

Jana Marković*

Fakultet bezbednosti, Univerzitet u Beogradu

Resursi privatne bezbednosti za zaštitu kritične infrastrukture u urbanim uslovima

SAŽETAK

Kritična infrastruktura obuhvata mreže, sisteme, objekte i sredstva koji obezbeđuju funkcionisanje države i osiguravanje osnovnih potreba stanovništvu. Ona predstavlja okosnicu svakog društva i kao takva obezbeđuje blagostanje, prosperitet i bezbednost. Zbog uloge koju ima u održavanju funkcionisanja, integriteta i bezbednosti u urbanim sredinama ona se može smatrati značajnom karikom urbane bezbednosti. Različiti društveni procesi savremenog doba doveli su do promena u organizacionim, tehničkim i operativnim aspektima kritične infrastrukture, a međusobna povezanost, složenost i zavisnost ovih infrastruktura dovela je do multiplikacije rizika. Kritična infrastruktura danas je ranjiva na različite pretnje, tradicionalne ili savremene, uključujući prirodne katastrofe, sajber napade i terorističke akte. Njena ranjivost preslikava se na ranjivost društva, te predstavlja visok nivo rizika po sveukupnu bezbednost, uključujući i bezbednost urbanih sredina. Ključnim segmentom zaštite kritične infrastrukture smatra se njena otpornost. U osnovi, otpornost jeste sposobnost sistema, mreže, objekta ili nekog drugog elementa kritične infrastrukture da apsorbuje negativne uticaje, da im se prilagodi i u što optimalnijem vremenskom periodu

* markovicfb22@gmail.com

vrati u stanje normalnog ili čak poboljšanog funkcionisanja. Samim tim, jačanjem otpornosti kritične infrastrukture, pored vršenja zaštite kritične infrastrukture, jača se i otpornost sredine u kojoj se ona nalazi, što dalje doprinosi otpornosti društva u celini. Jedan od provajdera zaštite kritične infrastrukture, kao i provajdera urbane bezbednosti jeste sektor privatne bezbednosti. Ovaj sektor ili industrija privatne bezbednosti, kako se često naziva, poslednjih decenija je značajan subjekat u areni pružanja usluga bezbednosti, dok je kritična infrastruktura čest referentni objekat kojem pružaju zaštitu. Autorka je u radu ukazala na ulogu koju sektor privatne bezbednosti ima u urbanim sredinama, uzimajući zaštitu kritične infrastrukture kao varijablu preko koje će tu ulogu predstaviti. Cilj rada jeste da prikaže teorijske uvide u različite resurse koje sektor privatne bezbednosti koristi za zaštitu kritične infrastrukture, čime posredno doprinosi i bezbednosti u urbanim uslovima.

KLJUČNE REČI: *privatna bezbednost, kritična infrastruktura, zaštita kritične infrastrukture, urbanost*

UVOD

Nedržavni sektor bezbednosti ili sektor (industrija) privatne bezbednosti sve više je deo svakodnevnog života kao nosilac određenih bezbednosnih funkcija. Privatne bezbednosne kompanije, kao deo ovog sektora, sve više su uključene u ostvarivanje i održavanje javne bezbednosti, što uključuje i zaštitu kritične infrastrukture, čija je zaštita ujedno i ozbiljan izazov za celokupan sektor bezbednosti. Na primer, Konfederacija evropskih službi bezbednosti smatra da je privatna bezbednost ključna u zaštiti lokacija kritične infrastrukture, s obzirom na to da kombinuje ljudski faktor sa merama obezbeđenja koje se koriste u zaštiti kritične infrastrukture (CoESS, 2016: 12). Naravno, na ovom mestu govorimo o profesionalnim kompanijama koje pružaju usluge bezbednosti na legalnoj osnovi, prema pravilima koja su utemeljena najpre u nacionalnim legislativama, a potom međunarodnim i nacionalnim standardima, kao i svim drugim dokumentima u kojima se određuju njihove delatnosti i aktivnosti i mere za koje imaju legitimitet u primeni.

Pored uvodnog razmatranja, rad obuhvata dve celine. Prvi deo rada odnosi se na koncepte kritične infrastrukture i njene zaštite, kako bi se ukazalo na značaj koji kritična infrastruktura ima za državu i društvo. Ujedno, njen značaj i vitalna uloga koju ima razlozi su zbog kojeg je izabrana kao posredujuća varijabla u izučavanju doprinosa privatne bezbednosti u urbanim sredinama, odnosno izučavanju načina na koji privatne bezbednosne kompanije doprinose

bezbednosti u urbanim sredinama.¹ Drugi deo rada posvećen je privatnim bezbednosnim kompanijama kao jednim od subjekata industrije privatne bezbednosti. Ovaj deo obuhvata i deskripciju resursa privatne bezbednosti (privatnih bezbednosnih kompanija), čijom se upotrebom zadovoljava potreba za bezbednošću kritične infrastrukture u urbanim uslovima i, dalje, doprinosi urbanoj bezbednosti.

