DOI: 10.5937/vojdelo1503192S

ZAŠTITA KRITIČNE INFRASTRUKTURE I OSNOVNI ELEMENTI USKLAĐIVANJA SA DIREKTIVOM SAVETA EVROPE 2008/114/ES

Mirko Škero
Bezbedno-informativna agencija
Vladimir Ateljević
Vlada Republike Srbije, Kancelarija za evropske integracije

Kompleksnost kriznih i vanrednih situacija, posebno činjenica da se njihovom pojavom ugrožavaju kritični kapaciteti koji su suštinski u redovnom procesu funkcionisanja društva, navele su većinu država da razviju različite aktivnosti i mere njihove zaštite. U tom smislu, Republika Srbija bi u toku procesa pridruživanja EU trebalo da usvoji zakon o kritičnim infrastrukturama koji će biti usklađen sa elementima Direktive 2008/114/ES.

Ključne reči: *Evropska unija, kritična infrastruktura, Direktiva Saveta Evrope 2008/114/ES*

Pojmovno određivanje kritične infrastrukture

Potreba dinamičkog, proaktivnog i strateškog pristupa naročito je neophodna u procesu planiranja zaštite kritične infrastrukture u uslovima različitih tipova kriznih i vanrednih situacija. Pre nego je sintagma „kritična infrastruktura " postala izuzetan predmet interesovanja u brojnim analizama koje su se odnosile na terorizam i unutrašnju bezbednost, pojam „infrastruktura" osamdesetih godina bio je referentna tačka kreatora javne politike i bezbednosti.

Naime, zbog sve većeg rizika povredljivosti i isključivanja iz redovnog funkcionisanja bilo je potrebno, za svaki sistem pojedinačno, predvideti odgovarajuće mere. Infrastruktura se posmatrala kao logistička funkcija kojom se obezbeđuju povoljni uslovi za kvalitetno obavljanje drugih funkcija logističke podrške. Porastom opasnosti od asimetričnih pretnji, naročito terorizma, u savremenim teorijskim analizama, ali i u praksi, sve je prisutniji izraz „kritična infrastruktura". Neposredno nakon terorističkih napada od septembra 2001. godine, kritična infrastruktura postala je bitan i suštinski deo nacionalne bezbednosti, a njena zaštita predstavlja jedan od prioriteta svake države.

Postoji više definicija kritične infrastrukture, ali se sve one, u principu, odnose na sredstva i imovinu, koja je ključna za neometano funkcionisanje ekonomije i društva. Kao primer navodimo nekoliko definicija.

Sjedinjene Američke Države: „Kritična infrastruktura i osnovni resursi je pojam koji se odnosi na širok opseg različitih sredstava i imovine koji su neophodni za svakodnevno funkcionisanje društvenih, ekonomskih, političkih i kulturnih sistema u Sjedinjenim Ame-

ričkim Državama (SAD). Bilo kakav prekid u elementima kritične infrastrukture predstavlja ozbiljnu pretnju za pravilno funkcionisanje ovih sistema i može dovesti do oštećenja imovine, ljudskih žrtava i značajnih ekonomskih gubitaka"[1].

Australija: „Kritična infrastruktura predstavlja one fizičke objekte, lance snabdevanja, informacione tehnologije i komunikacione mreže, koje bi ako se unište ili na duže vreme onesposobe, mogle značajno uticati na društveno ili ekonomsko blagostanje nacije, ili bi uticale na sposobnost Australije da održi nacionalnu odbranu i obezbedi nacionalnu sigurnost"[2].

Evropska Unija: „Kritična infrastruktura predstavlja imovinu, sistem ili njegov deo koji se nalazi na teritoriji zemlje članice i koji je neophodan za održavanje ključnih društvenih funkcija, zdravstva, bezbednosti, sigurnosti, ekonomskog ili socijalnog blagostanja, a čije bi ometanje ili uništenje imalo značajan uticaj na zemlju članicu".

Evropska Unija: „Evropska kritična infrastruktura – EKI, podrazumeva kritičnu infrastrukturu lociranu na teritoriji zemlje članice, čije bi ometanje ili uništenje imalo značajan uticaj na bar dve zemlje članice. Značaj poremećaja u funkcionisanju elemenata kritične infrastrukture treba da se proceni na osnovu kriterijuma međuzavisnosti. To podrazumeva efekte nastale kao rezultat međusektorske zavisnosti od drugih tipova infrastrukture"[3].

Generalno, definisanje okvira kritične infrastrukture u mnogim zemljama je različito i zavisi od raznih specifičnosti, počevši od političkih prilika do geografskih lokacija. Za lakše sagledavanje područja ovog pojma pregledno su dati okviri za nekoliko zemalja u tabeli 1.

Tabela 1 – *Kritična infrastruktura različitih zemalja sveta*

KANADA	VELIKA BRITANIJA	SAD	NEMAČKA	NORVEŠKA	ŠVAJCARSKA
ENERGIJA (objekti električne i nuklearne energije, prirodni plin i nafta, proizvodni i transportni sistemi)	**ENERGIJA**	**ENERGIJA**	**ENERGIJA** (električna, nafta i plin)	**ENERGIJA I OBJEKTI**	**OBJEKTI I SLUŽBE**
KOMUNIKACIJE	**TELEKOMUNIK.**	**INFORMACIJE I TELEKOMUNIK.**	**TELEKOMUNIK. I INFORMACIONA INFRASTRUKTURA**	**SNABDEVANjE NAFTOM I PLINOM**	**TELEKOMUNIK.**
SERVISI (finansije, distribucija hrane, javno zdravstvo)	**ZDRAVSTVENE SLUŽBE**	**JAVNO ZDRAVSTVO**	**JAVNO ZDRAVSTVO** (uključujući i snabdevanje pitkom vodom i hranom)	**TELEKOMUNIK.**	**DISTRIBUCIJA INFORMACIJA**

[1] T.G.A.T. Murray, „Critical Infrastructure protection; The vulnerability conudrun" Telematics and Informatics, vol. 29, no. 1, February 2012.

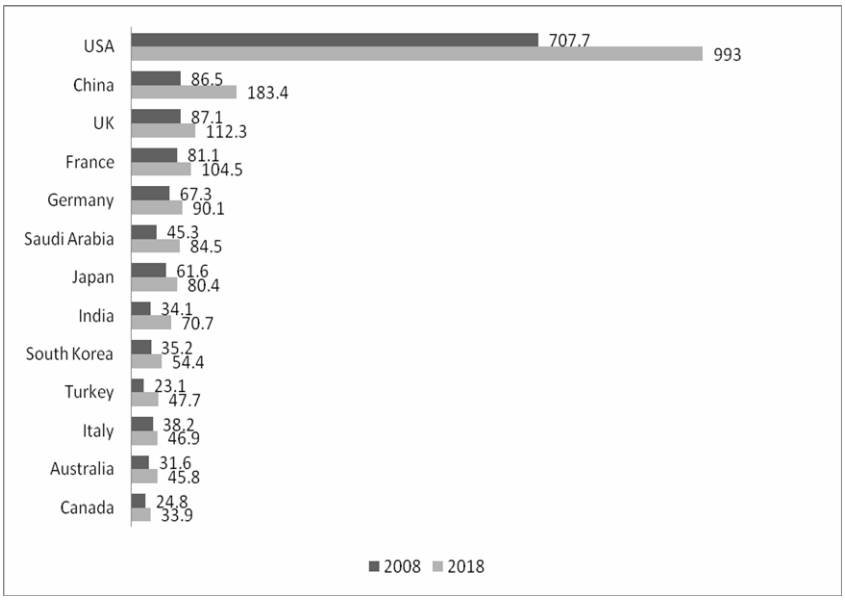
[2] „Critical Infrastructure Emergency Risk, Management and Assurance" Emergency Management Australia, A Division of The Attorney Generals Department, 2003.

