ZBORNIK RADOVA

„ZAŠTITA KRITIČNE INFRASTRUKTURE – OBAVEZE DRŽAVA I MOGUĆNOSTI PRIVATNOG SEKTORA BEZBJEDNOSTI”

Banja Luka, 2021. godine

COLLECTION OF PAPERS

"CRITICAL INFRASTRUCTURE PROTECTION - STATE OBLIGATIONS AND PRIVATE SECURITY SECTOR OPPORTUNITIES"

Banja Luka, 2021

Zaštita kritične infrastrukture – obaveze država i mogućnosti privatnog sektora bezbjednosti

Autori:

Branislav Milosavljević
Dragana Kosić
Dragiša Jurišić
Gjorgji Alceski
Gojko Pavlović
Marjan Gjurovski
Milan Baltić
Milica Sikimić
Nenad Komazec
Nikola Terzić
Tatjana Gerginova
Željko Zorić

Izdavači:
Istraživački centar Banja Luka
Aleja Svetog Save 7A, 78000 Banja Luka, Republika Srpska – BiH
www.thinktankbl.org, istrazivackicentarbl@gmail.com
Sector Security Banja Luka
Siniše Mijatovića 9, 78000 Banja Luka, Republika Srpska – BiH
www.sectorsecurity.org, info@sectorsecurity.org

Za izdavače:
Dr Gojko Pavlović, direktor
Mr Dragana Kosić, direktor

Glavni i odgovorni urednici:
Dr Nikolina Grbić Pavlović
Dr Željko Zorić

Recenzenti:
prof. dr Ljubinko Mitrović
prof. dr Armin Kržalić

Prevod i lektura:
Gordana Višekruna

Kompjuterska priprema:
Stevica Kekić

Štampa:
Glas Srpske A.D.

Za štampariju:
Boris Dmitrašinović

Tiraž:
100 primjeraka

ISBN:
978-99976-914-3-9

Naučni odbor Konferencije:

prof. dr Ljubinko Mitrović, Ombudsmen za ljudska prava BiH i počasni član Istraživačkog centra Banja Luka (BiH)
prof. dr Marjan Gjurovski, prorektor Univerziteta „Sv. Kliment Ohridski" u Bitolju (MKD)
doc. dr Damjan Podparić, docent Univerziteta u Ljubljani (SVN)
doc. dr Armin Kržalić, docent Univerziteta u Sarajevu (BiH)
doc. dr Nikolina Grbić Pavlović, Istraživački centar Banja Luka (BiH)

Programski odbor:

prof. dr Ljubinko Mitrović, počasni član Istraživačkog centra Banja Luka
mr Dragana Kosić, generelani direktor kompanije Sector Security

Sekretarijat konferencije:

dr Gojko Pavlović (BiH), dr Željko Zorić (BiH),

САДРЖАЈ / SADRŽAJ / CONTENT

Dr Gojko Pavlović: DIREKTIVE EVROPSKE UNIJE U OBLASTI ZAŠTITE KRITIČNE INFRASTRUKTURE I KRITIČNE INFORMACIONE INFRASTRUKTURE - UVODNI REFERAT / EUROPEAN UNION DIRECTIVES IN THE FIELD OF CRITICAL INFRASTRUCTURE AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION - INTRODUCTORY PAPER ***str. 1 – 6.***

Др Бранислав Милосављевић, Др Ненад Комазец: КРИТИЧНА ИНФРАСТРУКТУРА И ДРУШТВЕНА БЕЗБЕДНОСТ / CRITICAL INFRASTRUCTURE AND SOCIAL SECURITY ***стр. 7*** – 24

Marjan Gjurovski, PhD, Gjorgji Alceski PhD: THE ROLE OF CORPORATE SECURITY IN THE PROTECTION OF CRITICAL INFRASTRUCTURE ***pp. 25 – 37.***