KRITIČNA INFRASTRUKTURA I NJENA ZAŠTITA

Kritične infrastrukture kakve danas poznajemo rezultat su njihovog razvoja proteklih decenija, ili čak vekova. Od niza malih, nezavisnih tehnologija nastale su infrastrukture „kada jedan tehnološki sistem dominira nad drugima ili kada se nezavisni sistemi razvijaju u mrežu” (Larkin, 2013: 330). Od rimskih akvadukta i puteva, preko železnica i luka, do savremenih infrastrukturnih mreža, „uglavnom u privatnom vlasništvu, (dodao autor: sastavljenih od) sistema koje je napravio čovek i procesa, koji funkcionišu zajedno i sinergijski kako bi proizveli i distribuirali kontinuirani tok osnovnih dobara i usluga (US President’s Commission on Critical Infrastructure Protection, 1997). Direktiva 2022/2557 Evropskog parlamenta i Veća definiše kritičnu infrastrukturu kao „imovinu, objekat, opremu, mrežu ili sistem ili deo imovine, objekta, opreme, mreže ili sistema, koji je potreban za pružanje ključne usluge”, dok je ključna usluga svaka „usluga koja je ključna za održavanje vitalnih društvenih funkcija, ekonomskih aktivnosti, javnog zdravlja i sigurnosti ili okoline” (Directive (EU) 2022/2557, 2022, art. 2).

Brojni društveni, ekonomski, politički i tehnološki razlozi doveli su do promena u organizacionim, operativnim i tehničkim aspektima infrastrukture (Setola, et al., 2016: 3). Kritična infrastruktura danas obuhvata „opremu, zgrade i konstrukcije, instalacije i usluge koje se tretiraju kao celina i kao takve čine kohezivne sisteme neophodne za nesmetano funkcionisanje države” (Žaboklicka, 2020:

1 Različiti su aspekti na kojima privatna bezbednost može da doprinese urbanoj bezbednosti. Kao što je navedeno, za proučavanje je na ovom mestu odabran samo jedan aspekt i to zaštita urbane kritične infrastrukture. U kontekstu rada, štice vrednosti jesu resursi urbane kritične infrastrukture, a privatne bezbednosne kompanije su jedan od provajdera (pružaoca) bezbednosti (prema Paraušić i Lipovac, 2019).

71), jer „proizvode ključni asortiman robe i pružaju one vrste usluga bez kojih nema opstanka, stabilnosti i razvoja društva kao takvog” (Бошковић, 2017: 72). Reč „kritično” ukazuje na to da se radi o pružanju robe (proizvoda i usluga) koja je ključna za ekonomsko i socijalno blagostanje, prosperitet, bezbednost i uopšte funkcionisanje države.

Kada kritična infrastruktura pripada urbanim sredinama i obezbeđuje zadovoljavanje vitalnih potreba pod urbanim uslovima, može se govoriti o urbanoj kritičnoj infrastrukturi. Ona oblikuje gradove društveno, politički i ekološki. Menja izgled gradova, rešava ili stvara nove ekološke probleme, može dovesti do podela unutar gradova, stvoriti nepogodnosti i nejednakosti, podeliti ili zbližiti zajednice, može se kupiti, prodati i biti u suvlasništvu (Steele and Legacy, 2017: 1)². Jednostavno, mreže urbane kritične infrastrukture jesu arterije naših gradova. Drugačije rečeno, u kontekstu zaštite ljudskog života obezbeđivanjem neophodne infrastrukture u naseljenim gradovima, termin „linija za spasavanje” (engl. *Lifeline*) koristi se da označi svaki sistem koji održava funkciju u gradovima. To su sistemi koji su klasifikovani prema uslugama koje pružaju na: 1. Sisteme vodosnabdevanja i prečišćavanja, 2. Energetske sisteme, 3. Informacione i komunikacione sisteme i 4. Transportne sisteme (Hamada, 2013: 3).

Sa jedne strane, razvoj gradova i urbanih sredina direktno je zavisn od urbane kritične infrastrukture, u prvom redu električne mreže, sistema za distribuciju vode ili komunalnih mreža cevovoda prirodnog gasa ili nafte. Energija, voda, hrana, transport, zdravlje, javni red i bezbednost najkritičnije su infrastrukture u rastućim gradovima sa sve većim brojem stanovnika. Više od polovine globalne populacije trenutno živi u urbanim područjima, a predviđa se da će stopa dostići 70 procenata do 2050. godine (Statistics Division, n.d.). Sa aspekta razvoja takozvanih „pametnih gradova”, energetska i IKT infrastruktura izbijaju u prvi plan. Takođe, koncept „pametnih gradova” trenutno omogućava međusobno povezivanje različitih međuzavisnih urbanih infrastrukture (Ersoy, 2017). Sa druge strane, isti taj razvoj je uvećao i učinio složenijim zahtev koji je postavljen