[3] „Council Directive 2008/114/EC of 8 Decembar 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" Official Journal of the European Union L, pp. 345-375, 23.12.2008.

KANADA	VELIKA BRITANIJA	SAD	NEMAČKA	NORVEŠKA	ŠVAJCARSKA
TRANSPORT (vazdušni, morski, kopneni)	**FINANSIJE**	**HRANA**	**BANKARSTVO, FINANSIRANjE I OSIGURANjE**	**JAVNO ZDRAVSTVO**	**JAVNO ZDRAVSTVO**
SIGURNOST (nuklearna sigurnost, službe spašavanja, hitne službe)	**TRANSPORT**	**POLjOPRIVREDA**	**TRANSPORTNI SISTEMI**	**BANKARSTVO I FINANSIJE**	**HRANA**
VLADA (bitni vladini objekti, službe i informacioni sistemi i mreže)	**HITNE SLUŽBE**	**BANKARSTVO I FINANSIJE**	**HITNE I SPASILAČKE SLUŽBE**	**TRANSPORT**	**FINANSIJE**
	CENTRALNA VLAST	**HITNE SLUŽBE**	**VLASTI JAVNE SLUŽBE** (uključujući policiju, carinu i oružane snage)	**SPASILAČKE SLUŽBE**	**TRANSPORT**
	VODA I ODVODNjA	**VLAST**		**ODBRANA**	**CIVILNA ODBRANA**
		OSNOVNA ODBRAMBENA INDUSTRIJA		**POLICIJA**	**ADMINISTRACIJA**
		VODA		**DRUŠTVENA SIGURNOST**	**VOJNA ODBRANA**
		HEMIJSKA INDUSTRIJA I OPASNE MATERIJE			**SNABDEVANjE VODOM**

Trenutno, svetska privreda prolazi kroz velike finansijske izazove, ali u područje nacionalne i javne bezbednosti u smislu zaštite kritične infrastrukture ulažu se velika sredstva sa stalnim trendom rasta, što govori o velikoj važnosti kritične infrastrukture.

Na slici 1 grafički je predstavljena potrošnja različitih zemalja sveta koja se odnosi na zaštitu kritične infrastrukture sa projekcijama za 2018. god, u milijardama dolara.



Slika 1 – *Potrošnja na zaštitu kritične infrastrukture ($Mr)*

Najnovija istraživanja tržišta kompanije „JP Freeman" procenjuju da je 38% integrisanih bezbednosnih sistema zasnovano na mrežnim tehnologijama. Ovaj trend intenzivirala je recesija i želja za racionalizacijom sistema, te poboljšanjem bezbednosne funkcionalnosti.

Elementi kritične infrastrukture i njihova međusobna zavisnost

U poslednjoj dekadi načinjeni su značajni koraci da se elementi kritične infrastrukture analiziraju sa aspekta rizika i pripreme za događaje koji mogu omesti njihov rad kroz izradu planova zaštite, tako da se ublaži ugroženost sistema na svim nivoima (regionalni, nacionalni i lokalni). Ipak, strategije koje su usmerene ka uspešnoj prevenciji krajnje negativnih scenarija (terorističkih napada ili prirodnih katastrofa većih razmera), iako veoma efikasne, ne moraju da potvrđuju da je izvršena optimalna alokacija resursa koji su potrebni za zaštitu. Ovo veoma složeno pitanje nivoa ugroženosti predstavlja veliki izazov za pravilno planiranje odgovora na prirodne ili druge nepogode.

Prema „Nacionalnom planu zaštite infrastrukture", koji je sastavni deo „Nacionalne strategije bezbednosti Sjedinjenih Američkih Država", glavni elementi nacionalne kritične infrastrukture su:

– informacije i komunikacije (telekomunikacije, mreže, internet)
– električna energija

– transport
– nafta i gas (snabdevanje, transport, rafinacija, distribucija)
– bankarstvo i finansije
– voda i službe za hitne slučajeve
– vlada (+vojska)

U okviru Direktive Saveta Evrope 2008/114/ES određeni su elementi/sektori za koje je potrebno definisati kritičnu infrastrukturu, kao što je prikazano u tabeli 2.

Tabela 2 – *Sektori kritične infrastrukture u Evropskoj uniji*

Sektor	Podsektor	Kritična infrastruktura
Energija	1. Električna energija	Infrastruktura i objekti neophodni za proizvodnju i prenos električne energije
	2. Nafta	Proizvodnja nafte i rafinisanje
	3. Gas	Proizvodnja gasa i rafinisanje
Transport	4. Drumski transport 5. Železnički transport 6. Vazdušni transport 7. Transport unutrašnjim plovnim putevima 8. Prevoz okeanom i morima	

Imajući u vidu definicije, možemo reći da kritične infrastrukture u okviru jedne države predstavljaju složene „podsisteme sistema". Veliki značaj koji infrastrukture, identifikovane kao kritične, imaju na društvo, obavezuje na stvaranje dovoljno dobrih sigurnosnih mera koje će služiti za umanjenje rizika od prekida rada. Međuzavisnosti obično nisu dovoljno dobro istražene i poremećaji u okviru jedne infrastrukture lako mogu da se prenesu u druge. Kritične infrastrukture povezane su na različitim nivoima i kvar na elementu jedne infrastrukture može lako da se odrazi na elemente druge i obratno[4].

Jasno je da između sektora telekomunikacija i velikog broja elemenata ostalih infrastruktura postoji veoma velika povezanost. Skoro svi elementi vezani za usluge proizvodnje i distribucije električne energije, vode, gasa i sl. imaju zahteve za komunikaciju u određenom obliku. Sa druge strane, komunikacioni sektor umnogome zavisi od drugih sektora. Na osnovu toga možemo zaključiti da telekomunikacioni sektor predstavlja infrastrukturu čija je pozicija centralna i da razumevanje i modelovanje rizika povezanih sa prekidom komunikacija treba da imaju prioritet u razmatranju kritične infrastrukture, radi povećanja nivoa javne bezbednosti i otpornosti infrastruktura na neželjene uticaje[5].

