%20initiatives.pdf?sequence=1
238. Telecommunications (Fraud) Act 1997, dostupno na: http://www.legislation.gov.uk/ukpga/1997/4/contents
239. *Terrorism Act 2000*, dostupno na: http://www.legislation.gov.uk/ukpga/2000/11/contents
240. Трбојевић М.: Заштита критичних инфраструктура-искуства транзиционих земаља, *Политичка ревија*, бр. 2, Београд, 2018
241. Trivan D.: *Korporativna bezbjednost*, Dosije, Beograd, 2012
242. Trivan D., Radović V.: Corporate security role in protecting critical infrastructure, In: Keković Z., at all (ed.): *National critical infrastructure protection, regional perspective*,Faculty of Security Studies, Belgrade, 2013
243. *The EIB role in Public-Private Partnerships*, European Investment Bank, Luxembourg, 2004
244. *The National CyberSecurity Agenda*, Ministry of Justice and Security, 2018, dostupno na:https://www.enisa.europa.eu/news/member-states/new-national-cyber-security-agenda-published-by-the-netherlands
245. *The protection of critical infrastructure against terrorist attacks: Compendium ofgood practices*, UN Office Counter-Terrorism, UN Counter-Terrorism Centre, 2018
246. *The Review of the European Programmefor Critical Infrastructure Protection(EPCIP)*, Commission Staff Working Document,SWD(2012) 190 final. Commission of theEuropean Communities, EuropeanCommission, Brussels, 2012, dostupno na: http://ccpic.mai.gov.ro/docs/epcip_swd_2012_190_final.pdf
247. *The Critical Infrastructure Protection in France. Secrétariat général de la défense et de la sécurité nationale (SGDSN)*, Retrieved from Secrétariat général de la défense et de la sécurité nationale, Paris, 2017, dostupno na: http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf
248. *National Security Strategy*, The White House, Washington, DC 2017, dostupno na https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
249. Thomson C., Goodwin J.: *Evaluation of PPP projects Financed by the EIB*, European Investment Bank, 2005
250. *National Emergency Plan for the Telecommunications Sector*, UK Department of Business Innovation and Skills, dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61807/emergency-plan-telecomms-sector.pdf
251. U.S. Environmental Protection Agency, Information about Public Water Systems, dostupno na: http://www.epa.gov/dwreginfo/information-about-public-water-systems

252. *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, U.S. Government Accountability Office 2015, dostupno na: http://www.gao.gov/assets/680/673779.pdf
253. Pre-Harvest Security Guidelines and Checklist, Government Printing Office, U.S. Department of Agriculture Washington, DC: U.S., 2006, dostupno na: http://www.usda.gov/documents/PreHarvestSecurity_final.pdf
254. Federal Emergency Management Agency- Grants, dostupno na:https://www.fema.gov/grants
255. Federal Office of Civil Protection and Disaster Assistance (BBK), dostupno na:https://www.bbk.bund.de/EN/Home/home_node.html
256. *Financing PPPs with project bonds, Issues for public procuring authorities*, The European PPP Expertise Centre, 2012
257. Fusion Centers, Department of Homeland Security, dostupno na: https://www.dhs.gov/fusion-centers
258. Halibozek E., Jones A., Kovacich L. G.: *The corporate security professional's handbook on terrorism*, ElsevierIn, 2008
259. Hämmerli B.: *Protecting critical infrastructure in the EU*, Task Force Report, Centre for European Policy Studies, Brussels, 2010
260. Hamerl T.: Austria, In: Ivan Mattei E. I., Rivera J. A.: *Public-Private Partnerships* Law Business Research Ltd, London, 2015
261. Hemme K.:Critical Infrastructure Protection: Maintenance is National Security, *Journal of Strategic Security*, Number 5 Volume 8, 2015, dostupno na:https://scholarcommons.usf.edu/jss/vol8/iss5/3/?utm_source=scholarcommons.usf.edu%2Fjss%2Fvol8%2Fiss5%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages
262. Hess M. K.: *Introduction to Private Security, Fifth Edition*, Wadsworth, Cengage Learning, 2009
263. Högselius P. et al. :*The Making of Europe's Critical Infrastructure: Common Connections and Shared Vulnerabilities*, Houndmills, Basingstoke, Palgrave Macmillan, 2013, dostupno na: https://www.researchgate.net/publication/262684604_The_Making_of_Europe's_Critical_Infrastructure_Shared_Connections_and_Common_Vulnerabilities
264. Hodge G., Greve C.: *The Challenge of Public–Private Partnerships, Learning from International Experience*,Edward Elgar Publishing, UK, 2005
265. Hodgson K.: *SIA Update* (Oct. 14, 2011), dostupno na:http://www.securityinfowatch.com/article/10506940/sia-update
266. Howar P.:*Howard Safe Cities Project. Hard WonLessons:HowPolice Fight Terrorism in the United Kingdom*, Manhattan Institute for Policy Research, New York, 2004
267. Hriciková L., Kaska K.: *National Cyber Security Organisation: Slovakia*, NATO Cooperative Cyber Defence Centre of Excellence the Centre Tallinn 2015
268. Carr M.: Public–private partnerships in national cyber-security strategies, *International Affairs, 92(1)*,2016