2 Kritična infrastruktura može biti u vlasništvu države (npr. javni putevi), u privatnom vlasništvu (npr. telekomunikacija), u vlasništvu zajednice (npr. sistemi za navodnjavanje) ili uključivati javno-privatna partnerstva (npr. snabdevanje naftom i derivatima).

pred tu kritičnu infrastrukturu, učinivši je istovremeno ranjivijom na pretnje. Na primer, uragani Katrina, Sendi i Harvi ozbiljno su pogodili gradove Nju Orleans, Njujork i Hjuston proizvodeći velike krize i nanevši ogromnu štetu urbanim kritičnim infrastrukturnama, a time i društvu utičajući, na primer, na snabdevanje energijom i komunikacijama ili na transportnu infrastrukturu i usluge (Lomba-Fernández, Hernantes and Labaka, 2019).

Kritična infrastruktura izložena je brojnim pretnjama iz unutrašnjeg ili spoljašnjeg okruženja. Te pretnje se mogu ugrubo podeliti na one koje potiču iz prirodnog okruženja, one koje prouzrokuje čovek svojim delanjem, odnosno one koje imaju tehničko-tehnološki karakter, poput tehnoloških akcidenata, eksplozija i požara. Kritična infrastruktura kao opšte dobro, od kojeg zavisi obezbeđivanje drugih dobara u državi i za potrebe stanovništva, ugrožena je posebno prirodnim nesrećama, tehnološkim udesima, kriminalnim aktivnostima i terorističkim aktima. Uzimajući u obzir to da gotovo svaka kritična infrastruktura danas posluje koristeći informaciono-komunikacione tehnologije, dakle, da je deo takozvane sajber sfere, kao značajna pretnja izdvaja se i sajber napad na kritičnu infrastrukturu. Kriza izazvana pandemijom KOVID-19 pokazala je da i bolesti i njima prouzrokovane pandemije takođe mogu biti pretnja po kritičnu infrastrukturu kada ona zavisi od kritičnog osoblja koje njom upravlja.

Prirodne katastrofe (npr. zemljotres, uragan, poplave), do kojih dolazi usled ekstremnih vremenskih prilika, kada jaki efekti vremenskih promena utiču negativno na strukturu i funkcionisanje kritične infrastrukture, ne mogu se izbeći. Danas, usled aktuelnih klimatskih promena, ova vrsta pretnji dobija na značaju i više nego što je to ranije bio slučaj. Iz tog razloga, zaštita kritične infrastrukture ima funkciju pravovremenog reagovanja i minimiziranja nastalih posledica takvog događaja. Tehnološki udesi prouzrokovani bilo ljudskom greškom u kontroli tehnologije ili kvarom tehnološkog sistema značajno mogu da ugroze funkcionisanje kritične infrastrukture. Potencijalni uzroci ovih nesreća ukazuju na važnost pouzdane tehnologije i stručnog ljudskog kapitala. Kriminalne aktivnosti, poput krađa, sabotaža, diverzija, i u krajnjoj liniji terorističkih aktivnosti, uvek se sprovode sa ciljem narušavanja bezbednosti kritičnih infrastrukture kao cilja za sebe ili cilja potrebnog za ostvarivanje nekih većih težnji (npr. političkih). Fizičko obezbeđenje kritične infrastrukture izlazi u prvi plan kada je reč o ovim pretnjama. Na kraju,

sajber napadi postaju sve češće pominjani u kontekstu neophodnosti zaštite kritične infrastrukture. Ovi napadi za cilj imaju ugrožavanje poverljivosti, integriteta i raspoloživosti podataka i informacija, koje su kod ove vrste organizacija od izuzetnog značaja, te je u osnovi zaštite bezbednosna tehnologija za informacione sisteme, poput kriptografije i bezbednosnih komunikacionih protokola.

Cilj zaštite kritične infrastrukture jeste obezbediti njeno kontinuirano funkcionisanje, kako bi se osiguralo kontinuirano snabdevanje proizvodima i uslugama koje su vitalne za jednu državu ili društvo. Zaštitu kritične infrastrukture možemo posmatrati kroz *otpornost*, kao sposobnost da se izdrži i oporavi od prirodnog ili namerno izazvanog poremećaja, i *bezbednost*, u smislu aktivnosti i mera za smanjenje verovatnoće i uticaja kriminalnih i terorističkih akcija (CoESS, 2016: 10). Mere bezbednosti bi na ovom mestu obuhvatile skup fizičkih, tehničkih i organizacionih mera za praćenje i zaštitu elemenata kritične infrastrukture. Celokupan sistem bezbednosti treba shvatiti kao integrisan sistem sastavljen od elemenata i procesa (radnji) koji funkcioniše kao instrument za zaštitu kritične infrastrukture. Potrebne funkcije ovog sistema su: odvracanje potencijalnih napadača, otkrivanje upada u zaštićeni objekat, prostore ili zone ili otkrivanje nastanka opasne situacije u objektu ili u njegovoj neposrednoj okolini, usporavanje kretanja napadača i odgovor na ometanje zaštićenog objekta, prostora ili zone i zabrana pristupa istom (Hofreiter and Zvaková, 2017: 143).

