351.824.11(497)
https://doi.org/10.18485/fb_nps.2018.ch13

Branislav Todorović
Nacionalni tehnički univerzitet Atine (NTUA)

Inicijativa „Pojas i put" i zaštita odgovarajuće kritične infrastrukture na balkanskom raskršću

Sažetak

Očekuje se da će Inicijativa „Pojas i put" uticati na širenje i razvoj kritične infrastrukture (KI) zemalja Zapadnog Balkana, ali će složenost Inicijative „Pojas i put" izložiti kritičnu infrastrukturu i nizu novih rizika i problema. Ovaj rad istražuje stanje kritične infrastrukture i mogućnosti za unapređenje aktivnosti u cilju zaštite kritične infrastrukture u Republici Srbiji imajući u vidu sadašnju situaciju na Balkanu i u svetu. U radu se definišu neka ključna pitanja u vezi sa zaštitom kritične infrastrukture u SAD, Evropskoj uniji i Kini, posebno u sajber prostoru i obrazlaže pravac strategije za zaštitu kritične infrastrukture na Balkanu, imajući u vidu da se nalazi na raskršću – i da je, samim tim, potrebno da se usvoji zajednički pristup zaštiti kritične infrastrukture.

Ključne reči:

zaštita kritične infrastrukture, sajber prostor, vanredna situacija, zakonodavstvo, „Jedan pojas, jedan put" – inicijativa P&P, Srbija, strategija

I. UVOD

Inicijativa „Jedan pojas, jedan put" – inicijativa P&P (One Belt, One Road – B&R initiative) sve više postaje, kao što se mnogi slažu, najveći konglomerat projekata u ovom veku. Sam obim ove inicijative zahteva ozbiljno promišljanje i planiranje u svim fazama i po svim zadacima, od konceptualnog okvira do detaljnog izgleda, preko izgradnje i kasnije tokom njenog korišćenja u decenijama koje dolaze. To je jedan od razloga zašto ova Inicijativa zahteva primenu najsavremenijeg rešenja, novog načina razmišljanja i snažnu saradnju između Kine i drugih zemalja, uključujući zemlje Srednje i Istočne Evrope (SIE). Inicijativa „Pojas i put" trebalo bi da promoviše sinergiju između Kine i ovih zemalja, i da pruži nove primere saradnje u oblasti proizvodnih kapaciteta, investicija, u oblasti trgovine i finansija i da proširi kulturnu razmenu.

Budući da je predviđena i planirana primena najnovijih tehnologija u okviru ove inicijative, na Trećem samitu Kine i zemalja Srednje i Istočne Evrope u Beogradu decembra 2014. je predloženo osnivanje *think tank* organizacija koje bi se bavile akademskim istraživanjima. Sledeći korak bio je osnivanje Think tank mreže (Think Tank Network) u okviru Inicijative „Pojas i put". Međutim, osim što obuhvata zajednička politička, finansijska, tehničko-ekonomska, tehnološka i kulturna pitanja, važno je da ova inicijativa uključi i najnovije domete u oblasti istraživanja i razvoja, planiranje i praktičnu primenu tehnika bezbednosti i zaštite i rukovođenja u ovim oblastima, posebno u oblasti kritične infrastrukture. Kada govorimo o ovoj inicijativi, infrastruktura bi mogla da obuhvati: puteve i železnicu za kopneni transport i luke za pomorski transport; dalekovode i druge sisteme za snabdevanje energijom; sisteme informacionih i komunikacionih tehnologija (IKT); različite oblike logističke infrastrukture npr. zgrade, objekti i postrojenja za snabdevanje vodom itd.

II. ŠTA INICIJATIVA P&P ZNAČI ZA ZAPADNI BALKAN

Čitav niz članaka i radova obrađivao je uticaj i značaj Inicijative P&P. Kada je reč o P&P i Zapadnom Balkanu, mogu se uočiti neki ključni elementi u delovima izveštaja dr Jensa Bastiana (Jens Bastian) za Evropsku banku za obnovu i razvoj [Bastian 2017]:

- Sa dostupnim kapitalom, tehnologijom i master planom pod okriljem P&P, kineske investicije u EU i zemljama koje ne pripadaju EU stvaraju pogodne uslove za nabavku i inoviranje infrastrukture do sada neviđenih razmera.
- Kineski ambiciozni projekat P&P može da doprinese i pomogne *transformaciji Zapadnog Balkana*.
- P&P uključuje i davanje inicijativa za donošenje mere u različitim oblastima, određivanje investicionih prioriteta i donošenje poslovnih odluka kineskih vlasti i kompanija koje mogu imati *ogroman uticaj na zemlje učesnice i njihove regulatorne institucije i organizacije civilnog društva*.

Inicijativa P&P utiče na zemlje Zapadnog Balkana na nekoliko načina koji su izvan opsega ovoga rada. Što se tiče kritične infrastrukture, možemo da očekujemo da će ova inicijativa doneti napredak, i u oblasti izgradnje nove infrastrukture i u oblasti osavremenjivanja i popravljanja postojeće, uz upotrebu novih tehnoloških rešenja. Nažalost, unapređenje infrastrukture je praćeno i povećanjem rizika svih vrsta, čemu smo svedoci poslednjih godina. Stoga, veoma je važno da taj proces napredovanja prate i odgovarajuće bezbednosne mere i mere zaštite.

