351.824.11:327(510)
https://doi.org/10.18485/fb_pip_rio.2019.ch12

Petar Stanojević
Fakultet bezbednosti Univerziteta u Beogradu

Zoran Jeftić
Fakultet bezbednosti Univerziteta u Beogradu

Goran Mandić
Fakultet bezbednosti Univerziteta u Beogradu

Kontinuitet funkcionisanja kritične infrastrukture u okviru projekta „Pojas i put"[1]

Sažetak

Zaštita kritične infrastrukture tema u preseku između prirodnih nesreća, politike, privatnog poslovanja, tehnologije i rizika. Projekat „Jedan pojas i jedan put" razvija veze između azijskih zemalja (Kine), preko Afrike, do Evrope, uključujući mnogobrojne luke, železničke puteve i autoputeve, brane, telekomunikacione institucije, naftne gasne cevovode, energetsku industriju i mnoge druge kompanije. Rizici koji utiču na ova preduzeća mogu biti kako eksterni (teroristi, prirodni hazardi, sajber napadi..) tako i interni (tehnološke nesreće, ljudske greške, zagađenja, bezbednost i zdravlje na radu, itd). Da bi se održali maksimalni profiti i ostvario povrat ulaganja, nove investicije zahtevaju kontinuitet, stabilnost i operativnu izvrsnost u njihovim poslovnim funkcijama. Nažalost, ugrožavanja mogu biti velikog obima i mogu imati različite izvore i motive. Venecuela i njihov sistem napajanja električnom energijom samo je poslednji primer uključivanja više aktera.

Skoro sve zemlje koje su uključene u projekat „Jedan pojas i jedan put" klasifikovane su kao zemlje u razvoju, pa su njihove mogućnosti i sredstva u ograničavanju potencijalnih nesreća ograničene. U isto vreme, neke od tih zemalja su članice Evropske unije (EU), gde je zaštita kritične infrastrukture i HSE (zdravlje, bezbednost i životna sredina kao poslovne funkcije) na visokom nivou razvijenosti ili su barem strogo regulisane. Projekat „Jedan pojas i jedan put" povezuje

[1] Ovaj rad deo je istraživačkog projekta III 47029, MESTD of RS.

zemlje, infrastrukture i kompanije i daće pun efekat ako su sve karike u potpunoj funkciji. Uzimajući u obzir to da su zaštitne mere jake onoliko koliko su slabe karike, javlja se potreba za razvijanjem Sveobuhvatnog pristupa.

Sveobuhvatni pristup mora da uključi zemlje, privatne entitete, sve državne i nadnacionalne aktere, kao i privatne, poslovne, sigurnosne i naučno-akademske organizacije u zaštiti kritične infrastrukture. On mora da ima proaktivnu, preventivnu, ali i poboljšanu ulogu otpornosti. Potrebna je istovremena zaštita kako od spoljašnjih tako i od unutrašnjih opasnosti. U okviru spoljne bezbednosti potreban je novi model zaštite koji će obuhvatiti vojsku, obaveštajni sistem, policiju, kompanije privatnog obezbeđenja i civilnu zaštitu. Na nivou pravnog lica (unutrašnja bezbednost), potrebna su nova poboljšanja HSE (bezbednosti i zdravlja na radu i zaštite životne sredine), da bi se postigla sinergija.

Da bi se postigao Sveobuhvatni pristup potrebna je konstruktivna saradnja zasnovana na zajedničkom regulativnom okruženju, standardima, uzajamnom poverenju, obuci, istraživanju i razvoju, razmeni informacija, alatima i merama i koordiniranoj akciji, koji su ključni faktori u smanjenju rizika ugrožavanja i zaštite kritične infrastrukture.

Ovaj rad se bavi potrebom da se razvije Sveobuhvatni pristup u zaštiti kritične infrastrukture u okviru projekta „Jedan pojas i jedan put", sa fokusom na očigledne potrebe i načine osnivanja. Uspostavljanje trajnih organa, koji će imati zadatak da istraže prilike i opcije, treba da bude prvi korak u jačanju saradnje. Model Evropske unije u zaštiti kritične infrastrukture takođe je u centru interesovanja u kontekstu uspostavljanja pravnog okvira.

Ključne reči:

kritična infrastruktura, kontinuitet poslovanja, projekat „Jedan pojas i jedan put", Sveobuhvatni pristup

1. UVOD

Zaštita kritične infrastrukture je savremena potreba i paradigma. Trenutno možemo da uočimo malu razliku po zemljama, u njihovim definicijama sektora kritične infrastrukture, kao i onoga što smatraju kritičnom infrastrukturom, pri čemu većina uzima u obzir sledeće: energiju, transport, poljoprivredu i hranu, vodu, javno zdravlje i bezbednost, hitne službe, vladu, odbrambenu industriju, informacije i telekomunikacije, bankarstvo i finansije, zaštitu životne sredine, industriju, proizvodnju i nauku. U slučaju „Pojas i put" luke, aerodromi, železničke pruge, autoputevi, distribucija električne energije, industrija gasa i nafte od primarne su važnosti, ali, takođe, uzimaju se u obzir i brojne druge organizacije koje su okrenute ka razvoju i proizvodnji.

Sve zemlje su svesne značaja koji ima zaštita kritične infrastrukture i, uprkos različitim shvatanjima, postoji svest o grupi pitanja koja su zajednička, ali je praksa povezana sa nedostatkom resursa i nadležnosti. Propisi, po zemljama, nisu slični i nisu na nivou moguće promenjivosti koju zahtevaju

moderni uslovi. Uprkos razlikama, propisi se podudaraju u nekim slučajevima. Ovaj problem je najviše zastupljen u državama u razvoju. Većina zemalja, učesnica u projektu „Pojas i put", u toj su grupi. Na drugoj strani imamo članice Evropske unije koje učestvuju u ovom projektu i koje imaju visokorazvijen pravni sistem.