Sa jedne strane, osnova zaštite jeste jačanje otpornosti kritične infrastrukture. Otpornost kritične infrastrukture je indikator koji kvantifikuje njegovu sposobnost da obezbedi rad u uslovima kada deluju negativni spoljašnji i unutrašnji faktori (Lukas and Hromada, 2011: 1138). Ona se može razumeti kao trodimenzionalni koncept, koji uključuje kapacitet apsorpcije (stepen do kojeg sistem može da apsorbuje uticaj i minimizira posledice uz malo napora), adaptivni kapacitet (sposobnost sistema da se prilagodi neželjenim situacijama podvrgavanjem nekim promenama) i restorativni kapacitet (brzina povratka na normalne ili poboljšane operacije) (Francis and Bekera, 2014: 94). Jačanjem otpornosti, kritična infrastruktura se ipak ne može u potpunosti zaštititi. Delovanjem spoljašnjih i unutrašnjih faktora, u najvećem broju slučajeva, ako ne i u svakom, doći će do degradacije funkcionisanja, s tim da se jačanjem otpornosti može uticati na stepen degradacije tako da se on svede na najmanji mogući

stupanj. Dodatno, izgradnja otpornosti kompleksna je u urbanim sredinama gde deluje veći broj različitih zainteresovanih strana.

Sa jedne strane, sveukupan sistem bezbednosti bilo koje kritične infrastrukture može se sagledati kroz prizmu korporativne bezbednosti. Korporativna bezbednost, kao deo privatne bezbednosti ili industrije privatne bezbednosti, jeste proces³ zaštite imovine organizacije ili njenog poslovanja u šta se ubrajaju ljudi, stvari i informacije koje su u njihovom vlasništvu ili su im poverene, što, u krajnjoj liniji, treba da doprinese sprečavanju gubitaka i uvećanju vrednosti (Kovacich and Halibozek, 2003: 48). U kontekstu kritične infrastrukture, krajnji cilj korporativne bezbednosti jeste obezbeđivanje kontinuiranog pružanja ključnih proizvoda i usluga. Izbor koji je načinjen u ovom radu u pogledu predmeta istraživanja fokus usmerava na privatne bezbednosne kompanije kao potencijalne provajdere zaštite kritične infrastrukture. Korporativna bezbednost kao sistem bezbednosti organizacije, u ovom slučaju, kritične infrastrukture može za potrebe postizanja bezbednosti kao stanja da iznajmljuje i koristi usluge privatnih bezbednosnih kompanija.

Na kraju, zaštita kritične infrastrukture nije samo pitanje otpornosti i aktivnosti i mera bezbednosti, već i zaštite sa tehničkog stanovišta. To bi značilo upotrebu novih naprednih materijala, inovativne kombinacije materijala ili funkcionalne strukturne elemente koji mogu da poboljšaju robusnost, strukturnu (fizičku) krutost i integritet objekata i postrojenja kritične infrastrukture (Mañas, 2011: 247).

PRIVATNE BEZBEDNOSNE KOMPANIJE KAO PROVAJDER ZAŠTITE KRITIČNE INFRASTRUKTURE

Privatna bezbednosna kompanija, kao jedna vrsta subjekta industrije privatne bezbednosti, jeste „jasno strukturisana i hijerarhijski ustrojena registrovana korporativna asocijacija koja pruža usluge bezbednosnog karaktera, takmičeći se za dobijanje poslova sa drugim takvim firmama na tržištu”. Ova kompanija pruža usluge fizičkog i tehničkog obezbeđenja lica, objekata i imovine (Centar za