III. RIZICI I ZAŠTITA KRITIČNE INFRASTRUKTURE – PRIKAZ

Rizici se vezuju za izgradnju, upotrebu i funkcionisanje komponenata i sistema infrastrukture. Izgradnja i planirano funkcionisanje se zasnivaju na projektu inženjera, tako da inženjeri moraju da razmotre sve odgovarajuće rizike i da planiraju kako da ih smanje. Nakon izgradnje, upotreba infrastrukture, njeno funkcionisanje i druge aktivnosti mogu da prouzrokuju dodatne rizike, i, stoga, oni koji planiraju i rukovode aktivnostima moraju sve vreme da budu uključeni u smanjenje ovih rizika i negativnih posledica (Slika 1).

Slika 1. *Upravljanje rizikom kao integralna komponenta zaštite infrastrukture*

U skladu sa tim, planiranje i projektovanje infrastrukture u okviru Inicijative P&P trebalo bi da obuhvati i upravljanje rizikom kao svoju značajnu komponentu, i kao integralni deo odluka koje donosi inženjer. „Upravljanje rizikom se odvija tokom projektovanja sistema i tokom samog funkcionisanja. Upravljanje rizikom vodi ka donošenju odluka da li nešto treba uraditi (i koje mere treba preduzeti) kako bi se smanjio rizik. Ako neko smatra da rizik predstavlja raspodelu verovatnoće u okviru mogućih ishoda, onda upravljanje rizikom podrazumeva odabir neke mere kojom bi se modifikovala ta raspodela verovatnoće" [Herrmann 2015]. Štaviše, imajući u vidu složenost sistema kako to predviđa Inicijativa P&P, važno je uključiti multidisciplinarne timove stručnjaka u sam proces projektovanja kako bi se postigla dobra koordinacija aktivnosti u različitim poljima, precizno planiranje aktivnosti i rada, i najbolja moguća pripremljenost za različite slabosti i rizike.

Na organizacionom nivou, kontinuitet poslovanja i planiranje za oporavak od katastrofa su važni činioci upravljanja rizikom. Rizik obuhvata, s jedne strane, i probleme sa opremom i prirodne katastrofe, preko ljudskih grešaka, do, s druge, neprijateljskih i terorističkih napada. Rizik pokriva zdravstvene i bezbednosne, finansijske i dr. potencijalne opasnosti. Stoga je upravljanje rizikom konstantan proces tokom celog veka trajanja infrastrukture, koji se odvija ciklično i čiji su glavni elementi procena, priprema, odgovor i oporavak (precizne definicije zavise od autora do autora). Svi se slažu da upravljanje rizikom i zaštitom kritične infrastrukture ima za cilj da poboljša spremnost za vanredne situacije kako bi se obezbedio kontinuitet poslovanja (Slika 2).

Slika 2. *Segmenti i komponente upravljanja rizikom i zaštitom*

Dve komponente kritične infrastrukture (fizička, koja uključuje i ljudski faktor, i sajber komponenta) predstavljaju suštinu upravljanja rizikom i trebalo bi da budu integrisani u proces upravljanja rizikom (Ministarstvo unutrašnje bezbednosti SAD – 2013). U razvijenim zemljama, rad i funkcionisanje kritične nacionalne infrastrukture zavise od kompjutera i informaciono-komunikacionih tehnologija i stoga lako mogu postati meta. Ako uzmemo u obzir da nacionalna infrastruktura uključuje određeni broj sistema koji se oslanjaju na razvijene tehnologije i njihovu podršku, između ostalog: energetski sistem, nuklearne elektrane, javno zdravlje, službe za hitne slučajeve, vlada, brane, sistem snabdevanja strujom i vodom, transportni saobraćaj, mreža telekomunikacija, lako se može zaključiti da potencijalni napadi na ove sisteme mogu imati ogromne posledice po zemlju i to, uglavnom, po civile [Ophandt 2010].

IV. ZAŠTITE KRITIČNE INFRASTRUKTURE U SRBIJI – PROBLEMI I TENDENCIJE

Republika Srbija je dobro organizovana da odgovori na prirodne katastrofe, kako je i pokazala nekoliko puta tokom prethodnih decenija, uprkos očiglednom porastu broja prirodnih katastrofa širom sveta i njihovoj sve većoj razornoj moći. Prirodne katastrofe često prouzrokuju gubitak velikog broja žitova, pored materijalne i nematerijalne štete. Osim toga, prekid rada kritične infrastrukture sprečava ili ograničava rad vitalnih državnih segmenata (upravljanje državom, njen zdravstveni, energetski, socijalni, obrazovni i bezbednosni segment), što se dalje odražava na bezbednost građana. Uprkos globalnom tehnološkom napretku, ipak ostaje činjenica da katastrofe i

njihov uticaj na ljude i kritičnu infrastrukturu ne mogu da budu sprečeni, ali mehanizmi predviđanja i ranog upozoravanja na katastrofe mogu da se unaprede. To znači da otpornost i sposobnost za brži i efikasniji oporavak rada i funkcionisanja kritične infrastrukture u okviru društva mogu da se poboljšaju. Pored stepena katastrofe, vreme za reagovanje i strategija za vanredne situacije ukazuju na stepen spremnosti, i u Srbiji zaslužuju najvišu ocenu za tu spremnost.