[4] Rajmonah, C., Subramanya G. and Sharma N., „Telecommunications Networks: Security Management", Tata Consultancy Services Limited, 2012.
[5] Rinaldi, S.M., „Modeling and Simulating Critical Infrastructures and Their Interdependencies", 2004.

Mere i inicijative za zaštitu kritične infrastrukture – iskustva SAD i EU

Iako su u SAD i Evropi postojali različiti stavovi o rizicima i pretnjama koji mogu da ugroze opštu sigurnost nacije i kritična nacionalna dobra, ubrzo je formirano zajedničko opredeljenje na dva nivoa koji su definisali:

– koji resursi predstavljaju kritičnu infrastrukturu,

– koje mere su neophodne u njihovoj zaštiti.

U Sjedinjenim Državama resursi identifikovani kao ključna kritična infrastruktura uglavnom obuhvataju: sistem snabdevanja električnom energijom, finansijski i bankarski sistem, telekomunikacije, skladišta i transport gasa i naftnih proizvoda, sistem za vodosnabdevanje, sektor transporta, industriju, službe u vanrednim situacijama, policiju, vatrogasnu službu, kao i sektor odgovoran za kontinuitet funkcionisanja vlade[6].

Druga sistematizacija usmerena je na 11 sektora u koje spadaju: voda, agrarni sektor i hrana, službe u vanrednim situacijama, oblast javnog zdravstva, industrijski sektor, energija, telekomunikacije, transport, finansije i bankarstvo, hemijske i druge hazardne supstance, poštanske usluge i usluge isporučivanja[7].

U Nacionalnoj strategiji zaštite kritične infrastrukture i ključnih materijalnih dobara SAD (Bela kuća, 2003a:9) identifikovani su osnovni elementi infrastrukture koje je neophodno zaštititi u uslovima različitih kriznih situacija.

U ključna dobra ulaze i nacionalni spomenici i ikone, postrojenja nuklearnih elektrana i nasipi. Pored toga, identifikovana su osnovna ministarstva koja moraju da preuzmu nadležnost u zaštiti nacionalne imovine. Ministarstvo nacionalne bezbednosti, Ministarstvo odbrane i unutrašnjih poslova svakako nose glavnu odgovornost, ali svoju obavezu preuzeli su i Ministarstvo energetike, pravde i državne uprave. Takođe, Ministarstvo zdravlja i javnih službi, Agencija za zaštitu životne sredine, Ministarstvo poljoprivrede i Ministarstvo finansija učesnici su vladinih aktivnosti koje se odnose na zaštitu vitalne nacionalne infrastrukture. U tom smislu, EU je takođe učinila značajne napore u analizi kritičnih resursa i preduzela je značajne korake u njihovoj zaštiti.

Istorijski gledano, Savet Evrope je 24. juna 2004. godine zatražio od Komisije da pripremi sveobuhvatnu strategiju zaštite kritične infrastrukture. Komisija je u odgovoru 20. oktobra 2004. godine usvojila dokument koji se odnosio na terorizam kao potencijalnu opasnost. Dokument je dobio naziv „Zaštita kritične infrastrukture u borbi protiv terorizma" koji predlaže jasne sugestije o tome šta bi poboljšalo evropsku prevenciju, spremnost i odgovor na teroristički napad koji pogađa kritičnu infrastrukturu. Savet je usvojio nameru Komisije da predloži Evropski program za zaštitu kritične infrastrukture (EPZKI/EPCIP) i saglasio se oko aranžmana Komisije za Informacionu mrežu za upozoravanje o kritičnoj infrastrukturi (IMUKI/CIWIN).

U novembru 2005. godine Komisija je usvojila Zeleni papir o Evropskom programu za zaštitu kritične infrastrukture (EPZKI/EPCIP) koji izlaže njena politička opredeljenja za ustanovljavanje EPZKI i IMUKI.

[6] Moteff, J., Risk, Management and Critical Infrastructure Protection: Assesing, Integrating and Managing Threats, Vulnerabilities and Consequences, Report for Congress, Science and Industry Division, Congressional Research Service, 2005.

[7] Radvanovsky, R., Critical Infrastructure (Homeland Security and Emergency Preparedness) New York, Taylor and Francis Group, 2006.

U Odluci Saveta za pravosuđe i unutrašnje poslove iz decembra 2005. godine od Komisije je zatražen nacrt Evropskog programa za zaštitu kritične infrastrukture.

U narednim godinama usvojeni su: Direktiva Saveta Evrope 2008/114/ES (2008), Interna strategija zaštite EU (EU Internal Security Strategy, (2010). Tokom 2012. godine rađena je revizija EPZKI/EPCIP programa i Direktive 2008/114/ES.

Cilj evropske politike u ovom području predstavlja osiguravanje prikladnog i jednakog stepena zaštite za postrojenja odabrane kritične infrastrukture, što je izvodljivo jedino na osnovu zajedničkog evropskog okvira za zaštitu kritične infrastrukture. Zanimanje EU za kritičnu infrastrukturu zemalja članica proističe iz opasnosti da bi razaranje ili poremećaj izvesne kritične infrastrukture u jednoj zemlji članici mogli neposredno doticati druge zemlje članice. U takvim slučajevima zaštitne mere su onoliko snažne koliko je to njihova najslabija karika[8].

U ovom smislu EU definiše evropsku kritičnu infrastrukturu kao infrastrukturu koja se sastoji od fizičkih resursa, službi, uređaja, informacione tehnologije, sigurnosti mreža i infrastrukture, bezbednosne, ekonomske ili socijalne dobrobiti: a) dve ili više zemalja članica, b) tri ili više zemalja članica.

Evropska komisija identifikovala je određene oblasti kritične infrastrukture. To su: energija, informacione i komunikacione tehnologije, voda, hrana, finansije, građanske vlasti, javni i pravni poredak i sigurnost, saobraćaj, hemijska i nuklearna postrojenja, kosmos i naučno istraživanje.

Kritična infrastruktura u EU – Direktiva Saveta Evrope 2008/114/ES

Direktiva Saveta Evrope 2008/114/ES iz 2008. godine predstavlja sastavni deo EPZKI/EPCIP programa. Ona definiše kritičnu infrastrukturu, zajedničke procedure 372 za identifikaciju i označavanje evropske kritične infrastrukture, zajednički pristup u proceni potreba za poboljšavanje zaštite, kao i sve rizične pristupe sa prvim prioritetom pretnje od terorizma.