3 Korporativna bezbednost može se odrediti i kao sistem, organizacija, funkcija, svojstvo ili stanje.

civilno-vojne odnose, 2008: 118–119). To je kompanija koja pruža usluge bezbednosti po ugovoru i uz dogovorenu nadoknadu. Subjekti koji iznajmljuju i koriste ove usluge mogu biti građani, druge organizacije i država. Ugrubo, usluge bezbednosti se mogu grupisati na usluge fizičke zaštite, usluge tehničke zaštite i ostale usluge (npr. usluge u oblasti kriznog menadžmenta ili upravljanja rizicima, usluge izrade akata, usluge konsaltinga, usluge obuke). Preciznije, usluge bezbednosti uključuju komercijalno obezbeđenje sa osobljem, patrolu, interno obezbeđenje (može biti shvaćeno kao korporativna bezbednost), obezbeđenje događaja, obezbeđenje na ulazu, telohranitelj, transport gotovine i transport dragocenosti, obrada gotovine, mobilne alarmne usluge i usluge odgovora na pozive, alarm i video nadzor, usluge monitoring centra, traženje i praćenje, vazduhoplovna bezbednost, skrining, usluge korišćenja obučениh pasa, pomorska bezbednost, *zaštita kritične infrastrukture*, kombinovana rešenja, korporativna istraga, usluge prve pomoći, usluge prevencije i zaštite od požara, *urbana bezbednost*, prevencija gubitaka, recepcioner/konsijerž, bezbednosni konsalting, specijalizovano obezbeđenje, obuka za privatno obezbeđenje i mnoge druge (CoESS, 2016: 6). U pojedinim oblastima poput obezbeđenja događaja ili zaštite kritične infrastrukture privatne bezbednosne kompanije rade zajedno sa policijom.

Resursi privatne bezbednosti, odnosno konkretnije privatnih bezbednosnih kompanija mogu se sagledati u osnovi kroz ljudske i materijalne resurse. Iz teksta koji sledi, može se primetiti da ovi resursi odgovaraju u određenoj meri tehnikama takozvane „situacione prevencije kriminala”. Reč je o tehnikama iz četiri grupe: za povećanje percipiranih napora, za povećanje percipiranih rizika, smanjenje predviđene nagrade i uklanjanja izgovora. Tako, recimo, mehaničke barijere ili kontrola pristupa spadaju u tehnike povećanja percipiranih napora. Nadzor u koji se ubraja nadzor od strane službenika obezbeđenja neposredno ili putem tehničkih elektronskih sredstava spada u tehnike za povećanje percipiranih rizika (Clarke, 1997: 18).

Ljudski resursi jesu lica zaposlena u ovim kompanijama. Ona se dele na one koji obezbeđuju funkcionisanje ovih kompanija (rukovodstvo, pravni sektor, sektor ljudskih resursa, informacioni sektor, marketinški i komercijalni sektor itd.), i one koji pružaju usluge bezbednosti. Druga grupa lica jesu, u prvom redu, službenici obezbeđenja koji vrše poslove fizičko-tehničkog obezbeđenja, odnosno vrše poslove obezbeđenja prisustvom i aktivnošću, uz korišćenje

sredstava tehničke zaštite. Oni sprovode kontrolu pristupa i ponašanja lica, obilazak i pregled prostora, pratnju i zaštitu vrednosti. Navedene aktivnosti su pre svega u funkciji prevencije različitih oblika kriminaliteta, te se ovi poslovi mogu grupisati u nekoliko kategorija: sprečavanje ili otkrivanje upada, neovlašćenog ulaska ili aktivnosti, vandalizma i ometanja privatnog vlasništva; sprečavanje ili otkrivanje krađe, gubitka, pronevere ili prikrivanja robe, novca, obveznica, akcija, novčanica, dokumenata ili hartija od vrednosti; zaštita pojedinaca od telesnih povreda; obezbeđivanje prisustva; poštovanje i sprovođenje utvrđenih pravila, propisa, mera, politika i praksi kompanije; prijavljivanje i privođenje prekršilaca; prijavljivanje incidenata i poziva (United Nations Office on Drugs and Crime, 2014: 7). Službenici obezbeđenja često su obučeni i za reagovanje u vanrednim situacijama i upravljanje kriznim situacijama. Pored službenika obezbeđenja, u ovu grupu ljudskih resursa spadaju i ostala lica koja sprovode druge vrste usluga bezbednosti. Ta lica se mogu nazivati službenicima obezbeđenja, ali ne nužno. Na primer, to mogu biti lica koja planiraju, projektuju ili implementiraju tehničke sisteme, lica koja izrađuju procene, planove ili druge akte bezbednosnog karaktera, lica koja sprovode savetovanja (konsalting) i obuke iz oblasti bezbednosti i slično. Ova lica poseduju resurs koji na ovom mestu takođe može biti izdvojen, a to je znanje – specijalizovano znanje koje se stiče obrazovanjem, obučavanjem, osposobljavanjem i usavršavanjem. Prema tome, jedan aspekt ljudskih resursa koji se na ovom mestu izdvaja jeste osposobljenost. Službenici obezbeđenja moraju biti osposobljeni i obučeni ljudi, koji imaju legitimno pravo (to znači da poseduju licencu za vršenje ovih poslova) da sprovode mere i aktivnosti bezbednosti. Pored opšteg obrazovanja, stručne obučenosti, neophodna je i konkretna edukacija prema karakteristikama sistema ili objekata gde sprovode ove mere i aktivnosti. Zadatak privatnih bezbednosnih kompanija, koji u praksi često nije do kraja ostvaren, jeste da obezbede legalan, etički, profesionalni i adekvatno plaćen rad službenika obezbeđenja.