U isto vreme, izvesna zbunjenost i haotična situacija se primećuju u Republici Srbiji kada je reč o bezbednosti kritične infrastrukture, njenoj zaštiti i otpornosti. Takvo stanje i dalje traje, čak i pošto je donesen Zakon o vanrednim situacijama (Službeni glasnik Republike Srbije broj 111/2009 i Nacionalna strategija zaštite i spasavanja u vanrednim situacijama, Službeni glasnik Republike Srbije, broj 86/2011). Pitanje je da li postoji jasna slika u Srbiji kako zaštititi kritičnu infrastrukturu, jer zakonodavci nisu precizno definisali tu oblast, tj. uslove, opseg i ciljeve zaštite kritične infrastrukture i njene otpornosti. U datim okolnostima i kako bi se prevazišle zakonske praznine, Vlada Republike Srbije je definisala Uredbu o sadržaju i načinu izrade planova zaštite i spasavanja u vanrednim situacijama na osnovu člana 45, stav 4. Zakona o vanrednim situacijama. Ova Uredba zvanično uvodi termin 'kritična infrastruktura' po prvi put u Srbiji. Međutim, ostaje nejasno na koju infrastrukturu se termin odnosi [Todorovic et al. 2016].

Zemlje u tranziciji, uključujući Srbiju i njene susede na Zapadnom Balkanu, podložne su specifičnim situacijama jer se suočavaju sa radikalnim transformacijama u svim oblastima (demokratizacija društva, prevazilaženje autoritarnog nasleđa, transformacija društvene svojine, pogoršanje infrastrukture, zastarele tehnologije itd). Ove zemlje značajno zaostaju za razvijenim zemljama koje imaju razvijenije i efikasnije sisteme zaštite kritične infrastrukture. Takođe, one se suočavaju sa problemima koji ih onemogućavaju da uspostave odgovarajući sistem zaštite (nedovoljno razvijene demokratske institucije, odsustvo odgovarajućih ekonomskih mera i politike, nedostatak jasno definisanih izvora i oblika ugrožavanja kritične infrastrukture, nedostatak jasne klasifikacije kritičnih sektora i koherentan pravni okvir koji bi regulisao ovu oblast). Paralelno sa identifikovanjem ovih problema, sa kojima je suočena većina zemalja u tranziciji, važno je imati u vidu da svaka od ovih zemalja ima svoje posebnosti koje otežavaju pronalaženje i definisanje univerzalnih zaključaka i preporuka [Kešetović et al. 2013]. Možda bi Inicijativa P&P mogla da bude ključna tačka jednog integrisanog pristupa zaštiti kritične infrastrukture na Zapadnom Balkanu. Za početak se mogu uzeti primeri i paradigme zaštite kritične infrastrukture razvijenih i tehnološki naprednih zemalja, a potom bi komparativna metoda mogla da se iskoristi da bi se identifikovali kritični sektori i usvojili

i primenili elementi i metodologije koje bi doprinele poboljšanju zaštite kritične infrastrukture u Srbiji, i sve to uz tesnu saradnju sa zemljama regiona.

Drugi faktor koji bi trebalo razmotriti je uloga privatne bezbednosti u Srbiji, koja se sve više razvija. Za to postoje tri glavna razloga. Posle 18 godina, privatno obezbeđenje u Srbiji je konačno ušlo u pravne tokove; trenutno je u proceduri usvajanje specijalnog zakon o privatnoj bezbednosti. Takođe, Srpsko udruženje preduzetnika u privatnoj bezbednosti i Udruženje za privatno obezbeđenje pri Privrednoj komori Srbije sve više podižu svest o značaju privatne bezbednosti i o neophodnosti da se ona profesionalizuje i standardizuje. Konačno, Konfederacija evropskih službi privatnog obezbeđenja EU (Confederation of European Security Services – CoESS) pruža značajnu pomoć srpskoj privatnoj bezbednosti kako bi se uklopila u evropski model. Privatna bezbednost u zaštiti kritične infrastrukture još uvek nije dostigla svoj puni potencijal u Srbiji. Primeri najbolje prakse koji su razmotreni u beloj knjizi Konfederacije evropskih službi privatnog obezbeđenja (CoESS), uključujući i smernice za uspostavljanje partnerstva između privatne i javne bezbednosti i primere primene u Ujedinjenom Kraljevstvu, Nemačkoj i dr. zemljama, mogu biti veoma korisni primeri ovog partnerstva u sektoru bezbednosti ne samo za Srbiju, već i za druge zemlje regiona [Davidović et al. 2012]. Na kraju, strategija zaštite kritične infrastrukture, koja je data u Direktivi ECI i koja je usklađena sa privatnom bezbednošću u EU, za koju je zadužena Konfederacija evropskih službi privatnog obezbeđenja (CoESS), zajedno sa smernicama za partnerstvo između javne i privatne bezbednosti, takođe, mogla bi da stvori uslove za zajednički sistem zaštite kritične infrastrukture na Zapadnom Balkanu. Osim službi privatnog obezbeđenja, ovaj proces bi trebalo da uključi i odgovorne rukovodioce (vlade, političari), vlasnike i zaposlene u kritičnoj infrastrukuturi i sve druge zainteresovane.