Razvoj infrastrukture finansiran je pretežno ili putem kredita ili direktnim investicijama. Manji prekidi u funkcionisanju objekata mogu da degradiraju sistem i izazovu ekonomske gubitke. Zemlje u razvoju su posebno ranjive i osetljive na moguće finansijske gubitke. Poslednji primer toga je Crna Gora, gde se vodi javna rasprava o mogućem bankrotu države, zbog duga koji imaju prema Kini, zbog izgradnje autoputa [27]. S obzirom na to da projekti koji se realizuju u okviru predmetne inicijative nisu uvek isplativi, ili će biti tek u budućnosti, dodatni prekidi mogu dovesti ne samo do ekonomskih nego i do političkih problema. Jedan od takvih primera je železnička pruga Beograd – Budimpešta, koja može imati ekonomski značaj samo u slučaju značajnog povećanja saobraćaja i to tek nakon dužeg vremena.

Problem sa kritičnom infrastrukturom je i u velikoj zavisnosti između različitih sektora. Na primer, ako se dogodi teroristički napad na neki od sektora, poput energetskog sektora, to će imati posledice na sve ostale sektore. Međuzavisnost među sektorima kritične infrastrukture mora se uzeti u obzir zbog uspostavljanja zaštitnih programa. Može se reći da je uvek prisutan višenivojski ili domino efekat. Posledice na primarnom subjektu se prenose na drugi, sa njega na treći itd., sve dok veoma mnogo subjekata biva involvirano. Ne treba zanemariti ni aktualizaciju asimetričnih oblika ugrožavanja države i kritične infrastrukture. Najnoviji primer jeste prekid sistema snabdevanja električnom energijom u Venecueli, što je imalo ogromne posledice za celokupno društvo. Efekat na više nivoa ili domino efekat zahteva uvek dodatne kontramere i resurse koji se ne mogu dobiti samo od jedne kompanije i stoga zahteva angažovanje eksternih, pretežno državnih snaga.

Zlonamerne radnje nisu jedini uzrok akcidenata. Zajedno s akcidentima, prouzrokovanim zbog propusta u poslovnom upravljanju i tehnološkim propustima, mogući uzrok nesreća su i prirodne katastrofe.

Jedna od ključnih uloga menadžmenta je upravljanje rizikom. Vlasnici (javni ili privatni) i menadžeri imaju zadatak da obezbede poslovnu stabilnost i kontinuitet, kao i da osiguraju sigurne radne uslove za svoje zaposlene i zaštitu životne sredine. Zemlje u razvoju, koje karakterišu slabe institucije, nedostatak kompetencija, finansijskih ciljeva, kao i zakonodavstva i stabilne ekonomije, imaju veliku potrebu da pruže bolje javne usluge i poboljšaju društveno-ekonomske uslove. Ove zemlje promovišu javno-privatno

partnerstvo, pored strogo javnog (državnog) i privatnog vlasništva i profesionalnog menadžmenta u kritičnim infrastrukturama.

Da bi se oduprli savremenim globalnim pretnjama i opasnostima i da bi se poboljšala bezbednosna situacija, potreban je intenzivan nivo integracije i interakcije između nacionalne i nadnacionalne strukture bezbednosti i međuzavisnosti nacionalnih, regionalnih i multilateralnih tela. Međutim, uloga države kao bezbednosnog entiteta u međunarodnim odnosima ostaje ključna i neophodna.

2. MEĐUNARODNI PRISTUPI I PROPISI

Sjedinjene Američke Države imaju Nacionalni plan zaštite infrastrukture od 2006. godine [1]. Infrastruktura i ključni resursi podeljeni su na osamnaest sektora. Ovi sektori infrastrukture su poljoprivreda i zaštita hrane, postupanje sa vodom za piće, energija/ informacione tehnologije/telekomunikacije, transportni sistemi, odbrambena industrija, javno zdravstvo, bankarstvo/finansije, poštanski saobraćaj i kritična proizvodnja. Ključni resursi su nacionalni spomenici/ikone, vladini objekti, objekti za hemijsku proizvodnju, komercijalni objekti, hidroelektrane i brane, hitne službe i komercijalni nuklearni reaktori, materijali i otpad. Samo transportni sistem, koji je veoma raznovrstan, pokriva: 5.000 javnih aerodroma, 120.000 milja glavnih puteva, 590.000 mostova, 2.000.000 milja cevovoda, 300 luka, 500 glavnih, gradskih i javnih ukrštenih puteva. Poslednji primeri podsećaju na projekat „Jedan pojas i jedan put" i njegovu veličinu.

Od 2004. godine Evropska komisija gradila je „Evropski pristup" sa idejom stvaranja Evropskog programa za kritične infrastrukture (EPCIP) [2, 3, 4, 5, 6, 7]. Cilj je da se podrže kompanije i vlade u EU u njihovim strategijama bezbednosti. On nastoji da obezbedi svestrane međusektorske pristupe (www.ec.europa.eu). Uredba pravi jasnu razliku između kritičnih infrastruktura država članica i evropskih kritičnih infrastruktura (infrastrukture važne za najmanje dve zemlje). Odgovarajuće direktive Evropske komisije su ključni elementi u stvaranju zajedničkog zakonodavnog okvira. "Contact Point" sastanci Evropskog programa za kritične infrastrukture organizuju se radi razmene informacija između država članica EU (www.ec.europa.eu). EU finansira i sprovodi multidisciplinarne studije kako bi identifikovala potrebe adekvatne zaštite kritične infrastrukture.

Član 2 Direktive (2008) navodi da se uticaj mora proceniti u smislu unakrsnih kriterijuma (infrastruktura međuzavisnosti). To znači da, kada kritične infrastrukture predstavljaju suštinske ili vitalne vrednosti u nekoliko

zemalja EU, bezbednosne strategije dobijaju evropsku dimenziju. Trenutni pristup se odnosi na to da evropske strategije treba da se fokusiraju na sisteme umesto na sektore (kritične infrastrukture su često suviše velike i složene). Evropski program za kritične infrastrukture odabrao je četiri ključne infrastrukture koje imaju evropsku dimenziju kako bi optimizovale njihovu zaštitu i otpornost. Ovi sektori su "Euro control" (Menadžment mreže za upravljanje vazdušnim saobraćajem u EU), "Galileo" (Globalni satelitski navigacioni sistem), "Electricity Transmission Grid and the European Gas Transmission Network" – mreža za prenos električne energije i Evropska mreža za prenos gasa. Najnoviji (prekogranični ili multilateralni) pristup je važan zbog razmatranja većine napora u okviru projekta „Jedan pojas i jedan put", koji su pretežno međunarodni i razvijaju transportne sisteme.