Tatjana Gerginova, PhD: ANALYSIS OF THE ENERGY INFRASTRUCTURE IN THE REPUBLIC OF NORTH MACEDONIA ***pp. 38 – 49.***

Nikola Terzić, MSc, Milan Baltić: STEPEN UGROŽENOSTI KRITIČNE INFRASTRUKTURE TERORISTIČKIM AKTIVNOSTIMA / DEGREE OF CRITICAL INFRASTRUCTURE VULNERABILITY TO TERRORIST ACTIVITIES ***str. 50 – 64.***

Dr Dragiša Jurišić: OSVRT NA ZAKON O BEZBJEDNOSTI KRITIČNIH INFRASTRUKTURA U REPUBLICI SRPSKOJ / REVIEW OF THE LAW ON SECURITY OF CRITICAL INFRASTRUCTURES IN THE REPUBLIC OF SRPSKA ***str. 65 – 81.***

Dr Željko Zorić, Mr Dragana Kosić: UMREŽENOST ZAKONA O MJERAMA BEZBJEDNOSTI U POSLOVANJU GOTOVIM NOVCEM I DRUGIM VRIJEDNOSTIMA SA ZAKONOM O BEZBJEDNOSTI KRITIČNE INFRASTRUKTURE U REPUBLICI SRPSKOJ / NETWORKING OF THE LAW ON SECURITY MEASURES IN CASH AND OTHER VALUE OPERATIONS WITH THE LAW ON CRITICAL INFRASTRUCTURE SECURITY IN THE REPUBLIC OF SRPSKA
str. 82 – 95.

Милица Сикимић, MA: ПОСЉЕДИЦЕ УГРОЖАВАЊА КРИТИЧНЕ ИНФРАСТРУКТУРЕ ПО НАЦИОНАЛНУ БЕЗБЈЕДНОСТ: ФАКТОР ЗА ИЗГРАДЊУ ПРАВНИХ И ИНСТИТУЦИОНАЛНИХ КАПАЦИТЕТА / CONSEQUENCES OF THREATENING CRITICAL INFRASTRUCTURE ON NATIONAL SECURITY: A FACTOR FOR BUILDING LEGAL AND INSTITUTIONAL CAPACITIES ***стр. 96 – 112.***

PREDGOVOR

Povodom obilježavanja pete godišnjice postojanja i rada Istraživačkog centra Banja Luka, Centar je u saradnji sa kompanijom Sector Security iz Banja Luke organizovao II. Naučno-stručnu konferenciju sa međunarodnim učešćem na temi: ***„Zaštita kritične infrastrukture – obaveze država i mogućnosti privatnog sektora bezbjednosti“.*** Navedena konferencija je održana 21. maja 2021.godine putem video live streaming platforme – Educor.

Cilj konferencije bio je da ukaže na dostignute pravne standarde u Evropskoj uniji u ovoj oblasti, zatim na postojeći strateški i normativni okvir kojim se propisuje obaveza zaštite kritične infrastrukture u Bosni i Hercegovini i zemljama iz regiona, kao i da se ukaže na institucionalne kapacitete i mogućnosti privatnog sektora bezbjednosti na zaštiti kritične infrastrukture.

Namjera nam je bila da na jednom mjestu okupimo predstavnike akademske zajednice, domaće i inostrane stručnjake iz sektora javne i privatne bezbjednosti iz cijelog regiona zemalja Zapadnog Balkana kako bismo ukazali na trenutno stanje u oblasti zaštite kritične infrastrukture, kao i na potrebu za izgradnjom pravnih i institucionalnih kapaciteta u jednom društvu radi preduzimanja različitih aktivnosti kojima je zajednički cilj da obezbijede neprekidno funkcionisanje kritične infrastrukture, odnosno da spriječe njeno ugrožavanje.

Istoimeni Zbornik radova sa konferencije pored uvodnog izlaganja, sadrži sedam naučnih radova koji su u predviđenom roku prijavljeni i dostavljeni za konferenciju.