Globalizacija i nagli i brzi tehnološki razvoj doveli su do sve većih rizika u informaciono-komunikacionim tehnologijama i do povećanog broja sajber napada, koji bi potencijalno mogli da unište ili da prouzrokuju probleme u funkcionisanju kritične infrastrukture jedne zemlje. Usled zastupljenosti IKT-a u gotovo svim aspektima svakodnevnog života i rada, veliki broj zemalja je već uspostavio mehanizme koji im omogućavaju da reaguju u slučaju sajber incidenata. Ovi mehanizmi uključuju saradnju između predstavnika države, s jedne strane, i privatnog sektora, akademske zajednice i civilnog društva, s druge. Kao i mnoge druge zemlje Balkana, Srbija zaostaje u ovoj oblasti. Zaposleni u elektronskim komunikacionim mrežama su obavezni da štite svoje IKT resurse, ali ove mere sigurno nisu dovoljne da pruže potpunu bezbednost kritične infrastrukture jedne zemlje od sajber

napada. S druge strane, imajući u vidu da je veliki deo kritične infrastrukture u rukama privatnika (privatnih kompanija) i da država ne može pružiti dovoljan nivo bezbednosti, neophodno je da se uspostavi poseban vid saradnje između državnog i privatnog sektora. Na globalnom nivou, EU je objavila da će revidirati regulatorni okvir elektronskih komunikacija i usluga s ciljem da se ojača bezbednost i integritet komunikacionih mreža. U ovom trenutku, teško je uočiti neku sličnu aktivnost institucija u Srbiji [Todorovic et al. 2016].

V. INTERNACIONALIZACIJA ZAŠTITE INFRASTRUKTURE U FIZIČKOM I SAJBER PROSTORU

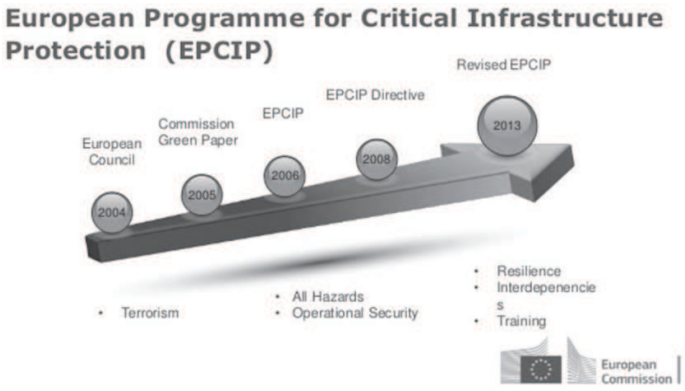
Napori da se zaštiti kritična infrastruktura na Balkanu svakako bi trebalo da budu povezani sa odgovarajućim aktivnostima EU, ali iskustva i *know-how* iz drugih oblasti moraju da se uzmu u obzir, takođe. U ovom slučaju, to bi se odnosilo barem na SAD, kao globalnog pionira u mnogim oblastima, i Kinu, kao novu silu u usponu. Ovo je posebno značajno jer brzi tempo uvođenja tehnoloških inovacija i njihove primene uslovljava digitalnu transformaciju u sistemima zaštite kritične infrastrukture, i u isto vreme povećava broj sajber pretnji.

Da krenemo od SAD, Direktiva američkog predsednika PDD-63, maj 1998. [Web link 1] uspostavila je nacionalni program „Zaštite kritične infrastrukture". Ona je ažurirana 17. decembra 2003, kada je predsednik Buš potpisao Direktivu američkog predsednika u oblasti unutrašnje bezbednosti HSPD-7 za *identifikaciju, određivanje prioriteta i zašititu kritične infrastrukture* [Web link 2]. Ključni elementi ove američke paradigme [Web link 3] su: (i) Plan osiguranja nacionalne infrastrukture / Plan zaštite nacionalne infrastrukture (usklađeni napori federalne vlade i privatnog sektora) i (ii) Sektor za kritičnu infrastrukturu Ministarstva odbrane, koji je usredsređen na radove od javnog značaja. U okviru najnovijih dešavanja, 2013. je *predsednikovom izvršnom naredbom* 1363 („Poboljšanje sajber bezbednosti kritične infrastrukture") zadužen Nacionalni institut za standarde i tehnologiju SAD (U.S. National Institute of Standards and Technology – NIST) da rukovodi razvojem okvira za smanjenje bezbednosnih rizika u sajber prostoru u okviru kritične infrastrukture, s ciljem da se dobije povratna informacija od svih učesnika u javnoj i privatnoj bezbednosti i uključe primeri najbolje prakse u što većoj meri [Web link 4]. Nacionalni institut za standarde i tehnologiju SAD je 2014. objavio Okvir sajber bezbednosti u cilju zaštite kritične