Direktiva 2008/114/ES je osnova za naredne korake u definisanju kriterijuma za kritičnu infrastrukturu. U aneksu III istog dokumenta navedene su procedure, koje svaka zemlja članica treba da implementira, kroz nekoliko konsekventnih koraka:

– korak 1: svaka zemlja članica treba da primeni sektorske kriterijume radi kreiranja inicijalne selekcije kritične infrastrukture u okviru sektora;

– korak 2: svaka zemlja članica treba da primeni definiciju kritične infrastrukture, shodno članu 2, tačka a)[9] na potencijalne evropske kritične infrastrukture identifikovane nakon koraka 1. Značaj učinka određuje se upotrebom nacionalnih metoda za utvrđivanje kritične infrastrukture ili upućivanjem na unakrsne, međusektorske kriterijume, na odgovarajućem nacionalnom nivou. Za infrastrukture koje se koriste za pružanje osnovnih

[8] Boin, A., Rhinhard, M., Prezelj, I., Shocks Without Frontiers - Transnational Breakdowns and Critical Incidents; What Role for the EU, European Policy Center Issue Paper, 42, Brussels, 2005.

[9] Član 2, tačka a) predviđa da je „kritična infrastruktura" imovina, sistem ili njihov deo koji se nalazi u državama članicama i neophodan je za održavanje vitalnih društvenih funkcija, zdravlja, bezbednosti, zaštite, državne i socijalne dobiti ljudi, čiji bi poremećaj rada ili čije bi uništenje, kao posledica neuspešnog održavanja tih funkcija, moglo imati značajne posledice u državi.

servisa treba uzeti u obzir dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa;

– korak 3: svaka zemlja članica treba da primeni prekogranični element za definisanje evropske kritične infrastrukture shodno članu 2, tačka b)[10] na potencijalne evropske kritične infrastrukture koje su prošle prva dva koraka ove procedure. Za potencijalnu evropsku kritičnu infrastrukturu koja zadovoljava definiciju primenjuje se sledeći korak procedure. Za infrastrukture koje se koriste za pružanje osnovnih servisa, treba uzeti u obzir dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa;

– korak 4: svaka zemlja članica treba da primeni unakrsne, međusektorske kriterijume za preostale evropske kritične infrastrukture. Unakrsni, međusektorski kriterijum treba da uzme u obzir: ozbiljnost napada, i za infrastrukture koje se koriste za pružanje osnovnih servisa dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa. Ukoliko potencijalna evropska kritična infrastruktura ne ispunjava unakrsne, međusektorske kriterijume smatraće se da nije evropska kritična infrastruktura.

Na ovaj način definisani su koraci u definisanju kriterijuma za kritičnu infrastrukturu, shodno Direktivi 2008/114/ES.

Kada je doneta, Direktiva 2008/114/ES predstavljala je prvi korak u identifikaciji i određivanju evropske kritične infrastrukture – EKI i potrebe da se unapredi njihova zaštita. U okviru nje naglašeno je da se odnosi na sektor energetike i transporta, ali i da je treba razmotriti sa posebnim osvrtom na procenu međuuticaja sektora, pored ostalog, posebno u odnosu na sektor informacionih i komunikacionih tehnologija. Prva revizija Direktive počela je januara 2012.

Evropski program zaštite kritične infrastrukture (EPZKI/EPCIP): ciljevi i procesi revizije

Prva revizija EPZKI/EPCIP predstavlja osnovne preliminarne zaključke nakon započinjanja procesa razmatranja Evropskog programa za zaštitu kritične infrastrukture (EPCIP), a posebno Direktive 2008/114/ES. Dokument pruža opštu analizu elemenata programa za zaštitu kritične infrastrukture i opisuje neprekidan razvoj metodologija za procenu rizika u ovoj oblasti[11].

Evropski program za zaštitu kritične infrastrukture ima utvrđeni horizontalni okvir, koji obuhvata:

– mere koje se preduzimaju radi olakšavanja implementacije EPZKI/EPCIP: informacioni sistem za uzbunjivanje u okviru kritičnih infrastruktura (IMUKI/ CIWIN); ekspertske grupe zadužene za zaštitu kritične infrastrukture; procesi zaštite kritične infrastrukture za deljenje informacija; identifikacija i analiza međuzavisnosti;

– podršku zemljama članicama u vezi sa nacionalnom kritičnom infrastrukturom;

– planiranje nepredvidivih situacija;

[10] Član 2, tačka b) predviđa da je evropska kritična infrastruktura ili EKI kritična infrastruktura koja se nalazi u državama članicama, a čiji bi poremećaj u radu ili čije bi uništenje imalo znatnu posledicu na najmanje dve države članice. Značaj posledice ocenjuje se s obzirom na unakrsne, međusektorske kriterijume. To uključuje efekte koje su rezultat međusektorskih zavisnosti od drugih vrsta infrastrukture.

[11] „Council Conclusions of 9-10 June 2011 on the development of the external dimension of the European Programme for Critical Infrastructure Protection"

– spoljne dimenzije;

– prateće finansijske mere – EU program „Prevencije, planiranje i upravljanje posledicama terorizma i drugim bezbednosnim rizicima" za period 2007–2013;

– Direktivu 2008/114/ES – procedure za identifikaciju i označavanje EKI.

Kao podrška procesu dodatnog razmatranja, krajem 2011. godine lansirano je evaluaciono istraživanje implementacije i primene Direktive 2008/114/ES. Rezultati su objavljeni u martu 2012.

Pored toga, organizovana je serija sastanaka sa zainteresovanim stranama. Evropska komisija je 15. februara 2012. godine organizovala radionicu na kojoj su potvrđeni rezultati evaluacione studije, a ujedno su razmotrene potrebe za zaštitom pojedinih elemenata kritičnih infrastruktura. U martu 2012. godine u Briselu je održana konferencija na temu zaštite kritične infrastrukture, čiji su učesnici bili predstavnici zemalja članica.

Dodatno razmatranje različitih do sada implementiranih elemenata EPZKI/EPCIP dovelo je do nekoliko važnih zaključaka koji će biti uključeni u oblikovani dokument za definisanje politike zaštite kritične infrastrukture (novembar 2012):

– sve zemlje članice zvanično su implementirale Direktivu 2008/114/ES tako što su ustanovile proces identifikacije elemenata Evropske kritične infrastrukture, što je dovelo do podizanja svesti o potrebi zaštite kritične infrastrukture u Evropskoj uniji i zemljama članicama;

– iako postoje dokazi da je Direktiva pomogla u samoj proceni potrebe da se evropska kritična infrastruktura bolje zaštiti, ne postoje pokazatelji koji bi dokazali da se bezbednost ovih sektora povećala;

– pristup predstavljen u ovoj Direktivi, a koji je orijentisan ka sektorima, predstavlja izazov za veliki broj zemalja članica, jer u praksi analiza kritičnih segmenata nije ograničena na sektor već se često odnosi na sistem ili servis;

– iako je Direktiva doneta sa namenom da definiše jasan evropski okvir koji bi služio kao jedinstven forum svih država u okviru EU, u praksi je podstakao uglavnom bilateralnu saradnju između zemalja članica.