Ukupno je 12 autora i koautora koji su napisali rad za ovu konferenciju, a oni su predstavnici akademske zajednice, agencija za provođenje zakona, privatnog sektora bezbjednosti, i sektora odbrane iz četiri zemlje: Bosne i Hercegovine, Crne Gore, Sjeverne Makedonije i Srbije.

U Zborniku su radovi objavljeni na srpskom, engleskom jeziku i crnogorskom jeziku.

Posebno smo ponosni na činjenicu da su u Zborniku radova objavljeni radovi mladih akademskih radnika - istraživača, a koji pohađaju doktorske studije, odnosno koji učestvuju u naučnoistraživačkom radu na visokoškolskim ustanovama širom Evrope.

Banja Luka, decembar 2021. godine

Glavni i odgovorni urednici:
Dr Nikolina Grbić Pavlović
Dr Željko Zorić

Uvodno izlaganje

DIREKTIVE EVROPSKE UNIJE U OBLASTI ZAŠTITE KRITIČNE INFRASTRUKTURE I KRITIČNE INFORMACIONE INFRASTRUKTURE[1]

Dr Gojko Pavlović

Koraci Evropske unije na izgradnji unutrašnje bezbjednosti, kao i nastanak prvih politika u ovom području, mogu se posmatrati uporedo sa usvajanjem Amsterdamskog ugovora, krajem XX vijeka, kada je inicirana ideja o stvaranju Evropske unije kao područja slobode, bezbjednosti i pravde. Tada se pristupilo donošenju niza politika s ciljem ostvarivanja prava na slobodu i bezbjednost kretanja unutar unije.

DIREKTIVA O UTVRĐIVANJU I OZNAČAVANJU EVROPSKE KRITIČNE INFRASTUKTURE I PROCJENI POTREBE POBOLJŠANJA NJENE ZAŠTITE IZ 2008.GODINE

Neposredno sa usvajanjem Evropske strategije bezbjednosti iz 2003.g., u aprilu 2004. godine Evropski savjet je pokrenuo inicijativu za izradu cjelovite strategije kojom bi se zaštitila kritična infrastruktura. Kao odgovor na ovaj zahtjev Evropskog savjeta, Evropska komisija je 20. septembra iste godine usvojila *Komunikaciju o zaštiti kritične infrastrukture u borbi protiv terorizma*, u kojoj su izneseni prijedlozi koji bi evropi omogućili adekvatnije sprečavanje terorističkih napada kojima su direktno pogođeni objekti ili subjekti kritične infrastrukture. Ovim dokumentom se predviđalo unapređenje reakcije na takve situacije, te spremnost da se na njih odgovori. Takođe, Evropska komisija je 2005. godine usvojila *Zelenu knjigu o evropskom programu zaštite kritične infrastrukture*, u kojoj se nude moguća rješenja za uspostavljanje programa i informacione mreže za uzbunjivanje radi zaštite kritične infrastrukture. Iste godine je Savjet za pravosuđe i unutrašnje poslove zatražio od Evropske komisije izradu prijedloga *Evropskog programa zaštite kritične infrastrukture* kojim su se u obzir uzele sve opasnosti, pri čemu je primat dat suprotstavljanju terorističkim prijetnjama. Tako je Evropski savjet 2007. godine usvojio

[1] Vidjeti više kod: Pavlović, G., Kosić, D., 2021, „Obaveza zaštite kritične energetske infrastrukture - evropski standardi i domaće zakonodavstvo“, u: Zbornik radova sa Naučno – stručne konferencije *Istočna ili Južna interkonekcija, politika ili ekonomija?*, Centar za lobiranje, Banja Luka.