Jedna od najzanimljivijih programa u okviru EU je Informaciona mreža za upozoravanje za kritičnu infrastrukturu (CIWIN), koja okuplja stručnjake iz EU kako bi pomogli Evropskoj komisiji u uspostavljanju mreža, da bi se olakšala razmena informacija o pretnjama, ranjivosti, merama i strategijama [8]. Jedna od ideja je da se stvori baza znanja o najboljim praksama na evropskom nivou, koja će sadržati preporuke, scenarije i smernice.

EU ima tri glavne strategije zasnovane na gledištu o otpornosti kritične infrastrukture, tj. prevenciji, spremnosti i odgovoru [2]. Prevencija ima za cilj stvaranje alata za procenu rizika i upravljanje rizikom. Privatni sektor mora u tome suštinski da učestvuje. Imajući u vidu činjenicu da obaveštajne informacije imaju ključnu ulogu, uključen je i Centar za analizu obaveštajne službe EU (INTCEN). Strategija pripravnosti i reagovanja zasnovana je na opremanju, obuci, podizanju svesti i vežbama.

U smislu mera zaštite kritične infrastrukture, sve zemlje, uključujući i Republiku Srbiju, moraju: a) identifikovati kritičnu infrastrukturu, b) izraditi mape kritične infrastrukture, c) odrediti mrežu razmene informacija, hijerarhiju i sadržaj, d) obučiti osoblje koje će raditi na poslovima i zadacima u kritičnoj infrastrukturi, e) obučiti osoblje kritične infrastrukture za slučaj krize ili hitne situacije, f) odrediti službenike za vezu u svim kritičnim infrastrukturama i g) razviti Planove zaštite (bezbednosti).

Treba primetiti da je u pogledu industrijske prakse EU uvela integrisani pristup, koji je predstavljen nizom direktiva, među kojima su najvažnije direktive o integrisanom sprečavanju i kontroli zagađenja (IPPC) (Directive 2008/1/EC of 15 January 2008 concerning integrated pollution prevention and control) i Direktiva Saveta (96/82/EC of 9 December 1996) o kontroli opasnosti od velikih udesa koje uključuju opasne materije (takođe poznate kao Seveso II direktiva) [9, 10]. Među nekoliko desetina drugih direktiva, ATEX i PED su možda najvažnije. Ovaj set propisa ima za cilj da smanji

verovatnoću udesa i poboljša otpornost. Prevencija, spremnost, odgovor, dokumentovani pristup, uključenost javnosti i stručna verifikacija su u samom središtu ovog modela. Vlasništvo nije od značaja; svaki akter mora izvršiti svoje zakonske obaveze. Navedene direktive imaju stručna i regulatorna tela u EU, uz učešće skoro svih država članica. Svi rizici moraju biti obuhvaćeni dokumentovanim planovima za zaštitu i hitne slučajeve.

3. VOJSKA, POLICIJA, OBAVEŠTAJNA SLUŽBA, CIVILNA ZAŠTITA, PRIVATNA BEZBEDNOST I ZAŠTITA KRITIČNE INFRASTRUKTURE

Zaštitom kritične infrastrukture štiti se njen ekonomski potencijal. Bezbednost i zaštita kritične infrastrukture je odgovornost vlasnika kompanije i propisana je od strane javnog sektora i vođena stvarnim potrebama, kako bi se sprečili nepotrebni gubici. Strukture bezbednosti kompanija fokusirane su na specifične zadatke zaštite i razvijaju specifična znanja, sposobnosti i resurse. S obzirom na to da kritične infrastrukture mogu biti ugrožene, manje ili više zajedničkim pretnjama, kao što su teroristički napadi, tehnološki udesi i prirodne katastrofe, značaj privatne bezbednosti se povećava posebno zbog specijalizacije i specifičnog sektorskog znanja [11], a korist se sastoji u smanjivanju troškova kompanija zbog veće specijalizacije i boljeg korišćenja resursa.

U većini evropskih zemalja zaštita kritične infrastrukture ocenjuje se kao važan zadatak za privatnu bezbednost. Shodno tome, zaštita kritičnih infrastruktura se generalno smatra odgovornošću koja mora biti podeljena između javnog i privatnog sektora [12]. Kompanije i zaposleni unutar njih moraju da dobiju sertifikat od državnih organa i prođu odgovarajuću obuku, ako žele da pruže usluge privatne bezbednosti [13, 14, 15].

Da bi se poboljšalo efektivno partnerstvo sa kompanijama, privatni sektor bezbednosti trebalo bi da bude angažovan od samog početka, tj. u izradi (konceptualizacija pristupa) i radu na zaštiti kritične infrastrukture [13]. Imajući u vidu činjenicu da se industrija privatne bezbednosti sastoji od korporacija, sektor ima u nadležnosti procenu rizika, identifikovanje bezbednosnih pretnji i razvijanje sektora za specifične obuke.

Obaveštajne službe imaju ključnu ulogu u planiranju i sprovođenju bezbednosnih strategija za kritične infrastrukture.

Savremene vojske imaju pet osnovnih zadataka [16]:

1. Zaštita nezavisnosti države, njenog suvereniteta i teritorijalnog integriteta, a u širem kontekstu i njenih građana;

2. Očuvanje mira na međunarodnom planu ili sprovođenje mira;
3. Humanitarna pomoć u slučaju katastrofa;
4. Zadaci državne bezbednosti i
5. Učešće u izgradnji nacije.

Generalno, to su interni i eksterni zadaci, ili ih neki nazivaju netradicionalnim i tradicionalnim zadacima. Ženevski centar za demokratsku kontrolu oružanih snaga (DCAF) sproveo je istraživanje u 15 zapadnih konsolidovanih demokratija[2] o mogućim unutrašnjim ulogama oružanih snaga. Rezultat je bio da je identifikovano 20 različitih uloga, a deset od njih spada u kategoriju širih zadataka vezanih za sprovođenje zakona. Među tim zadacima je zadatak izgradnje svesti i sigurnosti stanovništva. Samo Luksemburg, Španija i Nemačka nemaju taj zadatak za svoju vojsku. Zaključak je takođe da je u svakoj zemlji vojska uključena u pružanje pomoći u slučajevima prirodnih ili humanitarnih katastrofa. Važno je naglasiti da zaštita kritične infrastrukture nije isključiv zadatak vojnih snaga. Oružane snage se često smatraju poslednjom mogućom merom, aktiviranom na zahtev civilnih vlasti [17].