infrastrukture koji je opisan kao „set industrijskih standarda i najboljih praksi zasnovan na rizicima koji bi trebalo da pomognu organizacijama da upravljaju bezbednosnim rizicima u sajber prostoru" [Web link 5]. Rad na poboljšanju i osavremenjivanju ovog Okvira se nastavlja.

U Evropi se paralelni dokument „Evropski program za zaštitu kritične infrastrukture" (*European Programme for Critical Infrastructure Protection* – EPCIP) [Web link 6] odnosi na doktrinu ili specifične programe koji su rezultat Direktive Evropske komisije EU COM (2006) 786, koja određuje evropsku kritičnu infrastrukturu koja bi, u slučaju incidenta, ili napada mogla da ima uticaj i na zemlju u kojoj se nalazi, kao i na bar još jednu državu EU. Države članice su se obavezale da usvoje ovu Direktivu 2006 i uključe je u svoja nacionalna dokumenta. Ključni stub ovog programa je Direktiva 2008 o evropskim kritičnim infrastrukturama (Slika 3). Ona uspostavlja proceduru za identifikovanje i određivanje Evropske kritične infrastrukture (European Critical Infrastructures – ECI) i za zajednički pristup u njenoj zaštiti. Direktiva obuhvata nekoliko sektora i primenjuje se samo u oblasti energetike i transporta. Metodologije koje se koriste na evropskom nivou ne mogu da pariraju, u smislu uspešnosti i sveobuhvatnosti, odgovarajućim segmentima u SAD. Naredni projekti bi trebalo da prevaziđu taj jaz kroz blisku saradnju sa EPCIP ili ENISA, kao i sa evropskim grupama eksperata npr. JRC.

Slika 3. *Zaštita kritične infrastrukture u EU*



Možda najnapredniji deo zaštite u EU je upravo u sajber prostoru. Direktivu za bezbednost mreža i informacionih sistema (The Directive on security of network and information systems – the NIS Directive) usvojio je Evropski parlament 6. jula 2016. i ona je stupila na snagu avgusta 2016. Ova Direktiva pruža zakonske okvire za jačanje ukupnog nivoa sajber bezbednosti.

Međutim, imajući u vidu stalnu evoluciju sajber sistema i odgovarajućih pretnji, neophodno je odmah primeniti Direktivu. Kada je reč o neumitnim rokovima do kada je neophodno Direktivu preneti na nacionalni nivo (9. maj 2018) i do kada bi trebalo identifikovati pružaoce usluga (9. novembar 2018), Komisija je septembra 2017. usvojila Saopštenje koje ima za cilj da podrži države članice u njihovim naporima da primene Direktivu brzo i koherentno širom EU [Web link 7]. U tom smislu, ona, takođe, predviđa 'NIS priručnik' koji pruža praktične informacije državama članicama, npr. tako što će dati primere dobre prakse zemalja članica i tako što će ponuditi objašnjenja i obrazloženja za specifične odredbe ove Direktive kako bi što bolje objasnili kako to izgleda u praksi. NIS priručnik bi trebalo da ima sledeće karakteristike, između ostalog: da bude od praktične koristi i pruži uputstvo za globalnu primenu, uključujući nove strategije u razvoju; da uputi na postojeće modele, alate za procenjivanje i druge priručne alate; da obezbedi propratne alate za procenjivanje kako bi se lako identifikovale ključne oblasti u kojima bi trebalo da dođe do poboljšanja i kako to postići; da definiše indikatore najbolje prakse da bi se procenilo poboljšanje nakon određenog vremena, itd. [Web link 8].

Kako bi se suočila sa problemima u sajber prostoru, EU sve vreme koordinira različite aktivnosti. Jedan dobar primer je Sajber Evropa 2016, četvrta panevropska vežba u oblasti sajber kriza koju je organizovala Agencija za mreže i informacionu bezbednost EU (the European Union Agency for Network and Information Security – ENISA). Ova vežba je simulirala realnu krizu koja se produbljivala tokom 6 meseci i koja je, na kraju, svoj vrhunac dostigla 13. i 14. oktobra 2016. u trajanju od 48 sati. Ciljevi ove vežbe su bili da se ojača prevencija, odgovor i sprečavanje krize velikih razmera, sa posebnim akcentom na saradnji na nacionalnom i međunarodnom nivou i adekvatnim bezbednosnim sposobnostima učesnika i organizacija iz privatnog i javnog sektora iz svih 28 država članica EU (uglavnom iz IKT sektora). Pored toga, naučene su mnoge lekcije iz upotrebe prototipičnih platformi koje je razvila ova Agencija kako bi se omogućila saradnja na nivou EU; one će se pozitivno odraziti na razvoj infrastrukture za saradnju tokom kriza na nivou EU koji finansira Instrument za povezivanje Evrope (Connecting Europe Facility – CEF) [ENISA, jun 2017].