zaključke o ovom programu, a kojima se ponovno naglašava da je konačna odgovornost za upravljanje rješenjima za zaštitu kritičnih infrastruktura na državama članicama. Konačno, Savjet donosi prvi dokument čiji je osnovni cilj upravo utvrđivanje i označavanje kritične infrastrukture i procjene njihove zaštite, a to je *Direktiva o utvrđivanju i označavanju evropske kritične infrastukture i procjeni potrebe poboljšanja njene zaštite iz 2008.godine*.[2]

Prema članu 2. Direktive „kritična infrastruktura je imovina, sistem ili njihov dio koji se nalazi u državama članicama i neophodan je za održavanje vitalnih društvenih funkcija, zdravlja, bezbjednosti, zaštite, ekonomije i socijalne dobrobiti ljudi, a čiji bi poremećaj rada ili čije bi uništenje, kao posljedica neuspjelog održavanja tih funkcija, moglo imati znatan učinak u državi članici". S druge strane, definisano je i pitanje evropske kritične infrastrukture – tzv. EKI. EKI je kritična infrastruktura koja se nalazi u državama članicama, a čiji bi poremećaj u radu ili čije bi uništenje imalo znatan učinak na najmanje dvije države članice.

Direktivom Evropske unije data je i definicija zaštite kritične infrastrukture. Naime, pod zaštitom podrazumijevaju se sve djelatnosti koje imaju za cilj osigurati funkcionalnost, neprekidnost i cjelovitost kritičnih infrastruktura kako bi se odvratila, ublažila ili neutralisala prijetnja, rizik ili slabost.

Utvrđivanje kritične infrastrukture podrazumijeva da svaka država članica utvrđuje potencijalne EKI-je koji ispunjavaju međusektorska i sektorska mjerila, a koji odgovaraju definicijama „kritične infrastrukture" i „evropske kritične infrastrukture".

Međusektorska mjerila obuhvataju: a) broj žrtava (koji se procjenjuje s obzirom na mogući broj mrtvih i ranjenih); b) privredne posljedice (koje se procjenjuju s obzirom na značaj privrednog gubitka i/ili srozavanje kakvoće proizvoda ili usluga; uključujući mogući uticaj na okolinu) i v) uticaj na javnost (koji se procjenjuje s obzirom na uticaj na povjerenje javnosti, tjelesne patnje i remećenje svakodnevnog života; uključujući gubitak osnovnih usluga) (član 2. stav 3. Direktive).

Svakako da se ova mjerila moraju prilagoditi karakteristikama pojedinih sektora eki-ja. ukoliko na nivou unije ili u državama članicama već postoje određene sektorske mjere, a koje se već bave zaštitom kritične infrastukture i kojima se postižu pozitivni rezultati u toj oblasti, trebalo bi ih i dalje nastaviti sprovoditi, a direktivom ih samo dopuniti.

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

Svaka država članica obavještava druge države članice čiji EKI bi mogao imati znatan nepovoljan učinak o njegovom postojanju i o njegovim razlozima za njegovo označavanje potencijalnim EKI-jem.

Država članica koja smatra da bi potencijalni eki na nju mogao imati znatan nepovoljni učinak, ali ga država članica na čijem se državnom području nalazi nije utvrdila kao takvog, može obavijestiti komisiju o svojoj želji da se uključi u bilateralne i/ili multilateralne rasprave o tom pitanju.

Važniji ciljevi direktive jesu uspostavljanje *bezbjednosnih planova (član 5. Direktive)* i postavljanje *službenika za bezbjednost (član 6. Direktive).* Bezbjednosnim planovima utvrđuje se važna imovina, zatim vrši procjena rizika, te u odnosu na prethodno utvrđuju i definišu prioriteti za primjenu adekvatnih mjera i postupaka za zaštitu. Svaka država članica ocjenjuje da li svaki označeni EKI koji se nalazi na njenom području ima svoj plan i da li postoje mjere kojima se već djeluje po pitanjima koja sačinjavaju navedeni plan. Ova pitanja utvrđena su u prilogu ii direktive.