Materijalni resursi se, kao i ljudski, dele na resurse koji obezbeđuju funkcionisanje ovih kompanija (koriste ih sektori nabrojani ranije) i one koje koriste službenici obezbeđenja. To je sva oprema koju u radu koriste službenici, uključujući oružje, sredstva za vezivanje, ručne detektore i druga sredstva za obavljanje pregleda, sredstva veze i drugu IKT opremu, uniformu, svoju dokumentaciju o obučenosti i angažovanju, evidencije i izveštaje itd. Međutim,

materijalni resursi nisu ograničeni samo na one koje koriste službenici. Privatne bezbednosne kompanije, osim pružanja fizičke (i fizičko-tehničke) zaštite, pružaju i usluge tehničke zaštite, odnosno planiranje, projektovanje, ugradnju i održavanje tehničkih sistema, sredstava i uređaja. To podrazumeva, u prvom redu, postavljanje sistema video obezbeđenja⁴, implementiranje alarmnih sistema, sistema kontrole pristupa, uređaja za brzo reagovanje, i to najčešće sa servisima za reagovanje. Ova vrsta resursa od posebnog je značaja na objektima gde nisu neposredno prisutni službenici obezbeđenja, poput udaljenih magacina, deponija, cevovoda, pumpnih stanica, rezervoara, električnih podstanica, brana i sl. Privatne bezbednosne kompanije kontinuirano ulažu u najsavremenije tehnologije i inovacije kako bi unapredile kvalitet svojih usluga i ujedno poboljšale zaštitu koju pružaju. Postavljanje mehaničkih barijera kao prepreka koje onemogućavaju, odnosno otežavaju upad uštićeni prostor i pristup šticeim vrednostima obično je u nadležnosti subjekta kojem se pružaju usluge bezbednosti. Međutim, nije isključena ni mogućnost postavljanja ove vrste tehničke, mehaničke zaštite i od strane privatnih bezbednosnih kompanija. Privatne bezbednosne kompanije mogu raspolagati značajnom IKT opremom, i u skladu sa tim biti važan subjekat u sistemu prikupljanja, razmene i čuvanja informacija. Štaviše, sama razmena informacija se identifikuje kao ključni element napora vlade i privatnog sektora (uključujući i sektor bezbednosti) da zaštite kritičnu infrastrukturu.

Značaj i ujedno još jedan pravac delovanja privatnih bezbednosnih kompanija ogleda se u njihovoj stručnosti u proceni rizika, koja je uvek početna tačka u obavljanju bilo koje vrste usluge u njihovom delokrugu. Ove kompanije često su specijalizovane i za bezbednosno savetovanje i obuku. Pored procene rizika, izdvajaju se još neke aktivnosti koje mogu biti poverene ovim kompanijama. Reč je o obradi bezbednosne dokumentacije (npr. strategije, politike, direktive, projekti, itd.), utvrđivanju potrebnog režima i organizacionih mera za obezbeđivanje pristupa objektima, utvrđivanju režima rada sa poverljivim podacima i informacijama, aktivnosti revizije i kontrole (Rehak, et al., 2023: 14). Navedene aktivnosti se mogu

4 Generalno, kada je reč o sistemima video obezbeđenja, upotreba ovih sistema ili takozvani „video-nadzor” dominira i kada su u pitanju mere urbane bezbednosti.

podvesti pod menadžment koji omogućava efikasno funkcionisanje sveukupne zaštite kritične infrastrukture.

Resursi se mogu sagledati i sa drugačijeg aspekta, i to kao fizički element zaštite (ljudski resursi, odnosno službenici obezbeđenja i drugi koji pružaju usluge bezbednosti), aktivni element zaštite (tehnički, elektronski sistemi i sredstva), pasivni element zaštite (tehnički, mehanički sistemi i sredstva, odnosno mehaničke barijere) i takozvane „režimske mere“ (bezbednosni menadžment) (Hofreiter and Zvaková, 2017: 142).

ZAKLJUČAK

Države zavise od kritične infrastrukture. Mreže, sistemi i objekti kritične infrastrukture obezbeđuju osnovne usluge i proizvode na kojima počiva funkcionisanje države i snabdevanje stanovništva. Gradovi zavise od (urbane) kritične infrastrukture. Gradovi funkcionišu i razvijaju se na osnovama kritične infrastrukture. Tehnički, ljudski i informacioni elementi kritične infrastrukture obezbeđuju osnovne potrebe stanovništva urbanih sredina. Iz razloga postojanja brojnih različitih potencijalnih pretnji, koje mogu da osujete obezbeđivanje ovih potreba, jedan od prioriteta urbanih sredina jeste zaštita kritičnih infrastrukture koje im pripadaju. Zaštita kritične infrastrukture je od suštinskog značaja u složenim društvima u kojima svi živimo.