U istočnoj Evropi[3] kapaciteti civilne zaštite ozbiljno su smanjeni zbog nedostatka finansiranja i promene strateške orijentacije. Kapaciteti vojnih snaga su takođe značajno niži iz istih razloga. U mnogim zemljama policija preuzima odgovornost za vatrogasne i vanredne situacije, kao u Srbiji. Policija i nova vladina odeljenja se bore da dobiju potrebne kapacitete i nadležnosti. Uloge i odgovornosti koje se smenjuju između različitih vladinih odeljenja prouzrokovale su opasne nesporazume i smanjile već neadekvatne kapacitete. U isto vreme verovatnoća i količina mogućih nezgoda u okviru kritičnih infrastruktura nisu smanjene, već, suprotno, povećale su se zbog novih infrastrukturnih objekata i industrijskog razvoja.

Nove pretnje, kao što su one u vezi sa sajber bezbednošću, zahtevaju novu vrstu visokosofisticiranih i obučenih resursa. Sve vladine službe i većina kompanija nemaju takve kapacitete.

Prethodno ukazuje na logičan zaključak, a to je da sve raspoložive snage moraju biti angažovane u rešavanju nezgoda koje se odnose na kritičnu infrastrukturu. Vojska je jedina vladina služba koja može imati neke viškove kapaciteta. Razlog tome pronalazimo u činjenici da se većina vojski u današnjem svetu pripremala za rat velikih razmera u doba hladnog rata.

---

[2] Austrija, Belgija, Danska, Finska, Francuska, Nemačka, Italija, Luksemburg, Holandija, Norveška, Španija, Švedska i Ujedinjeno Kraljevstvo, zajedno sa Sjedinjenim Američkim Državama i Kanadom.

[3] Skoro sve zemlje istočne Evrope učestvuju u inicijativi 16+ i projektu „Pojas i put", koje predvodi Kina.

Takođe, vojska je tradicionalno izvor visokoobučenog i motivisanog osoblja. Novi zadaci dati vojnoj organizaciji zahtevaju novi model organizacije koji se lako prilagođava za sve vrste mogućih situacija i zadataka, kao što je predstavljeno u [18].

Značajno je da su glavne uloge vojnih snaga u novom dobu, kao što je pobeda u ratu očuvanje mira i lokalne i globalne operacije pomoći u slučaju opasnosti, međusobno suprotstavljene i problematične sa stanovišta projektovanja, organizovanja i korišćenja vojnih taktičkih sposobnosti, ako su izložene kao zajednički zahtevi. To sugeriše kreatorima odbrane, posebno za kopnene snage i združene jedinice, da moraju da napuste taktičke vojne organizacije dvadesetog veka i da prepoznaju nove pristupe vojnog angažmana.

Multinacionalna razmena i iskorišćavanje ključnih resursa i infrastrukture, smeštenih u okviru domaće teritorije, takođe, nosi veliki međunarodni rizik, posebno u obliku asimetričnih ili terorističkih akcija. Pitanja implementacije vojnih kapaciteta u prevenciji potencijalne asimetrične ugrožavajuće situacije moraju se posmatrati kao zadaci odbrane nacionalnih i međunarodnih vojnih snaga. U ovom trenutku većina vojnih snaga u malim zemljama nemaju odgovarajući nivo kapaciteta, tehnologija i fleksibilnosti organizacije, da bi se efikasno koristile u različitim misijama, uključujući operacije za civilne hitne slučajeve i rizike za zaštitu infrastrukture.

Mali budžeti opterećuju vojne i druge vladine agencije i institucije i nameću nacionalnim ekonomijama konačno razvijanje zajedničkih, civilnih i vojnih kapaciteta za vanredne situacije, podelu odgovornosti u odbrani, zaštiti mira i sigurnosti u rizičnim situacijama. To podrazumeva odgovarajuće učešće vojnih snaga sa drugim civilnim naoružanim i neoružanim snagama, kao što su civilna zaštita, žandarmerija, policija, specijalne snage ili privatne domaće ili međunarodne bezbednosne jedinice.

Uključivanje vladinih i nevladinih agencija i organizacija u zajedničke vojne formacije zasnovane na situacionoj bazi korisna je i neizbežna praksa, naročito u slučaju nacionalne opasnosti od katastrofa, ali, takođe, može se očekivati i u međunarodnom rešavanju sukoba i održavanju mira. Takođe, resursi za pomoć u slučaju civilnog ugrožavanja treba da budu integrisani u sveobuhvatno planirane operacije za vojne snage i moraju biti sastavni deo paketa borbenih timova.

Vojne organizacije poput NATO-a imaju cilj da zaštite linije snabdevanja energijom. Uloga NATO-a u energetskoj bezbednosti prvi put je definisana 2008. godine na samitu u Bukureštu i od tada je učvršćena [26].

U skladu sa [19]: „U Persijskom zalivu i Izraelu razvijeni su koncepti koji, zajedno sa odgovornošću samih kompanija, obezbeđuju saradnju sa vladom u interesu bezbednosti. Generalno, za zaštitu gasovoda mogu se

angažovati policija i oružane snage. Tamo gde vojska i policija, iz bilo kog razloga, ne mogu da se staraju o bezbednosti gasovoda mogu se angažovati privatne kompanije. Preduzeća – vlasnici gasovoda, odgovorni su svojim partnerima, kupcima i investitorima. Zadaci privatnih bezbednosnih kompanija su da sprovedu strateške konsultacije, procene postojeće rizike i zaštite objekte i zaposlene.

Sigurnosni sistem naftovoda Baku – Tbilisi – Džeihan može poslužiti kao odličan primer modernog pristupa bezbednosti naftovoda. Naftovod je celom dužinom zakopan u zemlju; na površini su samo terminali i kompresorske stanice. Pored toga, obezbeđene su dodatne mere zaštite da bi se instalacija zaštitila od krađe i oštećenja. Naftovod je u potpunosti zaštićen od strane osoblja službe bezbednosti, u upotrebi su i snage za brzo reagovanje, a primenjuju se i savremene tehnike i tehnologije (kao što su optički i slični kablovi).