Još jedan koristan primer iz EU se odnosi na ubrzan rast tržišta sajber osiguranjem. Očekuje se da će se ono i dalje širiti sa usvajanjem GDRP i Direktive NIS koje će podsticati relevantne organizacije da traže način za transfer rezidualnog rizika. Međutim, industrija uviđa nedostatak zajedničkih elemenata u jeziku procene rizika. Dok su neke inicijative počele da poprimaju određenu formu, industrija, zbog čitavog niza razloga, još uvek mora da preduzme niz značajnih koraka ka usklađivanju. Prateći potrebe,

ENISA je objavila izveštaj koji predlaže dva seta preporuka, jedan za industriju i jedan za kreatore politike u različitim oblastima kako bi podržala ovaj prelazak na harmonizaciju jezika, a da pri tom ne guši inovacije. Industrija je ohrabrena da standardizuje jezik politike date oblasti i upitnika, da promoviše razmenu podataka među svim učesnicima, da razvija svoje standarde, da razvije unutrašnju stručnost u oblasti sajber bezbednosti, da doprinese prikupljanju podataka o mogućim lošim scenarijima, ponudi rešenja za regulativu u oblasti informacione bezbednosti i privatnosti, da usvoji sektorski pristup usklađivanju jezika, da zadovolji potrebe SME tržišta i poboljša kvalitet podataka tako što će integrisati raznovrsne izvore. Rukovodioci i političari EU i država članica su ohrabreni da stvore minimalne standarde, da iskoriste predstojeće obavezne šeme o izveštavanju o incidentima kroz Direktivu NIS i GDPR kako bi došli do smislenih podataka, kreirali centralni repozitorij podataka o incidentima za EU, podigli svest o neophodnosti podizanja nivoa potražnje i zrelosti kupaca i razvili smernice za sajber osiguranje [ENISA, November 2017].

Slika 4. *Internacionalizacija zaštite kritične infrastrukture*
[Web link 10]

	U.S.	E.U.	China
Primary CIP Policy Drivers	Executive Order and NIST Cybersecurity Framework	NIS Directive (Law)	China Cybersecurity Law, Draft CIIP Regulation, Cross Border Data Transfer Regulation, Cybersecurity Review Regulation, MLPS
Private Sector Participation During Legislation	Yes	Yes	No
Primary Legislation Feedback Channel(s)	Workshops and Request for Information (RFI)	Public Consultations; Surveys	30-Day Public Comment Period
Risk-Based Definition of Critical Infrastructure	Yes	Yes	Yes
Data and Operation Residency Requirements	No	No	Yes
Endorsement of Global Standards	Yes	Yes	No[19]

U Kini, Državni savet je objavio 27. decembra 2017. petogodišnji plan za nacionalnu informatizaciju (2016–2020). Pema ovom planu, Kina će uložiti značajne resurse u razvoj najnovijih informacionih tehnologija, uključujući i 5G bežične sisteme, IPv6, pametnu proizvodnju, računarstvo u oblacima i internet stvari. Ovaj plan je usmeren na sajber bezbednost, unapređenje zakona i regulative u odgovarajućim oblastima, uspostavljanje sistema upozorenja na rizike i mehanizama za vanredne situacije [Web link 9]. U okviru sprovođenja Zakona o sajber bezbednosti, koji je stupio na snagu 1. juna 2017, Administracija za sajber prostor Kine (Cyberspace Administration of China – CAC) dala je nacrt Uredbe o zaštiti kritične infrastrukture na javnu raspravu 11. jula 2017. Ona se sastoji od 8 poglavlja i 55 članova koji su napisani, prema pravilima, i „sa ciljem da se obezbedi bezbednost kritične informacione infrastrukture i u skladu sa Zakonom o sajber prostoru Kine".