269. Carter Smith F.C., Schmalleger F., Siegel J. L.: *Private Security Today*, Pearson Education, Inc, 2017
270. Cartlidge D.: *Public Private Partnerships in Construction*, Taylor & Francis, New York, 2006
271. Castellon N., Frinking E.: *Securing Critical Infrastructures in the Netherlands: Towards a National Testbe*, Hague 2015
272. *Center for the Protection of National Infrastructure, What We Do*, dostupno na:http://www.cpni.gov.uk/About/whatWeDo.aspx
273. *Civil Contingencies Act 2004: a shortguide*, Civil Contingencies Secretariat, dostupno na:https://www.cambridge.gov.uk/media/1253/cca-short-guide.pdf
274. Cvetković P., Sredojević S.: *Javno-privatno partnerstvo, priručnik za sprovođenje na nivou lokalne samouprave*, Stalna konferencija gradova i opština, Beograd, 2013
275. Ciaramella C.J.: Abolish the TSA, *The Washington Post (April 16, 2015)*, dostupno na: https://www.washingtonpost.com/posteverything/wp/2015/04/16/abolish-the-tsa/
276. *Climate Change and Hungary: Mitigating the hazard and preparing for the impacts*, The "Vahava" report, Budapest, 2010
277. Collier S.J., Lakoff A.ndrew: Distributed Preparedness: The Spatial Logic of Domestic Security in the United States. In: *Environment and Planning D: Society and Space*, 26 (1), 2008
278. Green Paper on PPPs and Community Law on Public Contracts and Concessions COM (2004)
279. Cordesman A. H., Cordesman J. G.:*Cyber-Threats, Information Warfare, and Critical Infrastructure Protectio*, Defending the U.S. Homeland. Westport, CT: Praeger, 2002
280. Cooperative models for effective public private partnerships, Desktop ResearchReport, ENISA. 2011, dostupno na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships/at_download/fullReport
281. COUNCIL DIRECTIVE 2008/114/EC,The identification and designation of European critical infrastructures and the assessment of the need to improve their protection, доступно на: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
282. *Critical Information Infrastructures Protection approaches in EU*, dostupno na: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf
283. *Critical Information Infrastructures Protection approaches in EU*, European Union agency for cybersecurity, 2015
284. *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, U.S. Government Accountability Office, 2015, dostupno na: http://www.gao.gov/assets/680/673779.pdf
285. Critchley T. A.: *History of Police in England and Wales*, 2nd edition, Legend, 1978

286. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013 JOIN(2013) 1 final, dostupno na: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
287. Cybersecurity: the Government's strategy, Government France, dostupno na: https://www.gouvernement.fr/en/cybersecurity-the-government-s-strategy
288. *Cyber Security Concept of the Slovak Republic for 2015 – 2020*
289. Cyber-Sicherheitsstrategie für Deutschland 2016, dostupno na: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html
290. Choate P., Walter S.: *America in Ruins: The Decaying Infrastructure*, Duke Press Policy Studies, New York, 1981
291. Christopher K.: *Port Security Management*, Second Edition, Taylor & Francis Group, 2015
292. Quingbin C., Lindly J: *Evaluation of Public Private Partnership Proposals*, University Transportation Center for Alabama, 2010
293. Weihe G., at all: *Strategic use of public-private cooperation in the Nordic region, Nordic Council of Ministers*, Copenhagen, 2011
294. Weihe G. : *Public–Private Partnerships: Meaning and Practice*, Copenhagen Business School, 2009
295. Why should governments turn to the private sector to help perform services they have traditionally handled themselves? NCPP: FAQs -, dostupno na: http://www.ncppp.org/ppp-basics/frequently-asked-questions /
296. Willems Tom, Verhoest K., at all: Ten Lessons from Ten Years PPP Experiencein Belgium, *Australian Journal of Public Administration*, Vol. 76, No. 3, Institute of Public Administration Australia, 2016
297. Williams J: Physical Security: Thret after september 11, 2001, In:Tripton F. H., Krause M.: *Information Security Management Handbook*, Taylor &Francis Group, 2007
298. The Clinton's Administration's Policy on critical infrastructure protection: presidential decision directive 63/PDD-63, White paper, White House 22 May 1998, dostupno na: http://fas.org/irp/offdocs/pdd/pdd-63.html
299. Yescombe R. E.: *Public–Private Partnerships, Principles of Policy and Finance*, Butterworth-Heinemann is an imprint of Elsevier, Oxford, 2007
300. Yescombe R. E., Farquharson E.: *Public-private partnerships for infrastructure, principles of policy and finance*, Butterworth-Heinemann, Oxford, 2018

PRILOG

Anketni upitnik

UVODNE NAPOMENE

Popunjavanjem ovog upitnika Vi doprinosite ostvarenju ciljeva naučnog istraživanja kojim se nastoji da se prikupe mišljenja i stavovi u vezi primjene javno-privatnog partnerstva u zaštiti kritične infrastrukture u Crnoj Gori. Istraživanje je anonimno što znači da ne treba potpisivati upitnik. Podaci prikupljeni iz ovog upitnika biće korišćeni isključivo za naučne analize i dostupni samo istraživačima angažovanim na ovom projektu. Izvinjavamo se ako su neka pitanja suviše jednostavna ili teška, ali u ispunjavanju ovog upitnika nema neispravnog odgovora, jer su svi odgovori tačni.

Molimo Vas da na pitanja odgovorite prema svom iskustvu i najdubljem uvjerenju. Od Vas se očekuje da na osnovu vašeg iskustva i saznanja, obilježavanjem jedne od više ponuđenih mogućnosti date odgovore na postavljena pitanja.

VAŠI OPŠTI PODACI

1. Godine strarosti i polna pripadnost

Godine starosti			pol	
do 35	od 36 do 45	preko 45	M	Ž

2. Nivo stečenog obrazovanja

Stepen obrazovanja				
Srednja stručna sprema	Viša stručna sprema	Visoka stručna sprema	Magistar/ Master	Doktor nauka

3. Naziv institucije (organizacije) u kojoj ste zaposleni

Naziv institucije	

4. Koja je vaša oblast stručnog angažovanja i koje poslove obavljate (ukratko)?

2. KRITIČNA INFRASTRUKTURA

5. Šta Vi podrazumijevate pod pojmom kritična infrastruktura?

	sredstvo, sistem ili njegov dio koji se nalazi u državama članicama koji je neophodan za održavanje vitalnih društvenih funkcija, zdravlje, bezbjednost, sigurnost, ekonomsko ili socijalno blagostanje ljudi, kao i narušavanje ili uništenje koje bi imalo značajan uticaj na državu
	sistemi i sredstva bilo fizički ili virtuelni koji su od vitalnog značaja za državu i njihova nesposobnost ili uništenje može imati uticaj na bezbjednost, ekonomsku sigurnost, javno zdravlje ili bilo koju kombinaciju ovih stvari.
	organizacije i ustanove od velikog značaja za zajednicu, čiji neuspjeh ili oštećenje može izazvati trajan nedostatak zaliha, velike poremećaje u javnom redu i druge dramatične posledice.
Vaše mišljenje	