Datim planom, najprije, potrebno je utvrditi imovinu kritične infrastrukture i bezbjednosna rješenja koja postoje ili se primijenjuju radi njihove zaštite.

Prema odredbama priloga iz direktive postupak izrade bezbjednosnog plana obuhvata najmanje: utvrđivanje važne imovine, zatim analizu rizika na osnovu glavnih prijetnji imovini, te u odnosu na prethodno obuhvata obavezu utvrđivanja i odabira prioriteta za primjenu adekvatnih mjera i postupaka za zaštitu. ove mjere i postupci mogu biti trajne bezbjednosne mjere kojima se utvrđuju neizostavna bezbjednosna ulaganja i sredstva za koja je važno da su trajno angažovana.

Na primjer, tehničke mjere - postavljanje sredstava za nadzor, kontrolu pristupa, zaštitu i sprečavanje; organizacione mjere - postupci za uzbunjivanje i upravljanje krizama; mjere za nadzor i provjeru; komunikaciju; podizanje svijesti i osposobljavanje, te bezbjednost informacionih sistema) i mogu biti privremene bezbjednosne mjere koje se koriste u zavisnosti od različitih stepena rizika i prijetnji.

Ukoliko država članica ustanovi da ne postoji ovakav bezbjednosni plan ili da nisu pripremljene adekvatne mjere za zaštitu, nastojaće da se osigura donošenje bezbjednosnog plana zaštite prema navedenim pitanjima iz priloga ii direktive.

Takođe, svaka država članica osigurava redovno preispitivanje plana i mjera u roku od jedne godine nakon što je kritična infrastruktura označena kao EKI taj se rok pod posebnim okolnostima može produžiti uz saglasnost nadležnog tijela države članice i uz obaviještenje Komisije.

Važna obaveza po direktivi jeste i određivanje *službenika za bezbjednost i vezu* kako bi se olakšala saradnja i komunikacija sa državnim

tijelima za zaštitu kritične infrastrukture. službenik za bezbjednost i vezu zadužen je za bezbjednost i djeluje kao kontakt tačka za bezbjednosna pitanja između vlasnika/operatera eki-ja i odgovarajućeg tijela države članice. takođe, svaka država članica uspostavlja odgovarajući mehanizam za komunikaciju između odgovarajućeg državnog tijela i službenika za bezbjednost, kao i vezu radi razmjene odgovarajućih informacija o utvrđenim rizicima i prijetnjama u odnosu na dotični EKI.

Kao važna karakteristika, koja bi svakako podrazumijevala dodatnu efikasnost u radu na zaštiti kritične infrastrukture, jeste ta da se u svakoj državi članici imenuje kontakt tačka koja bi koordinisala pitanjima koja su u vezi sa zaštitom evropske kritične infrastrukture u zemlji, ali i sa drugim državama članicama i Evropskom komisijom.

Direktivom je regulisana i zaštita podataka o zaštiti EKI-ja, koja podrazumijeva da svaka osoba, koja raspolaže informacijama u skladu s ovom direktivom, prolazi odgovarajuće bezbjednosne provjere. države članice, komisija i odgovarajuća nadzorna tijela osiguravaju da se informacije o zaštiti evropske kritične infrastrukture koje se podnose državama članicama ili komisiji ne koriste ni u koju drugu svrhu osim zaštite kritičnih infrastruktura. Ova pravila se odnose i na nepisane informacije koje se razmjenjuju na sastancima na kojima se raspravlja o osjetljivim temama.