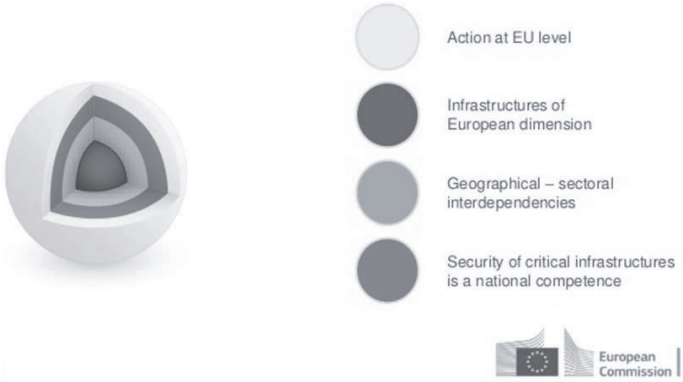
Kao što se može videti, SAD, EU i Kina ostaju na svojim formativnim nivoima razvoja svojih pristupa zaštiti kritične infrastrukture. Pored drugih razlika u ovom pristupu, vredi pomenuti one koji se odnose na ulogu privatnog sektora. Tradicionalni činioci kritične infrastrukture su u privatnom vlasništvu u velikoj meri u SAD i u nekim zemljama EU, dok su većina aktera u sličnim sektorima u okviru zaštite kritične infrastrukture u Kini u vlasništvu države, osim sektora Internet mreže (Internet web). SAD i EU promovišu ideju o učešću privatnog sektora u ovom zakonodavnom procesu, i, zauzvrat, privatni sektor smatra da je ova podrška, zapravo, njihova obaveza da daju svoje mišljenje i iznesu svoja očekivanja od mera u oblasti zaštite kritične infrastrukture i njihove primene. Kineska vlada smatra da je sve veća transparentnost veoma važna. Bez obzira na sastav i geografsku lokaciju aktera kritične infrastrukture i onih koji su zaduženi za tehnologiju, veoma je važno da državna politika u oblasti zaštite kritične infrastrukture ostane „fleksibilna, podobna za gradiranje, i tehnološki neutralna" [Web link 10]. Slika 4 predstavlja pregled različitih pristupa zaštiti kritične infrastrukture onako kako ih koriste vlade SAD, EU i Kine.

VI. ZAŠTITA KRITIČNE INFRASTRUKTURE NA BALKANSKOM RASKRŠĆU

Kada sve bude funkcionisalo, različiti delovi projekata u okviru Inicijative P&P će biti međusobno zavisni, direktno ili indirektno. Po nastanku ozbiljnih problema u nekom od segmenata kritične infrastrukture, njihova međuzavisnost bi mogla da prouzrokuje ozbiljne prekide u povezanoj strukturi P&P unutar Balkana i šire u Evropi. Koncept P&P pokriva veliku oblast i niz

zemalja, sa različitom morfologijom i klimom, stepenom razvoja, zakonodavstvom, navikama i drugim značajnim parametrima. Kao što je ranije pomenuto na primerima iz EU i drugih delova sveta, kompleksan sistem kao što je P&P je, zajedno sa postojećom infrastrukturom, podložan pojavi brojnih slabosti i rizika koji bi zahtevali detaljno planiranje i dobru koordinaciju aktivnosti. EU pokušava da reši i izbalansira jedan integrisani pristup procesu zaštite kritične infrastrukture u pogledu individualnih karakteristika i kompetencija država članica (Slika 5).

Slika 5. *Pristup zaštiti kritične infrastrukture u EU*



Imajući u vidu razlike među zemljama na Balkanu, u pogledu različitog istorijskog, političkog i tehnološkog razvoja, izuzetno je značajno da se postigne saglasnost i da se uspostavi zajednički pristup zaštiti kritične infrastrukture u regionu. Zajednički pristup bi trebalo da pokrije sve nivoe, od politika do primene, sa posebnim akcentom na jurisdikciji i finansijama (npr. u pomenutom primeru sajber osiguranja, bilo bi teško, ali značajno, definisati uloge svih aktera u kritičnoj infrastrukturi, interese i obaveze vlasnika kritične infrastrukture i osoblja kako bi se procenila odgovornost i dao savet za upravljanje korporativnim rizicima). Međutim, pre nego što se počne sa realizacijom tako ambicioznog, ogromnog i dugoročnog zadatka, kao što je stvaranje zajedničke strategija zaštite kritične infrastrukture, zemlje koje učestvuju u Inicijativi P&P trebalo bi da se slože, zajedno sa Kinom, o zajedničkoj platformi za funkcionisanje zaštite kritične infrastrukture.

Još jedan aspekt koji ne sme ostati zanemaren je činjenica da zaštita kritične infrastrukture nije jednostavan zadatak koji treba pokrenuti, uraditi i završiti, već da je to jedan kontinuirani proces. Samo ako se usredsrede na proces zaštite kritične infrastrukture kao na jedan kontinuum, svi akteri i zainteresovani mogu bolje planirati i upravljati tekućim ciklusom

zaštite kritične infrastrukture, i obezbediti da svi učesnici razmenjuju naučene lekcije u daljem planiranju svojih aktivnosti, funkcionisanju i investiranju. Takođe je važno napomenuti da ne postoji neka specifična oblast koja se zove zaštita. Zaštita je skup svih sposobnosti i funkcija koje, uzete kao celina, pomažu da se smanji rizik, poveća otpornost i obezbedi funkcionisanje ključnih sistema, usluga i funkcija [Microsoft 2014]. Što se pre zemlje na Balkanu slože u tome kako da zajedno zaštite kritičnu infrastrukturu – to bolje.