Prema standardima „Gazproma" („Gazprom"), kompresorske stanice će uvek biti ograđene metalnom mrežom visine dva metra, na čijem vrhu će na obe strane biti tri reda bodljikave žice. Ukupna visina ograde biće dva metra i pedeset centimetara. Za zaštitu i sprečavanje nezakonitog ometanja funkcionisanja kompresorskih stanica kao komponenti linearnog (linijskog) upravljanja cevovodima mora se uspostaviti služba obezbeđenja. Odredbe, grupe i komande službe obezbeđenja obezbeđuju bezbednost kompresorskih stanica i linearnih delova gasovoda. Zaposleni službe obezbeđenja moraju biti posebno obučeni, licencirani da bi se bavili obezbeđenjem i moraju da imaju adekvatnu opremu i oružje. Obezbeđenje kompresorskih stanica mora biti prisutno 24 sata dnevno, naoružano i raspoređeno na stražarskim položajima, a treba da poseduju i odgovarajuću opremu za signalizaciju (alarmi, kamere, itd.).

Za zaštitu gasovoda „Južni tok" predviđano je zajedničko angažovanje Sektora za vanredne situacije Ministarstva unutrašnjih poslova Republike Srbije, Centra za vanredne situacije u Nišu i Vojske Srbije.

Primeri vojnih angažmana, pored njihovih tradicionalnih angažmana, su: a) 2008. godine, oko 1.000 vojnika je upućeno da čuvaju javna mesta označena kao mesta „visokog rizika" (mesta gde se okuplja veći broj građana), kao što su železničke stanice i katedrala Sv. Petra u Rimu i b) više od 3.000 italijanskih vojnih lica bilo je raspoređeno kao podrška policijskim patrolama u borbi protiv kriminala u 2008. [17]

Sve gorenavedeno opravdava potrebu za angažovanjem svih dostupnih resursa u zaštiti kritične infrastrukture. Ovo je mnogo važnije u kompleksnim poduhvatima kao što je projekat „Jedan pojas i jedan put", u kojem zemlje učesnice nemaju dovoljno resursa i kompetencija.

4. NOVI PRAVCI U ZAŠTITI KRITIČNE INFRASTRUKTURE: UVOĐENJE OTPORNOSTI

NIAC je 2009. godine objavio izveštaj studije pod nazivom "Critical Infrastructure Partnership Strategic Assessment Study", koji je imao neke zanimljive rezultate [20]. Fokus se nalazi na značaju otpornosti, za javni i privatni sektor, odnosno u izradi njihovih strategija za procenu rizika. Otpornost infrastrukture je sposobnost da se smanji veličina, uticaj i/ili trajanje događaja koji narušavaju bezbednost. Efikasnost otporne infrastrukture ili preduzeća zavisi od njene sposobnosti da predvidi, apsorbuje, prilagodi i/ili da se brzo oporavi od potencijalnog ugrožavajućeg događaja. Stoga, upravljanje rizikom treba da obuhvati i otpornost kritične infrastrukture.

Tri osobine karakterišu otpornost kritične infrastrukture [20]. Ove karakteristike su sposobnost (održavanje funkcionisanja rada u uslovima krize), snalažljivost (priprema za reagovanje i upravljanje krizom ili poremećajem dok se odvija) i brz oporavak (povratak i/ili rekonstrukcija normalnog poslovanja što brže i efikasnije nakon prekida rada).

Goreobjašnjeni pristup je ono što zemlje u razvoju moraju da razviju kako bi poboljšale troškove/efektivnost svojih sistema za zaštitu kritične infrastrukture.

5. KORPORATIVNA BEZBEDNOST I BEZBEDNOSNI MENADŽMENT (HSSE MANAGEMENT)

Korporativna bezbednost i bezbednosni menadžment (koji se nazivaju i bezbednost i zdravlje na radu – HSSE) imaju glavni cilj da sistematski identifikuju propuste u tehnološkim i upravljačkim aktivnostima i nadgledaju akcije upravljanja kako bi kontrolisali rizike u kompanijama. Cilj je da se sagleda široka slika i prikažu relativni bezbednosni prioriteti i efikasnost korektivnih mera upravljanja.

HSSE utvrđuje bezbednosne politike[4] kompanije kao sastavni deo celokupnog poslovanja. Svaka kompanija mora da implementira sistem koji najbolje funkcioniše u njihovoj specifičnoj situaciji – ne postoji sistem koji je „univerzalan za sve". Na kraju, HSSE postaje uvezan u strukturu organizacije i postaje deo njene kulture. Mnoge vodeće kompanije imaju sličnu HSSE

[4] Pojam „politika" odnosi se na opšte namere, pristupe i ciljeve organizacije, zajedno sa kriterijumima i principima na kojima se temelje akcije i odgovori. Efektivna politika bezbednosti i obezbeđenja postavlja jasan pravac za organizaciju. Ona doprinosi svim aspektima poslovnog delovanja kao deo dokazane posvećenosti stalnom poboljšanju.

strukturu, politike, tehnike koje su zasnovane na standardima upravljanja, kao što su ISO 9001, ISO 14001, ISO 31000, ISO 45001, itd. i integrisani sistem bezbednosnih standarda i direktiva u EU.

Postoje brojni elementi sistema upravljanja bezbednošću i bezbednosnim menadžmentom. Glavni elementi se mogu klasifikovati na sledeći način:

„1. Politika bezbednosti u kojoj se navode obaveze organizacije odgovorne za obezbeđenje i zaštitu;
2. Struktura koja osigurava sprovođenje obaveza obezbeđenja i zaštite;
3. Obuka za zaposlene za bezbedan rad i bez ugrožavanja kako trećih lica tako i zaposlenih;
4. Interna pravila za obezbeđenje i zaštitu koja obezbeđuju instrukcije za postizanje ciljeva i način upravljanja bezbednosnog menadžmenta;
5. Program inspekcije za identifikaciju opasnih uslova i za ispravljanje takvih uslova u redovnim intervalima ili po potrebi;
6. Program za identifikaciju opasnog izlaganja ili rizika od takvog izlaganja radnicima i trećim licima i obezbeđivanje odgovarajuće lične zaštitne opreme kao krajnjeg sredstva u slučajevima kada inženjerske kontrolne metode nisu izvodljive;
7. Istraživanje nesreća ili incidenata radi otkrivanja uzroka bilo koje nesreće, ili incidenta i razvoja hitnih mera za sprečavanje ponovnog incidenta;
8. Spremnost da u vanrednim situacijama razviju, komuniciraju i izvrše planove koji se propisuju za efikasno upravljanje vanrednim situacijama;
9. Ocenjivanje, odabir i kontrola podugovarača kako bi se osiguralo da su podizvođači u potpunosti svesni svojih obaveza vezanih za bezbednost i da ih u potpunosti ispunjavaju;
10. Odbori za bezbednost;
11. Procena opasnosti ili potencijalnih opasnosti vezanih za radni proces i razvoj procedura obezbeđenja i zaštite;
12. Promocija, razvoj i održavanje svesti o bezbednosti i zaštiti;
13. Program kontrole akcidenata i otklanjanja opasnosti, pre izlaganja zaposlenih i trećih lica bilo kojem riziku;
14. Program zaštite radnika od opasnosti po zdravlje." [21]

Sistemi HSSE kompanija su nerazdvojni deo celokupnog sistema bezbednosti i zaštite kritične infrastrukture. Ako ovaj sistem funkcioniše na najbolji mogući način smanjuje se verovatnoća i posledice neželjenih doga-

đaja. Na taj način se čuva značajan deo uvek nedostajućih resursa i finansijskih sredstava, koje stvara država. Zbog toga poboljšanja na nivou kompanija moraju biti neodvojivi deo svakog sistema/organizacije zaštite kritične infrastrukture.

6. SVEOBUHVATNI PRISTUP U OKVIRU ZAŠTITE KRITIČNE INFRASTRUKTURE „JEDAN POJAS I JEDAN PUT"

Zaštita kritične infrastrukture je sama po sebi veoma složena i zahtevna aktivnost. Imajući u vidu raznovrsnost kritične infrastrukture, posebno u projektima koji su veličine kao „Pojas i put", mogu se pojaviti značajni izazovi u zaštiti kritične infrastrukture, kao što su [22]:

- Složenost sistema kritičnih infrastruktura, tako da je gotovo nemoguće zaštititi celokupnu kritičnu infrastrukturu i sastavne komponente, na primer, u sektoru transporta gotovo je nemoguće zaštititi brojne komunikacijske linije koje su duge kilometrima, veliki broj aerodroma, morske luke, brojne mostove i slične građevine.
- Nedostatak nadzora i odgovornosti u sektoru u kojem je angažovano više javnih i privatnih institucija.
- Nedovoljna razmena informacija između angažovanih institucija, što dovodi do nove ranjivosti i uticaja na efikasnost odgovora u zaštiti kritične infrastrukture.
- Složenost znanja s obzirom na veliku količinu posebnih veština.
- Međuzavisnost sektora kritične infrastrukture.
- Nesavršenost alata za analizu rizika za kritične infrastrukture i njihove ranjivosti.
- Asimetrični konflikti su posebno efikasna forma koja može uticati na ranjivost kritične infrastrukture.

Takođe, postoji problem u nepostojanju razumevanja između javnih i privatnih subjekata u percepciji ranjivosti i efikasnosti, jer je glavni cilj privatnog kapitala, efikasnost, uslovljen tržišnim aktivnostima, a ranjivost će se razmatrati samo ako se javlja stvarna potreba da se to učini.

Dodatni problemi se javljaju u a) brzim promenama izvora ugrožavanja i njihove prirode, koja sputava istraživače koji rade na kontramerama, b) jak politički uticaj, jer incidenti mogu uticati veoma destabilizujuće na domaću i međunarodnu javnost, c) u nepredvidivosti životne sredine, jer je nemoguće predvideti sve uzroke i posledice. To je razlog zašto

zaštita kritične infrastrukture mora biti detaljno istražena i mora biti u stanju da integriše multidisciplinarni pristup. Menjanje gledišta na prevenciju i zaštitu od nesreća zahteva implementiranje različitih stavova iz nekoliko naučnih disciplina kao što su teorija konflikata, studije odbrane, ekonomija, tehnologija, upravljanje, pravo, sociologija, kriminologija i sl.

Asimetrična priroda današnjih rizika i pretnji za kritičnu infrastrukturu stvara neospornu i uslovnu potrebu za sveobuhvatnim merama bezbednosti. Imajući u vidu svu složenost napora i aktera uključenih u projekat „Jedan pojas i jedan put", cilj pristupa se može definisati kao stvaranje procedura i praksi u cilju jačanja otpornosti kritične infrastrukture i njihove spremnosti za prevenciju, ublažavanje, odgovor i oporavak (slično Kanadskoj nacionalnoj strategiji za kritične infrastrukture [23]).

Cilj se može postići samo kroz Sveobuhvatni pristup, koji mora obuhvatiti:

- identifikaciju nacionalnih, regionalnih ili sektorskih kritičnih infrastruktura povezanih sa održivim funkcionisanjem projekta „Pojas i put", kao i pomoćnih struktura,
- identifikaciju nacionalnih, regionalnih ili sektorskih rizika i pretnji za kritične infrastrukture;
- istraživanje rizika, pretnji i izazova za zaštitu kritičnih infrastruktura,
- identifikaciju aktera i zainteresovanih strana,
- izgradnju partnerstva među akterima,
- implementaciju pristupa upravljanja rizikom od svih opasnosti,
- utvrđivanje minimuma potrebnih zajedničkih propisa i resursa,
- razvoj na praksi kontinuiteta poslovanja,
- uspostavljanje koordinacionih tela,
- poboljšanje i uspostavljanje akademske i naučne saradnje i kapaciteta,
- razvoj procedura za rešavanje incidenata u zemlji i inostranstvu,
- zajedničku obuku i razvoj resursa,
- omogućavanje pravovremene razmene informacija sa zainteresovanim stranama,
- planiranje i dokumentaciju upravljanja vanrednim situacijama,
- uspostavljanje odgovarajućih sistema ranog upozoravanja,
- poboljšanje komunikacije između država, kompanija, građana i javnosti,
- postizanje veće posvećenosti državnih organa i operatera, a sve u vezi prevencije i upravljanja incidentima,
- praćenje napretka,
- analizu i konstantna poboljšanja.