Direktiva EU 2008/114/EC direktno se usmjerava na zaštitu kritične infrastrukture u sektorima energije i prevoza, ali se ne ograničava samo na ove sektore te se ističe da se mogu odrediti kritične infrastrukture i iz drugih sektora, a daje se prednost informaciono komunikacionim tehnologija. Iz ova dva sektora posebno su kao podsektori navedeni:

SEKTOR	PODSEKTOR	
I. Energetika	1. Električna energija	Infrastruktura i objekti za proizvodnju i prenos električne energije vezano za snabdijevanje električnom energijom
	2. Nafta	Proizvodnja, rafiniranje, prerada, skladištenje i prenos nafte naftovodima
	3. Gas	Proizvodnja, rafiniranje, prerada, skladištenje i prenos gasa gasovodima
II. Prevoz	4. Drumski prevoz 5. Željeznički prevoz 6. Vazduhoplovni prevoz 7. Prevoz kopnenim plovnim putovima	

	8. Prekookeanski prevoz i pomorski prevoz na kratkim udaljenostima i lukama

Definisanje i određivanje kritičnih infrastruktura, naročito izrada metodologije procjenjivanja rizika i njihove ugroženosti, u isključivoj je nadležnosti država članica Evropske unije.

DIREKTIVA O MJERAMA ZA VISOKI ZAJEDNIČKI NIVO BEZBJEDNOSTI MREŽNIH I INFORMACIONIH SISTEMA U EU - NIS DIREKTIVA

Direktiva o mjerama za visoki zajednički nivo bezbjednosti mrežnih i informacionih sistema u EU - NIS Direktiva, je usvojena 2016. godine, a države članice su imale rok do 09. maja 2018. godine da transponuju odredbe direktive u nacionalna zakonodavstva, kao i da do 09. novembra 2018. godine identifikuju operatore sistema koji pružaju usluge od posebnog značaja[3].

U ovoj Direktivi se pozivaju sve države članice da propišu osnovne standarde bezbjednosti nacionalnih mrežnih i informacionih sistema, a posebno da: usvoje strategiju za mrežnu i informacionu bezbjednost (NIS); usvoje kooperacioni plan za NIS; uspostave kompetentni autoritet za NIS i uspostave tim nadležan za odgovore na bezbjednosne računarske incidente (*Computer Security Incident Response Team - CSIRT)*.

Prema tome, NIS Direktivom najprije se propisuju obaveze državama članicama u oblasti uspostavljanja strateškog i pravnog okvira.

U tu svrhu, državama članicama je savjetovano da izrade nacionalne strategije koje će uključiti sve relevantne dimenzije društva i privrede.

Direktivom se takođe određuje i da bezbjednosne mjere treba da budu zasnovane na principu upravljanja na osnovu procjene rizika, što je kultura koja treba da bude razvijena kroz odgovarajuće regulatorne okvire, kao i na osnovu postojećih praksi u različitim branšama.

U pogledu kritične informacione infrastrukture, NIS Direktiva propisuje da su države članice odgovorne za utvrđivanje kritične infrastrukture u oblasti koju Direktiva uređuje. NIS Direktiva u stvari prepoznaje dvije vrste subjekata: operatore IKT sistema koji pružaju usluge od posebnog značaja (*eng. operators of essential services*) i pružaoce digitalnih usluga (*eng. digital services providers*).

[3] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. Official Journal of the European Union L 194/1.

Aneksi II i III sadrže spisak usluga koje spadaju u prvu grupu, na osnovu kojeg se može utvrditi da li određeni pružalac usluga spada u pružaoce usluga koje su posebno značajne za održavanje ključnih društvenih i ekonomskih aktivnosti (usluge od posebnog značaja). Spisak usluga zapravo izjednačava ovu grupu sa operatorima kritične infrastrukture u koju spada sljedeće: Energetski sektor (struja, nafta i gas); Sektor transporta (vazdušni, željeznički, vodni i drumski transport); Bankarski sektor; Infrastrukture finansijskog tržišta; Zdravstveni sektor (zdravstvene ustanove, uključujući bolnice i privatne klinike); Snabdijevanje i distribucija vode za piće i Digitalna infrastruktura (IXP, pružaoci usluga DNS i registri domena TDL) (Aneks II). Onlajn tržište; Onlajn pretraživač i Usluga računarstva u oblaku (*eng. cloud computing*) (Aneks III).