VII. ZAKLJUČAK I NAREDNI KORACI

Iako se možda čini da je najočiglednije rešenje za Srbiju i Balkan usvajanje sistema za zaštitu kritične infrastrukture koji već postoji u EU, to nije baš tako jednostavno. Kao što je rečeno u prethodnim delovima, EU još uvek ima određenih nedoumica u vezi sa zaštitom kritične infrastrukture, uglavnom zbog razlika među državama članicama EU. P&P uvodi dodatne razlike i novine u pogledu kompetencija, međuzavisnosti i zakonodavnih pitanja od značaja za zaštitu kritične infrastrukture. Stoga, pošto su Inicijativa P&P i Kina uključene u ovu jednačinu, izbor najbolje zajedničke platforme za zaštitu kritične infrastrukture postaje još složeniji i osetljiviji. Neko bi mogao da kaže da bi Republika Srbija, zbog svog geopolitičkog položaja u regionu, specifičnog istorijskog nasleđa i tekućih međunarodnih političkih odnosa, mogla da bude idealan kandidat da predvodi razvoj zajedničke platforme zaštite kritične infrastrukture na Balkanu. To bi se poklopilo sa zadatkom koji predstoji Srbiji da osavremeni i kompletira svoje planove i zakone u oblasti zaštite kritične infrastrukture.

Štaviše, neprijatelji nastavljaju da razvijaju nove načine i metode napada, prekidaju i onesposobljavaju funkcionisanje kritične infrastrukture uprkos različitim merama zaštite koje se kontinuirano usavršavaju i primenjuju. Procena rizika je značajno napredovala tokom prethodnih godina, ali rešenja bazirana na riziku imaju tendenciju da se fokusiraju na procenu i jačanje komponenata kompleksnih sistema u okviru specifičnih pretećih scenarija. Nemogućnost da se ili u potpunosti predvide pretnje, ili da se obuhvati rasprostranjenost i raspon incidenata, uključujući i prirodne uzroke i greške, dovela je do značajnog interesovanja za upravljanje kritičnom infrastrukturom koje se zasniva na izgradnji otpornosti [Todorovic and Bletas 2016]. Možda bi paralelno sa aktivnostima na unapređenju zaštite kritične infrastrukture u Republici Srbiji bilo dobro da se radi i na otpornosti kritične infrastrukture, kao trenutno najsavremenijem konceptu

za obezbeđivanje kontinuiteta kritične infrastrukture i za zaštitu društva i ljudi koji zavise od njenog funkcionisanja.

LITERATURA

1. Bastian, J. (2017). The potential for growth through Chinese infrastructure investments in Central and South-Eastern Europe along the "Balkan Silk Road", Report prepared for the European Bank for Reconstruction and Development – EBRD (with funding from the Central European Initiative), Athens / London, July 2017.
2. Davidović, D., Kešetović, Ž., Pavicevic, O. (2012). National Critical Infrastructure Protection in Serbia: The Role of Private Security, *Journal of Physical Security*, 6(1), pp. 59–72.
3. ENISA (June 2017). Cyber Europe 2016: After Action Report, Findings from a cyber crisis exercise in Europe, European Union Agency for Network and Information Security (ENISA), Heraklion, Greece.
4. ENISA (November 2017). Commonality of risk assessment language in cyber insurance – Recommendations on Cyber Insurance, European Union Agency for Network and Information Security (ENISA), Heraklion, Greece.
5. Herrmann, J. W. (2015). Engineering Decision Making and Risk Management, John Wiley & Sons, Inc., Hoboken, New Jersey, US.
6. Kešetović Ž., Putnik N., Rakić M. National Critical Infrastructure Protection – Regional Perspective, University of Belgrade – Faculty of Security Studies, Belgrade, Serbia.
7. Microsoft, (2014). Critical Infrastructure Protection: Concepts and Continuum, White Paper, Microsoft Corporation.
8. Ophandt J. A. (2010). Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield. Duke Law Technol Rev, Page 7.
9. Todorovic B., Bletas A. (2016). Resilience planning for critical infrastructure linked to "One Belt One Road" initiative in Balkans and Greece, The Belt and Road: The Balkans Perspective – Political and Security Aspects, University of Belgrade – Faculty of Security Studies, Belgrade, Serbia.
10. Todorovic B., Trifunovic D., Jonev K., Filipovic M. (2016). Chapter 22 – Contribution to Enhancement of Critical Infrastructure Resilience in Serbia, Resilience and Risk – Methods and Application in Environment, Cyber and Social Domains, Proceedings of the NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, Azores, Portugal, 26–29 June 2016.

11. Web link 1: https://en.wikipedia.org/wiki/Presidential_directive
12. Web link 2: https://en.wikipedia.org/wiki/Critical_infrastructure_protection#-cite_note-HSPD7bush-2
13. Web link 3: https://www.dhs.gov/water-and-wastewater-systems-sector
14. Web link 4: https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
15. Web link 5: https://www.nist.gov/cyberframework
16. Web link 6: https://en.wikipedia.org/wiki/European_Programme_for_Critical_Infrastructure_Protection
17. Web link 7: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
18. Web link 8: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf
19. Web link 9: http://english.gov.cn/policies/latest_releases/2016/12/27/content_281475526646686.htm
20. Web link 10: https://www.scribd.com/document/364544590/A-Comparative-Study-The-Approach-to-Critical-Infrastructure-Protection-in-the-U-S-E-U-and-China#from_embed