Pristup bi trebalo da obuhvati sve nezgode uprkos njihovim izvorima: 1) prirodni događaji, 2) greške (tehničke ili ljudske greške) i 3) organizovano nasilje (terorizam, kriminal, rat) itd. [24].

Poboljšanja u sprovođenju ovog pristupa bila bi vidljiva u postizanju veće konkurentnosti, produktivnosti i isplativosti, ali i društvene odgovornosti u radu kritične infrastrukture.

Odgovornost za nacionalnu bezbednost i bezbednost u celini je pre svega u rukama svake pojedinačne nacionalne države. Države su u obavezi da obezbede sistematski okvir za odgovore na različite vrste kriza u oblasti kritičnih infrastruktura. Veliki broj i vrste kritičnih infrastruktura znači da svi nivoi vlasti treba da učestvuju u zaštiti kritične infrastrukture. Takođe, kompanije moraju da iskoriste sve svoje postojeće resurse. S obzirom na to da akcident, na sreću, nije stalna i svakodnevna situacija, nije racionalno uspostaviti i održavati kontramere permanentno. Spajanje resursa, informacija i razmena znanja je način na koji se resursi mogu koristiti na najbolji i održivi način u smislu efikasnosti, ali i sa stanovišta troškova i održivosti. Zato se zaštita kritične infrastrukture u projektu „Pojas i put" mora oslanjati na koordinaciju uključenih država, na nacionalnom i podnacionalnom nivou, na „PPP", na privatne subjekte i na deljenje resursa i informacija.

7. USPOSTAVLJANJE SVEOBUHVATNOG PRISTUPA

Da bi se obezbedio održiv, siguran i ekonomičan sistem zaštite kritične infrastrukture, on mora imati sledeće karakteristike:

- zajedničke vrednosti,
- razumevanje situacije i zajedničke ciljeve,
- mehanizme koordinacije,
- mehanizam za razmenu informacija,
- strukture za razvoj i planiranje,
- strukture za nadgledanje i rano upozoravanje,
- uspostavljanje partnerstva i multilateralnog razumevanja, kroz zajedničko obrazovanje, izgradnju vrednosti, obuku, vežbanja, analizu i planiranje odgovora na potencijalne ugroženosti kritične infrastrukture iz mogućih scenarija.

Zbog tradicionalno nametnutog nedostatka vremena i dobropoznatog okvira "modus operandi" često se zaboravlja na širok spektar mogućnosti u međusobnoj saradnji. Infrastruktura i propisi su, takođe, često ozbiljne prepreke.

Da bi se uklonili nedostaci u funkcionisanju, nedostatak resursa, nedostatak znanja i smanjenje vremena reagovanja, neophodni su mehanizmi koordinacije i tela. Koordinacijska tela moraju biti trajna. Osnivanje stalnih tela zaduženih za istraživanje mogućnosti i opcija predstavlja prvi korak u jačanju saradnje i rešavanju pitanja u:

- Različitosti interesa i pronalaženju zajedničkog imenioca zasnovanog na ravnoteži;
- Iskorišćavanju prednosti sinergije;
- Postavljanju politike saradnje sa fokusom na dve opcije: a) da se postigne nivo visokostrukturirane organizacije poput EU ili b) da se uspostavi mehanizam „slobodnih ruku" i manje strukturirani mehanizmi koordinacije;
- Rešavanje prvih koraka u definisanju aktera, kritične infrastrukture, razmene informacija i znanja itd.

Dobar primer koji treba slediti jeste onaj koji je uspostavljen 2016. godine, kada su Kina i arapske zemlje potpisale „Kinesko-arapsku politiku" ("China's Arab Policy Paper") [25]. Navedeni dokument uspostavlja osnovne principe saradnje i koordinacije na multilateralnim osnovama.

Koristeći takav pristup, zemlje mogu:

- postepeno 'proširiti' svoj razvojni model i izbeći oštre promene,
- izabrati dinamički efikasan pristup i u tranziciji, postaviti sebe u položaj za dugoročno preživljavanje,
- da nađu balans između strategije „Čekaj i gledaj" i brzopletog reagovanja na određene rizike,
- da zajednički razvijaju strategije koje će biti dizajnirane da budu fleksibilne i sposobne da se brzo razvijaju kao odgovor na očekivane promene,
- postaviti ciljeve i prioritete u investiranju, radu, istraživanju i razvoju i budućim tehnologijama.

8. ZAKLJUČAK

Zaštita kritične infrastrukture je na preseku prirodnih opasnosti, politike, biznisa, tehnologije i rizika. Projekat „Jedan pojas i jedan put" razvija veze između prostora i država od Azije (Kine), preko Afrike, do Evrope, uključujući brojne luke, železnice i puteve, brane, telekomunikacione objekte, naftovode i gasovode, linije električnih mreža, elektrane i mnoge druge različite kompanije. Rizici povezani sa objektima su kako spoljašnji

(teroristi, prirodne opasnosti, sajber-napadi itd.) tako i unutrašnji (tehnološke nesreće, ljudske greške, zagađenje, pitanja bezbednosti i zdravlja na radu itd.). Da bi se ostvarile maksimalne koristi i povrat investicija, novim tvorevinama su potrebni kontinuitet, stabilnost i operativna izvrsnost u poslovanju. Nažalost, poremećaji mogu biti masivni i mogu imati različite izvore i motive. Venecuela i njen sistem snabdevanja električnom energijom poslednji su primer koji uključuje mnoge aktere.

Skoro sve zemlje uključene u projekat „Jedan pojas i jedan put" klasifikovane su kao zemlje u razvoju, tako da su njihove sposobnosti i resursi u tretiranju potencijalnih opasnosti manje ili više ograničeni. U isto vreme, neke od njih su članice EU, gde su zaštita kritične infrastrukture i HSE (zdravlje, bezbednost i životna sredina kao poslovna funkcija) razvijene ili bar dobro regulisane. Projekat „Jedan pojas i jedan put" povezuje zemlje, infrastrukturu i kompanije i daće puni efekat samo ako su sve veze u potpunom funkcionisanju. S obzirom na to da su zaštitne mere jake kao i njihova najslabija karika, postoji potreba za razvojem Sveobuhvatnog pristupa.