Onda kada se unapređuje otpornost i bezbednost urbane kritične infrastrukture unapređuje se i otpornost i bezbednost celokupne zajednice i urbane sredine. Naime, zaštitom kritične infrastrukture obezbeđuje se kontinuiran pristup dobrima koja stanovništvo grada svakodnevno koristi, što u vidu zadovoljenja potreba, što u vidu pristupa različitim uslugama, a u prvom redu onim koje pružaju javne ustanove. Zaštitom kritične infrastrukture obezbeđuju se, u prvom redu, energija, nafta i prirodni gas, voda i hrana, kanalizaciona rešenja, transport, javne usluge poput zdravstva, javnog reda i bezbednosti. Time se u krajnjoj liniji doprinosi sveukupnoj bezbednosti (i zaštiti) urbanih sredina, čime se i zadovoljavaju potrebe stanovništva i poboljšava kvalitet života i privlačnost grada.

Kritična infrastruktura može da poboljša svoju otpornost i bezbednost koristeći ekspertizu i resurse privatne bezbednosti i privatnih

bezbednosnih kompanija. Privatna bezbednost igra višestruku ulogu u zaštiti kritične infrastrukture. Privatne bezbednosne kompanije su specijalizovane za poslove koji su od značaja za zaštitu kritične infrastrukture. Naravno, na ovom mestu se govori o profesionalnim kompanijama koje, ulagajući u svoje ljudske i materijalne resurse, doprinose kvalitetu usluga koje nude i pružaju. Ljudski resursi treba da ispunjavaju uslove postavljene normativom zemlje u kojoj pružaju usluge i usvojenim standardima, da se osposobljavaju i kontinuirano obučavaju uvažavajući pravila struke, nove trendove i potrebe privatnog sektora bezbednosti. Materijalni resursi treba da budu prilagođeni uslovima u kojima se implementiraju, održavani funkcionalnim i što je više moguće da budu inovativni. Privatne bezbednosne kompanije znaju da je uslov njihovog opstanka na tržištu i sticanja profita rad usklađen sa zahtevima tržišta i novim trendovima koji se javljaju. Ova dva elementa ujedno su i pretpostavka efikasne zaštite, u ovom slučaju, kritične infrastrukture.

Uloga privatnog sektora u domenu nacionalne bezbednosti nije nova. Istina, o angažovanju privatnog sektora u zaštiti kritične infrastrukture govori se intenzivno tek nakon 11. septembra 2001. godine.⁵ Sve veće uključivanje privatnih bezbednosnih kompanija u zaštitu vitalnih objekata društva povlači, sa jedne strane, sve veću odgovornost tih kompanija, dok, sa druge, povlači i sve veću odgovornost vlada kada biraju kompanije koje će se starati o bezbednosti ovih objekata. Samim tim što se ovim kompanijama poveravaju poslovi koji su povezani sa najosetljivijim elementima objekata, postrojenja i sistema koji sami po sebi predstavljaju najosetljivije elemente države i društva, jasan je izazov koji postoji kada se pravi izbor kompanija koje će biti angažovane u službi nacionalne bezbednosti.

LITERATURA

Бошковић, Милица (2017). *Индустријска безбедност и заштита*. Београд: Универзитет у Београду, Факултет безбедности.

“Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and

5 Do tada je veći fokus bio na angažovanju privatnih vojnih kompanija u konfliktnim područjima i angažovanju privatnih bezbednosnih kompanija u postkonfliktnim područjima, kao i proizvodnju i trgovinu naoružanjem.

repealing Council Directive 2008/114/EC” Official Journal of the European Union L, 164–198, 27.12.2022.

Centar za civilno-vojne odnose (2008). *Privatne bezbednosne kompanije u Srbiji – prijatelj ili pretnja?* Beograd: Centar za civilno-vojne odnose.

Clarke, V. Ronald (1997). *Situational Crime Prevention: Successful Case Studies*. New York: Harrow and Heston.

CoESS (2016). *Critical Infrastructure Security and Protection: The Public-Private Opportunity*. Belgium: Confederation of European Security Services.

Ersoy, Aksel (2017). Smart cities as a mechanism towards a broader understanding of infrastructure interdependencies. *Reg Stud Reg Sci* 4(1), 26–31.

Francis, Royce, and Bekera, Behailu (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab Eng Syst Saf*, 121, 90–103.

Hamada, Masanori (2013). “General”. In: M. Hamada (Ed.). *Critical Urban Infrastructure Handbook* (pp. 3–10). Boca Raton: CRC Press.