Osnovni elementi za usklađivanje sistema zaštite kritične infrastrukture po Direktivi Saveta Evrope 2008/114/ES

Direktiva 2008/114/ES uspostavlja evropsku proceduru/proces za identifikaciju i određivanje evropske kritične infrastrukture (EKI). Istovremeno, ona obezbeđuje zajednički pristup za procenu zaštite ove infrastrukture, sve radi poboljšanja zaštite potreba građana. Najpre, države članice moraju da prođu kroz proces identifikacije potencijalnih EKI, uz pomoć Komisije, ukoliko je potrebno. Države članice treba da iskoriste niz kriterijuma za identifikovanje tih potencijalnih EKI. Unakrsni kriterijumi uzimaju u obzir moguće gubitke, kao i ekonomske i javni efekte, dok su sektorski kriterijumi uzimaju u obzir specifičnosti svakog EKI sektora.

Ova direktiva odnosi se na sektore energetike i saobraćaja i njihove podsektore, kao što su identifikovani u aneksu I Direktive. Dodatni sektori mogu biti dodati sa osvrtom na direktive.

Svaka država članica treba da ide preko procesa saradnje oznaka za potencijalne EKI koje se nalaze na njenoj teritoriji. Ovaj proces uključuje razgovore sa drugim državama članicama, koje bi mogle biti jako pogođene u slučaju gubitka servisa koje pruža infrastruktura.

Da bi infrastruktura formalno bila određena kao EKI, država članica na čijoj teritoriji se nalazi mora dati svoj pristanak. Država članica na čijoj teritoriji se nalazi EKI mora godišnje obaveštavati Komisiju o broju potencijalnih i određenih EKI za svaki sektor.

Države članice moraju da obezbede Plan sigurnosti operatera (OSP) ili ekvivalent mera koji je na snazi za svaku određenu EKI. Svrha OSP procesa jeste da se identifikuju kritične imovine EKI, kao i postojećih bezbednosnih rešenja za njihovu zaštitu. Minimum sadržaja koji mora biti pokriven definisan je u aneksu II Direktive. Takođe, OSP se mora redovno pregledati.

Države članice moraju osigurati da bezbednosni oficir za vezu ili njegov ekvivalent bude određen za svaku EKI. Oficir služi kao kontakt između vlasnika/operatera EKI države članice i organa vlasti. Cilj je da se omogući razmena informacija u vezi sa rizicima i pretnjama koji se odnose na EKI.

U roku od godinu dana od određivanja EKI sektora i podsektora, države članice treba da izvrši procenu pretnji koje se odnose na njega. Pored toga, države članice treba da izveštavaju Komisiju svake dve godine o rizicima, pretnjama i ranjivostima sa kojima se, u različitim sektorima, EKI suočavaju. Potreba za dodatnim merama Zajednice za zaštitu EKI ocenjivaće se na osnovu ovih izveštaja.

Da bi podržali vlasnike/operatere EKI, Komisija obezbeđuje pristup najboljim praksama i metodologijama u vezi sa zaštitom kritične infrastrukture. Osim toga, Komisija podržava srodne aktivnosti obuke i razmene novih tehničkih informacija.

Svakoj osetljivoj informaciji u vezi sa zaštitom EKI pristup i uvid u njih mogu imati samo lica koja imaju odgovarajući nivo bezbednosne provere i samo za potrebe informisanja u vezi EKI kojoj je prvobitno namenjen.

Kontakt-tačka evropske kritične infrastrukture (EKI kontakt-tačka) mora biti određena u svakoj državi članici. Njihova svrha je da, u ime države članice, sprovodi komunikaciju i koordinaciju sa nadležnim telima EU i drugih država, radi razmene informacija o kritičnim infrastrukturama i sprovođenju utvrđenih aktivnosti u njihovoj zaštiti i osiguranju neprekidnog funkcionisanja.

Odnos Republike Srbije prema zaštiti kritične infrastrukture

Republika Srbija učinila je značajne napore u stvaranju integrisanog sistema zaštite i spasavanja, koji bi na adekvatan način odgovorio u uslovima ugrožavanja kritičnih nacionalnih resursa.

Zakonom o vanrednim situacijama, koji je usvojen 2009. godine, država se opredelila da Ministarstvo unutrašnjih poslova bude nadležno za izradu procene ugroženosti od elementarnih nepogoda i drugih nesreća, te je dostavlja Vladi na usvajanje. Autonomne pokrajine, jedinice lokalne samouprave, ministarstva i drugi organi i organizacije izrađuju procenu ugroženosti u delu koji se odnosi na njihov delokrug i dostavljaju je Ministarstvu unutrašnjih poslova.

Istim zakonom, u članu 46, propisuje se da se procenom ugroženosti identifikuju izvori mogućeg ugrožavanja, sagledavaju moguće posledice, potrebe i mogućnosti sprovođenja mera i zadataka zaštite i spasavanja od elementarnih nepogoda i drugih nesreća. Procena ugroženosti sadrži naročito: 1) karakteristike teritorije, kritična postrojenja, kritična mesta i prostore sa gledišta ugroženosti od elementarnih nepogoda i drugih nesreća,

sa eventualnim prekograničnim efektima udesa; 2) povredljivost teritorije od elementarnih nepogoda i drugih nesreća; 3) analizu mogućih posledica od elementarnih i drugih nesreća; 4) potrebe i mogućnosti za zaštitu ljudi, materijalnih dobara i životne sredine od posledica elementarnih i drugih nesreća.

Vlada Republike Srbije je, na osnovu člana 45, stav 4 Zakona o vanrednim situacijama donela Uredbu o sadržaju i načinu izrade plana zaštite i spasavanja u vanrednim situacijama. Ovim dokumentom, pored već navedenih elemenata procene ugroženosti, koji su definisani u Zakonu o vanrednim situacijama, predviđa se da će deo procene biti i procena kritične infrastrukture sa gledišta elementarnih nepogoda i drugih većih nesreća.

U Srbiji se ovom uredbom prvi put uvodi pojam kritične infrastrukture, ali i dalje bez jasnog definisanja o kojim je elementima ili oblastima infrastrukture reč. Takođe, nisu određeni subjekti koji bi snosili odgovornost u zaštiti kritične infrastrukture. U narednom periodu predviđa se i donošenje Uputstva o metodologiji za izradu procene ugroženosti i izradu planova za zaštitu i spasavanje.

Takođe, pitanje kritične infrastrukture može se prepoznati i u drugim normativnopravnim dokumentima koji su predlagani u Republici Srbiji i koji su predstavljali novi korak u njenoj zaštiti.

Jedan od dokumenata u kojem se pominje kritična infrastruktura je „Strategije razvoja informacionog društva u Republici Srbiji do 2020", u kojoj se u okviru poglavlja 6.2. definiše: „Potrebno je razvijati i unapređivati zaštitu od napada primenom informacionih tehnologija na kritične infrastrukturne sisteme, što pored informaciono-komunikacionih sistema mogu biti i drugi infrastrukturni sistemi kojima se upravlja korišćenjem informaciono-komunikacionih, poput elektroenergetskog sistema. U vezi toga je potrebno dodatno urediti kriterijume za utvrđivanje kritične infrastrukture sa stanovišta informacione bezbednosti, kriterijume za karakterizaciju napada primenom informacionih tehnologija na takvu infrastrukturu u odnosu na klasične oblike napada, kao i uslove zaštite u ovoj oblasti".