Sveobuhvatni pristup mora obuhvatiti zemlje, privatne subjekte, sve vladine i nadnacionalne aktere, privatne, poslovne i sigurnosne i naučno-akademske organizacije u zaštiti kritične infrastrukture. Mora imati proaktivnu, preventivnu, ali i poboljšanu ulogu otpornosti. Potrebna je istovremeno zaštita od spoljašnjih i unutrašnjih opasnosti. Spoljna zaštita zahteva novi model zajedničkog učešća vojske, obaveštajne službe, policije, privatnih bezbednosnih kompanija i civilne zaštite. Na nivou kompanije potrebni su novi poboljšani modeli i operacije u oblasti HSE kako bi se postigla sinergija i racionalizovala upotreba javnih resursa.

Da bi se postigao Sveobuhvatni pristup, konstruktivna saradnja, zasnovana na zajedničkom regulativnom okruženju, standardima, uzajamnom poverenju, obuci, istraživanju i razvoju, razmeni informacija, alatima i merama i koordiniranoj akciji, treba da bude ključni faktor u smanjenju rizika ugrožavanja i povećanja zaštite kritične infrastrukture.

Razvoj Sveobuhvatnog pristupa u zaštiti kritične infrastrukture u okviru projekta „Jedan pojas i jedan put ' je očigledna potreba i može značajno poboljšati mogućnosti svih uključenih zemalja u zaštiti kritične infrastrukture. Osnivanje stalnih tela zaduženih za istraživanje mogućnosti i opcija trebalo bi da bude samo prvi korak u jačanju saradnje. Model EU u zaštiti kritične infrastrukture je takođe od značaja zbog uspostavljanja regulatornog okvira.

Kina i uključene zemlje trebalo bi da imaju interes u zaštiti kritične infrastrukture u okviru projekta „Pojas i put", jer bi njihovi proizvodi i ljudi bili glavni korisnici razvijene infrastrukture, poboljšala bi se zaštita snabde-

vanja energijom i povećao i ubrzao čitav spektar komunikacijskih mogućnosti. Bolja zaštita kritične infrastrukture osigurala bi ekonomske efekte ulaganja i izbegla nepotrebne gubitke.

LITERATURA

1. United States' National Infrastructure Protection Plan 2006.
2. European Commission Staff Working Document. A new approach to the European Programme for Critical Infrastructure Protection: making European critical infrastructures more secure. Brussels. August 28, 2013.
3. European Commission Staff Working Document. On the review of the European Programme for Critical Infrastructures Protection (EPCIP). Brussels. June 22, 2012.
4. European Commission, Critical Infrastructures; http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm, June 20, 2013.
5. European Union Council Directive. 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. December 23, 2008.
6. European Union Counter-Terrorism Strategy, Brussels 30th November 2005; http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf, June 20, 2013.
7. European Union (2007–2013). Specific programme: prevention, preparedness and consequence management of terrorism (2007–2013); http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33262_en.htm, June 20, 2013.
8. Van Nevel Hannes (2010). *De bescherming van kritiekeinfrastructuren: eenpublieke of overheidstaak? Eencasestudy in de Zeebrugse Haven*. Master Dissertation. Ghent University.
9. Directive 2008/1/EC of 15 January 2008 concerning integrated pollution prevention and control – IPPC.
10. Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances (Seveso II Directive).
11. Müller, J. (2012). Schutz kritischerInfrastrukturen. In: Stober, R., Olschok, H., Gundel, S. & Buhl, M. (eds.). *Managementhandbuch: Sicherheitswirtschaft und Unternehmenssicherheit*. Stuttgart: Richard Boorberg Verlag, 366–375.

12. Davidovic, D., Kesetovic, Z. & Pavicevic, O. (2012). National critical infrastructure protection in Serbia: the role of private security. *Journal of Physical Security*, 6(1): 59–72.

13. CoESS – APROSER (2013). The socio-economic value of private security services in Europe. Fourth White Paper on Private Security. Wemmel: CoESS.

14. CoESS (2012a). Critical infrastructure security and protection: the public-private opportunity. White Paper and guidelines by CoESS and its working committee. Wemmel: CoESS.

15. CoESS (2012b). Critical infrastructure private guarding company requirements checklist. Wemmel: CoESS.

16. Žugić B. R. (2007). *Civilna kontrola vojske*. VIZ, Beograd, str. 21.

17. Schnabel A. and M. Krupanski (2012). *Mapping Evolving Internal Roles of the Armed Forces*. DCAF, SSR Paper 7.

18. Milinović M., Jeftic Z. (2013). Challenges of National Defense in International State and Private Corporative Management of Infrastructure Protection, National Critical Infrastructure Protection – Regional Perspective. International Scientific Conference, Belgrade: University of Belgrade–Faculty of Security Studies and Institute for Corporative Security Studies Ljubljana, pp. 119–131.

19. Mitar Kovač, Nenad Dimitrijević, Brankica Potkonjak-Lukić (2013). Security aspects of the "South stream" as a critical infrastructure element of the Republic of Serbia, Challenges of National Defence in International State and Private Corporative Management of Infrastructure Protection, National Critical Infrastructure Protection – Regional Perspective. International Scientific Conference, Belgrade: University of Belgrade–Faculty of Security Studies and Institute for Corporative Security Studies Ljubljana.

20. National Infrastructure Advisory Council (2009). Critical Infrastructure Resilience. Research Report. USA.

21. Hong Kong Labour Department, Occupational Safety and Health Branch. (April, 2002). Code of Practice on Safety Management First ed. Retrieved from http://www.info.gov.hk/labour/public/index.htm

22. Prezelj, I. (2008). *Konceptualna opredelite v kritične infrastrukture*. FDV, Ljubljana, str. 13.

23. Canadian government (2009). National Strategy for Critical Infrastructure. Her Majesty the Queening Right of Canada.

24. Federal Republic of Germany, Federal Ministry of the Interior (2009). National Strategy for Critical Infrastructure Protection (CIP Strategy).

25. "China's Arab Policy Paper", 2016; https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1331683.shtml

26. Bucharest Summit Declaration; https://www.nato.int/cps/us/natohq/official_texts_8443.htm

27. https://www.blic.rs/biznis/vesti/opasan-projekat-crne-gore-ako-kini-ne-vrate-kredit-za-autoput-beograd-bar-ostaju-bez/b8pjkxz?utm_source=blic_kat_kultura_sidebar&utm_medium=sidebar_najnovije_info