Hofreiter, Ladislav, and Zvaková, Zuzana (2017). “Theoretical Aspects of Critical Infrastructure Protection”. In: A. Kravcov, E. Cherepetskaya, and V. Pospichal (Eds.), *Durability of Critical Infrastructure, Monitoring and Testing* (pp. 139–147). Singapore: Springer.

Kovacich, L. G., and Halibozek, P. E. (2003). *The manager’s handbook for corporate security: establishing and managing a successful assets protection program*. Burlington: Butterworth–Heinemann is an imprint of Elsevier Science.

Larkin, Brain (2013). The politics and poetics of infrastructure. *Annual review of anthropology*, 42, 327–343.

Lomba-Fernández, Cinta, Hernantes, Josune, and Labaka, Leire (2019). Guide for Climate-Resilient Cities: An Urban Critical Infrastructures Approach. *Sustainability*, 11(17), 4727.

Lukas, Ludek, and Hromada, Martin (2011). Resilience as main part of protection of critical infrastructure. *International journal of mathematical models and methods in applied sciences*, 5(6), 1135–1142.

Mañas, Pavel (2017). “The Protection of Critical Infrastructure Objects – Technical Principles”. In: A. Kravcov, E. Cherepetskaya, and V.

- Pospichal (Eds.), *Durability of Critical Infrastructure, Monitoring and Testing. Lecture Notes in Mechanical Engineering* (pp. 239–248). Singapore: Springer.
- Paraušić, Ana, i Lipovac, Milan (2019). Karakteristike pretnji urbanoj bezbednosti. *Politička revija: časopis za politikologiju, političku sociologiju, komunikologiju i primenjenu politiku*, 19(2), 255–277.
- Rehak, David, Lovecek, Tomas, Hromada, Martin, Walker, Neil, and Haring, Ivo (2023). “Critical Infrastructures Resilience in the Context of a Physical Protection System”. In: R. Shinkuma, F. Xhafa, T. Nishio, T. (Eds.), *Advances in Engineering and Information Science Toward Smart City and Beyond. Engineering Cyber-Physical Systems and Critical Infrastructures* (pp. 1–33). Cham: Springer.
- Setola, Roberto, Luiijf, Eric, and Theocharidou, Marianthi (2016). “Critical infrastructures, protection and resilience”. In: R. Setola, V. Rosato, E. Kyriakides, E. Rome (Eds.), *Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach* (pp. 1–18). Springer International Publishing.
- Statistics Division. (n.d.). *Make cities and human settlements inclusive, safe, resilient and sustainable*. United Nations. Dostupno na: <https://unstats.un.org/sdgs/report/2023/goal-11/>.
- Steele, Wendy, and Legacy, Crystal (2017). Critical Urban Infrastructure. *Urban Policy and Research*, 35(1), pp. 1–6.
- United Nations Office on Drugs and Crime (2014). *State Regulation concerning Civilian Private Security Services and their Contribution to Crime Prevention and Community Safety*. New York: United Nations.
- Żaboklicka, Ewa (2020). Critical infrastructure in the shaping of national security. *Security and Defence Quarterly*, 28(1), 70–81.

PRIVATE SECURITY RESOURCES FOR CRITICAL INFRASTRUCTURE PROTECTION IN URBAN CONDITIONS

SUMMARY

Critical infrastructure includes networks, systems, facilities and assets that ensure the functioning of the state and ensure the basic needs of the population. It represents the environment of every society and as such ensures well-being, prosperity and security. Due to the role it plays in maintaining

functioning, integrity and security in urban areas, it can be considered a significant link of urban security. Different social processes of the modern era have led to changes in the organizational, technical and operational aspects of critical infrastructure, and the interconnectedness, complexity and dependence of these infrastructures has led to the multiplication of risks. Critical infrastructure today is vulnerable to a variety of threats, traditional and modern, including natural disasters, cyber attacks and acts of terrorism. Its vulnerability reflects the vulnerability of society, it represents a high level of risk for overall security, including the security of urban areas. A key segment of critical infrastructure protection is its resilience. Basically, resilience is the ability of a system, network, facility or other element of critical infrastructure to absorb negative impacts, to adapt to them and return to a state of normal or even improved functioning in the most optimal period of time. Therefore, by strengthening the resilience of critical infrastructure in addition to protecting the infrastructure, the resilience of the environment in which it is located is also strengthened, which further contributes to the resilience of society as a whole. One of the providers of critical infrastructure protection, as well as providers of urban security, is the private security sector. In recent decades, this sector or the private security industry, as it is often called, has been a significant entity in the arena of security services, while critical infrastructure is a frequent reference object to which they provide protection. The author pointed out the role that the private security sector plays in urban areas, taking the protection of critical infrastructure as a variable through which she will present that role. The goal of the work is to present theoretical insights into the various resources that the private security sector uses to protect critical infrastructure, which indirectly contributes to security in urban conditions.

KEYWORDS: *private security, critical infrastructure, critical infrastructure protection, urbanity.*