U okviru „Strategije nacionalne bezbednosti Republike Srbije", pojam „kritična infrastruktura" se ne spominje decidno, ali se u okviru tačke II navode njeni elementi u delovima koji se odnose na: probleme ekonomskog razvoja Republike Srbije usled višegodišnjih ekonomskih sankcija i uništenja vitalnih objekata privredne i saobraćajne infrastrukture, energetsku međuzavisnost i osetljivost infrastrukture za proizvodnju i transport energenata i visokotehnološki kriminal i ugrožavanje informacionih i telekomunikacionih sistema.

Potreba za razmatranjem kritične infrastrukture prepoznata je u okviru projekta „Upravljanje kritičnom infrastrukturom za održivi razvoj u poštanskom, komunikacionom i železničkom sektoru Republike Srbije 2011–2014". U jednom delu, pojedine elemente pojma „kritična infrastruktura" možemo prepoznati i u okviru Uredbe o određivanju poslova bezbednosne zaštite određenih lica i objekata..

Osim navedenog, Vlada Republike Srbije je 19. 9. 2002. godine podnela Narodnoj skupštini predlog zakona o fizičko-tehničkom obezbeđenju objekata. Tako se u članu 8. predloga ovog zakona predlaže da objekti od strateškog značaja za Republiku Srbiju ili njene građane, ili koji predstavljaju povećanu opasnost za život i zdravlje ljudi, moraju imati fizičko i tehničko obezbeđenje. Kao obavezno obezbeđeni objekti navode se: 1) objekti za proizvodnju, preradu, distribuciju i skladištenje nafte, naftnih derivata i gasa; 2) objekti za proizvodnju, preradu, distribuciju i skladištenje vode; 3) objekti za proizvodnju i distribuciju električne energije; 4) objekti u kojima se proizvode, koriste ili skladište radioaktivne i druge opasne i štetne materije; 5) objekti od značaja za saobraćaj u svim

vrstama saobraćaja; 6) objekti u kojima se drže stvari od izuzetnog značaja za nauku, kulturu i umetnost; 7) objekti u kojima se okuplja veliki broj ljudi i drugi objekti za koje Vlada utvrdi da se obavezno obezbeđuju.

Ovim nacrtom zakona bilo je propisano da se obezbeđivanje obavezno štićenih objekata vrši kao poslovna funkcija predviđena u osnovnom, opštem aktu, u skladu sa Planom obezbeđivanja i aktom o organizovanju i vršenju fizičkog obezbeđivanja, koji predstavljaju poslovnu tajnu i na koje saglasnost daje nadležni organ.

Obavezno obezbeđene objekte vlasnik, odnosno korisnik, može obezbediti organizovanjem sopstvene službe ili angažovanjem pravnih lica koja obavljaju delatnost obezbeđivanja objekata, uz saglasnost nadležnog organa. Pored brojnih nedostataka, i ovaj normativnopravni dokument upotpunjuje pitanje zaštite ključnih objekata države.

Zaključno, dokumenti koji bi trebalo da obrađuju pitanja kritične infrastrukture su Nacionalna strategija zaštite i spasavanja u vanrednim situacijama i Zakon o vanrednim situacijama. Međutim, u ovim dokumentima se ne pominje kritična infrastruktura.

Treba naglasiti da institucionalni okviri za definisanje kritične infrastrukture postoje, a to su Sektor za vanredne situacije MUP-a Republike Srbije, nadležna ministarstva, kao i nadležna regulatorna tela. Određene mere zaštite delova infrastrukture preduzeli su operatori, ali nisu donesene ni strategija, ni politika zaštite na nivou zemlje.

Različiti pristupi za utvrđivanje kritične infrastrukture

Analiza postojećih mehanizama zaštite kritične infrastrukture u zemljama EU ukazala je na to da postoje razlike u pristupu i merilima koje različite države članice EU koriste za identifikovanje kritične nacionalne infrastrukture. Konkretno, „polazne tačke" analize znatno se razlikuju[12].

Na primer, neke države članice započinju određivanjem koje su to osnovne usluge koje su društvu potrebne za funkcionisanje, te koje infrastrukture podržavaju te usluge. Drugi započinju identifikovanjem ključne infrastrukture u svakom sektoru, a zatim procenjuju uticaj na društvo koji bi se dogodio u slučaju njihovog pada. Treći započinju identifikovanjem ključnih operatora u svakome kritičnom sektoru, a zatim prepuštaju operatorima da odrede koje su infrastrukture kritične za stalnu isporuku njihovih usluga.

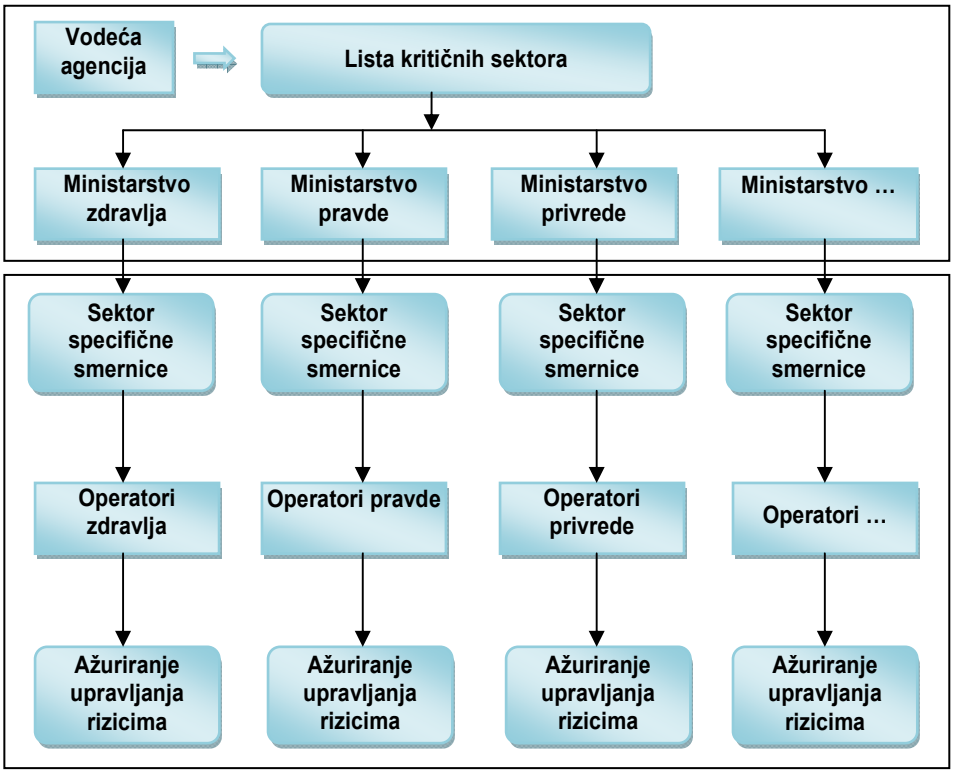
Nakon sužavanja kompletnog asortimana infrastruktura do uže liste „potencijalno kritičnih" infrastruktura, merila koja se koriste kako bi se dala konačna ocena o „kritičnosti" pojedinih infrastruktura takođe se razlikuju. Dok neke države članice navode specifična, objektivna merila kao što su finansijski gubitak ili broj stanovnika na koje se može uticati, druge se države oslanjaju na više subjektivna merila koja se zasnivaju na stručnim mišljenjima viših članova vladinih agencija i privatnih operatora odgovornih za pojedini sektor.