6. Koliko godina se bavite poslovima vezanim za kritičnu infrastrukturu ?

do 5 godina	od 5 do 10	od10 do 20	od 20 do 30	preko30

7. Koliki je značaj kritične infrastrukture za funkcionisanje države i društva?

nema značaj	mali značaj	veliki značaj	veoma veliki značaj	ne mogu da ocijenim

8. Koliki je značaj vaše organizacije za funkcionisanje države i društva ?

nema značaj	mali značaj	veliki značaj	veoma veliki značaj	ne mogu da ocijenim

9. Da li je u Crnoj Gori potrebno donošenje posebnog zakona iz oblasti zaštite kritične infrastrukture regulisana?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

10. Da li je postojeća zakonska regulativa zaštite kritične infrastrukture usklađena sa savremenim oblicima ugrožavanja (terorizam, organizovani kriminal) vaše organizacije?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

11. Koja su tri najvažnija potencijalna rizika koja mogu dovesti do vanredne situacije u vašoj organizaciji ?

1.	2.	3.

12. Koliki je stepen opasnosti od prirodnih i tehničko-tehnoloških rizika u vašoj sredini ?

nizak	srednji	visok	veoma visok	ne mogu da ocijenim

13.Koja su tri objekta kritične infrastrukture u Crnoj Goripo vašem mišljenju najviše izloženi potencijalnim terorističkim napadima?

14. Da li je potpuni državni nadzor jedino adekvatno rešenje u zaštiti kritične infrastrukture ?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

3. PRIVATNI SEKTOR BEZBJEDNOSTI KAO JAVNO PRIVATNO PARTNERSTVO

15. Šta Vi podrazumijevate pod pojmom javno-privatno partnerstvo?

	zajedničko (kooperativno) djelovanje države s privatnim kompanijama u proizvodnji javnih proizvoda ili pružanju usluga
	korporativno udruživanje između javnog i privatnog sektora zasnovano na ekspertizi svakog od partnera koje na najbolji način služi jasno definisanim javnim potrebama kroz odgovarajuću alokaciju resursa, podjelu rizika i dobiti
	investicioni projekti transferisani privatnom sektoru koje je tradicionalno izvršavao ili finansirao javni sektor
vaše mišljenje	

16. Da li postojeći propisi adekvatno uređuju oblast javno-privatnog partnerstva u Crnoj Gori?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

17. Da li je u Crnoj Gori potrebno donošenje posebnog zakona o javno-privatnom partnerstvu?

da	ne	ne mogu da ocijenim

18. Da li je model javno-privatnog partnerstva primenljiv u zaštiti kritične infrastrukture Crne Gore?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

19. Da li je model javno-privatnog partnerstva primenljiv u vašoj organizaciji ?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

20. Da li privatnom sektoru bezbjednosti treba zakonom omogućiti investiranje u zaštitu kritične infrastrukture u Crne Gori?

da	ne	ne mogu da ocijenim

21. Da li postojeći subjekti privatnog sektora bezbjednosti u Crnoj Gori posjeduju kapacitete za zaštitu kritične infrastrukture?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

22. Da li postojeći subjekti privatnog sektora bezbjednosti u Crnoj Gori posjeduju kapacitete za zaštitu vaše organizacije

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

23. Da li je Zakon o zaštiti lica i imovine dovoljan normativni okvir za angažovanje privatnog sektora bezbjednosti u zaštitu kritične infrastrukture u Crnoj Gori?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

24. Da li privatni sektor bezbjednosti u Crnoj Gori doprinosi povećanju opšte bezbjednosti?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

25. Da li bi angažovanjem privatnog sektora bezbjednosti bio povećan stepen zaštite kritične infrastrukture Crne Gore?

ne	djelimično (nepotpuno)	da	ne mogu da ocijenim

HVALA NA SARADNJI!