Bez obzira na razlike u procesu određivanja kritične nacionalne infrastrukture, proces upravljanja rizicima tih infrastruktura (jednom kada su identifikovane) mora biti u skladu s najboljim međunarodnim praksama životnog ciklusa upravljanja rizicima, preporučenog i

[12] Hamidović, H., „CT Pripravnost za zaštitu kritične infrastrukuture; Objektivne opasnosti – subjektivna merila", InfoTrend, 2012.

normama kao što su BS 25999-1:2006 (Upravljanje kontinuitetom poslovanja) i ISO/IEC 27001:2005 (Upravljanje informacionom bezbednošću).

Kod mnogih kritičnih infrastruktura koje se danas nalaze u vlasništvu i njima upravlja privatni sektor, vladine agencije su prilagodile svoj stil odnosa s tim operatorima iz regulatornog položaja u pristup „uzajamna korist". Nakon što se odgovornost za neki sektor dodeli određenom ministarstvu, to ministarstvo uglavnom lakše prihvata, za taj sektor specifične „smernice", za rad s operatorima. Navedene aktivnosti prikazane su na slici 2.



Slika 2 – *Primer nacionalne strategije za zaštitu kritične infrastrukture*

U većini slučajeva, centralna agencija se usredsređuje na ukupnu koordinaciju aktivnosti zaštite kritične infrastrukture, dok pojedina ministarstva nose sektor specifične odgovornosti. S tim u vezi, samo dve države članice EU imaju nacionalne agencije s težištem isključivo na zaštiti kritične infrastrukture (Velika Britanija – CPNI, Španija – CNPIC), dok je 45% nacionalnih agencija s težištem na zaštiti kritične infrastrukture bilo pod okriljem Ministarstva unutrašnjih poslova ili slične agencije za nacionalnu bezbednost.

Generalno, istraživanje je pokazalo da je najčešći organizacijski model zasnovan na centralnoj agenciji koja predsedava radnom grupom čiji su članovi iz različitih ministarstava. Takođe, mora se napomenuti da se Direktivom 2008/114/ES od država članica zahteva da procene

postoji li za svu EKI infrastrukturu, koja se nalazi na njihovoj teritoriji, plan sigurnosti operatora ili su uspostavljene druge ekvivalentne mere usmerene na rešavanje bezbednosnih pitanja.

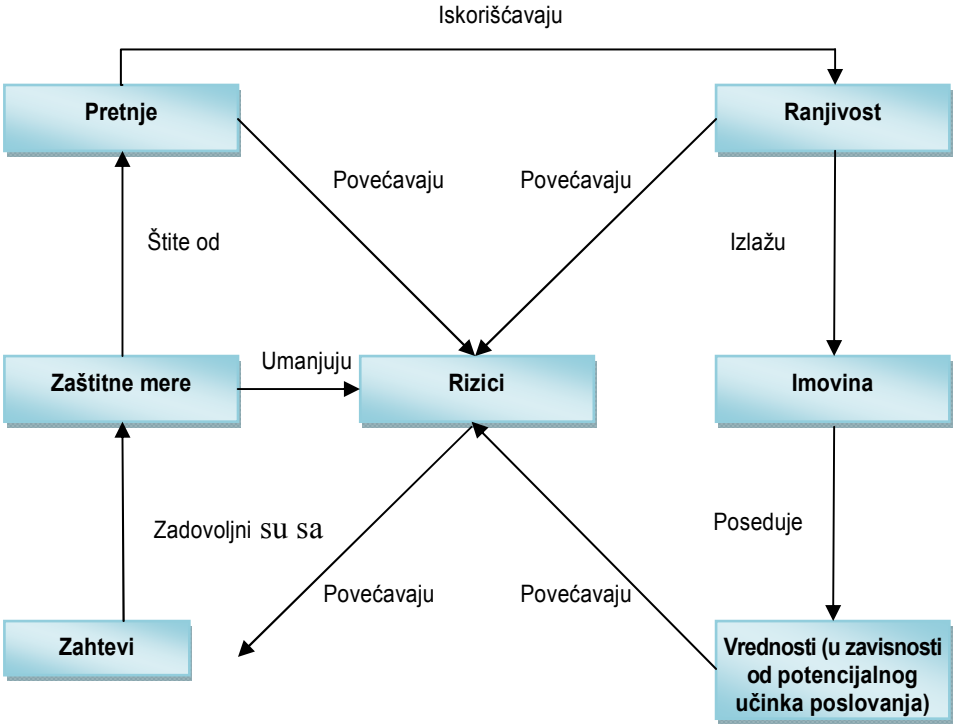
Plan sigurnosti operatora treba da uključi bar:

1. identifikaciju značajne imovine;
2. sprovođenje analize rizika na osnovu scenarija glavnih pretnji, ranjivosti svake imovine i mogućeg uticaja i
3. identifikaciju, izbor i postavljanje prioriteta protivmera i postupaka s razlikovanjem između:

– stalnih mera bezbednosti, koje identifikuju nužna bezbednosna ulaganja i sredstva za koja je bitno da budu u funkciji sve vreme. To poglavlje će sadržavati podatke o opštim merama kao što su tehničke mere (uključujući i implementaciju mera za detekciju, nadzor pristupa, mera zaštite i sprečavanja), organizacione mere (uključujući postupke za upozorenja i upravljanje krizom), nadzor i proveru mera, komunikaciju, podizanje svesti i obrazovanje, kao i bezbednost informacionih sistema;

– postupnih mera bezbednosti koje se mogu aktivirati u skladu s različitim nivoima rizika i pretnji.

Na slici 3 prikazan je odnos između elemenata bezbednosti, neretko povezanih sa upravljanjem rizicima. Radi jasnoće prikazani su samo glavni odnosi.



Slika 3 – *Odnos između elemenata bezbednosti*

Put koji nam predstoji – institucionalizovanje sistema zaštite kritične infrastrukture u Republici Srbiji

Imajući u vidu sve što je rečeno, a radi institucionalizovanja sistema zaštite kritične infrastrukture u Republici Srbiji, odnosno usklađivanja pozitivnopravnog sistema Republike Srbije sa osnovnim elementima Direktive 2008/114/ES, neophodno je preduzeti sledeće korake:

– identifikovati nacionalnu i evropsku kritičnu infrastrukturu;

– izvršiti analizu rizika, odnosno razmatranje mogućih scenarija ili pretnji kako bi se ocenile ranjivost i mogući učinak poremećaja u radu kritične infrastrukture ili njenog uništenja;

– ustanoviti sistem međusektorskih merila, kao skup opštih merila/pravila na osnovu kojih se procenjuje rizik za pojedine sisteme i mreže kritičnih infrastruktura u svim sektorima;

– ustanoviti sistem sektorskih merila, kao skup specifičnih merila/pravila na osnovu kojih se procenjuje rizik za sisteme i mreže kritičnih infrastruktura u pojedinom sektoru;

– definisati poverljive podatke koji se odnose na nacionalnu i evropsku kritičnu infrastrukturu, način njihove razmene sa državama članicama EU i drugim državama, kao i sistem njihovog prijema, eksploatacije i arhiviranja;

– odrediti kontaktnu tačku koja je centralno telo državne uprave, a koja u ime države sprovodi komunikaciju i koordinaciju sa nadležnim telima EU i drugih država, radi razmene informacija o kritičnim infrastrukturama i sprovođenju utvrđenih aktivnosti u njihovoj zaštiti i osiguranju neprekidnog funkcionisanja.

– odrediti sigurnosnog koordinatora za kritičnu infrastrukturu – osobu koja je nadležna za pitanja u vezi sa zaštitom kritične infrastrukture između vlasnika/operatora i centralnih tela državne uprave nadležnih za pojedini sektor kritične infrastrukture;

– uspostaviti Plan sigurnosti vlasnika/operatora – plan koji osigurava poverljivost, celovitost i raspoloživost organizacionih, kadrovskih, materijalnih, informaciono-komunikacionih i drugih rešenja, te stalnih i stepenovanih bezbednosnih mera potrebnih za neprekidno funkcionisanje kritične infrastrukture;

– urediti postupanje sa osetljivim podacima koji se odnose na zaštitu kritične infrastrukture;

– odrediti inspekcijski nadzor nad sprovođenjem svih preporučenih elemenata zaštite kritične infrastrukture, u skladu sa Direktivom 2008/114/ES;

– predvideti i sprovoditi prekršajne odredbe koje bi se primenjivale u slučaju nepostupanja u skladu sa Direktivom 2008/114/ES.

Zaključak

Opšteprihvaćena je činjenica da su krizne i vanredne situacije deo svakodnevnog života i da se sa razvojem društva povećavaju izvori, oblici njihovog javljanja, kao i gubici ljudskih života, praćeni ogromnim materijalnim štetama.

Kompleksnost kriznih i vanrednih situacija, posebno činjenica da se njihovom pojavom ugrožavaju kritični kapaciteti koji su suštinski u redovnom procesu funkcionisanja društva, navele su većinu država da razviju akcije koje su imale za cilj da: 1) shvate elemente kritičnosti i ranjivosti različitih infrastruktura države, 2) definišu mere za smanjenje tih ranjivosti, 3) osmisle i razviju planove za krizne i vanredne situacije i poslekrizni oporavak, 4) podstaknu razvoj senzibiliteta kod javnih i privatnih operatera u pogledu problema zaštite kritične infrastrukture, 5) podrže međunarodnu saradnju.

Takođe, u pogledu mera zaštite kritične infrastrukture, sve države, uključujući i Republiku Srbiju, moraju da utvrde i određene postupke, čiji je redosled: a) identifikacija kritične infrastrukture, b) izrada mapa kritične infrastrukture, c) razmena informacija, d) osposobljavanje osoblja angažovanih na poslovima i zadacima u sistemima kritične infrastrukture, e) uvežbavanje sistema za zaštitu kritične infrastrukture ili oporavak u slučaju krizne ili vanredne situacije.

Analizirajući nacionalne strategije država članica EU u delovima koji se odnose na zaštitu nacionalne i evropske kritične infrastrukture, ustanovljeno je da se odluke oko određivanja kritičnih sektora i/ili usluga, kao i odgovornosti odgovarajućih ministarstava za te sektore/usluge na državnom nivou, uglavnom definišu kroz zakone, uredbe itd., koje donose nacionalne vlade.

U tom smislu, Republika Srbija bi u toku procesa pridruživanja EU trebalo da usvoji zakon o kritičnim infrastrukturama koji će biti usklađen sa elementima Direktive 2008/114/ES. Na taj način, podigli bi nivo interoperabilnosti Republike Srbije sa EU, ali bi i regulisali značajnu oblast koja do danas nije adekvatno regulisana.

Literatura

1. Direktiva Saveta Evrope 2008/114/ES o utvrđivanju i označavanju evropske kritične infrastrukture i procene potrebe poboljšanja njene zaštite, „Službeni list EU", Brisel, 08.12.2008.

2. Стратегија националне безбедности Републике Србије, Београд, 2009.

3. Стратегија развоја информационог друштва у Републици Србији до 2020, *Службени гласник Републике Србије*, бр. 51/2010.

4. Национална стратегија заштите и спасавања у ванредним ситуацијама Р Србије, *Службени гласник Републике Србије*, бр. 86/2011.

5. Закон о ванредним ситуацијама, *Службени гласник Републике Србије*, бр. 111/2009, 92/2011 и 93/2012.

6. Zakon o kritičnim infrastrukturama, Zagreb, „Narodne novine" br. 56/13.

7. Уредба о одређивању послова безбедносне заштите одређених лица и објеката, *Службени гласник Републике Србије*, бр. 72/2010.

8. Уредба о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама, *Службени гласник Републике Србије*, бр. 8/2011.

9. „Управљање критичном инфраструктуром за одрживи развој у поштанском, комуникационом и железничком сектору Републике Србије 2011-2014", Институт Саобраћајног факултета, Универзитета у Београду, 2011.

10. Цветковић, В.: *Ризик, мој, заштита*, Факултет безбедности, Универзитет у Београду, 2010.

11. Keković, Z., Čaleta, D., Kešetović, Ž., Jeftić, Z.: *National Critical Infrastructure Protection – Regional Perspective*, Fakultet bezbednosti Univerziteta u Beogradu, 2013.

12. Jakovljević, V., Gačić, J.: „Zaštita kritične infrastrukture u kriznim situacijama", Međunarodna naučna konferencija, Mladenovac, 2012.

13. Gospić, N., Murić, G., Bogojević, D.: „Definisanje kritične telekomunikacione infrastrukture u Srbiji", 30. Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju, Beograd, 2012.

14. Kljaić, Z., Mandžuka, S., Škorput, P.: „Primjena ICT-a u upravljanju kritičnom infrastrukturom u tranzicijskim zemljama", Telekomunikacioni forum TELFOR, Beograd, 2010.

15. Hamidović, H.: „CT Pripravnost za zaštitu kritične infrastrukuture; Objektivne opasnosti – subjektivna merila", Internet sajt InfoTrend, 2012.

16. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_ terrorism/jl001 3 _en.htm

17. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism /critical-infrastructure/index_en.htm