Države članice su dužne da redovno, a najmanje jednom u dvije godine, ažuriraju spisak identifikovanih pružalaca usluga od posebnog značaja na svojoj teritoriji, kao i metodologiju za identifikaciju i klasifikaciju navedenih pružalaca usluga po značaju, kao i da o tome obavijeste Evropsku komisiju.

Kompetentni autoritet je najznačajnija institucija sa obavezama da prati primjenu NIS Direktive na nacionalnom nivou, da sarađuje sa nacionalnim kompetentnim autoritetima drugih država članica, sa odgovarajućim bezbjednosnim službama i autoritetima za zaštitu podataka u svojoj zemlji i da prima i postupa po prijemu obavještenja o incidentima kod javne administracije i javnih operatora telekomunikacionih i informacionih usluga.

Pored kompetentnog autoriteta, predviđeno je da svaka država članica formira i sljedeće tijela:

- Autoritet za informacionu bezbjednost (IAA);
- Autoritet za tempest (TA);
- Autoritet za odobravanje kriptografskih rješenja (CAA) i
- Autoritet za distribuciju kriptografskih materijala (CDA).

***

Imajući u vidu značaj usklađivanja domaćih pravnih propisa sa propisima Evropske unije, sa aspekta zaštite kritične infrastukture u budućnosti je potrebno najprije na normativnom, a potom i na institucionalnom nivou, u skladu sa najboljim uporednim rješenjima pristupiti izradi zakonskih i podzakonskih dokumenata, zatim izradi strateških i akcionih planova, te donošenju adekvatnih bezbjednosnih planova kojima bi se detaljno regulisalo ovo pitanje.

Оригинални научни чланак

КРИТИЧНА ИНФРАСТРУКТУРА И ДРУШТВЕНА БЕЗБЕДНОСТ

Др Бранислав Милосављевић[1]
Др Ненад Комазец[2]

Абстракт: Догађаји са негативним деловањем који нарушавају безбедност друштвених заједница последњих деценија,имају за последицу масовна страдања цивилног становништва, материјалних добара и животне средине. Савремено друштво се суочава са бројним изазовима и претњама повезаним са рањивостима техничко-технолошке и социо-демографске природе. Њихова разарајућа природа је најчешће последица удруженог деловања техничких, социјалних и економских чинилаца. Без обзира на разноврсност узрока и последица, неке заједничке каракатеристике описују већину опасности које долазе од природних катастрофа, терористичких напада, техничко- технолошких акцидената и других несрећа које погађају савремени свет. Психолошко дејство, комплексност, међузависност и мултидимензионалност су им заједничка обележја, која су питања управљања кризама одвели у саме приоритете светске политике и политике националне безбедности разних земаља.

Многе кризе потврђују правило да су безбедносне претње такве природе да се може говорити о рањивости угрожене инфраструктуре. Различити су приступи али постоје заједнички напори појединаца, организација, приватног сектора и влада у припреми, превенцији, одговору и опоравку фундаменталних функција државе и друштвених вредности. Према Кековићу и Кешетовићу, подела на државне и друштвене функције је овде ирелевантна, будући да се ангажују сви капацитети друштва и у свим кључним фазама неке ситуације која има потенцијал да изазове кризу. Исти аутори, даље сматрају да овакав, у основи холистички приступ у управљању кризама, наглашава интеоперабилност кључних актера у превенцији и одговору на кризне ситуације и, оно што га разликује од многих сличних концепата, комбиновани приступ одоздо на горе и одозго на доле у препознавању безбедносних претњи, хазарда и одговора на њих. Евидентно је да је критична инфраструктура значајан чиниалц друштвене безбедности.

Кључне речи: критична инфраструктура, друштвена безбедност, ризик, заштита

---

[1] Универзитет одбране, Институт за стратегијска истраживања, Београд, Србија
[2] Универзитет одбране, Војна академија, Београд, Србија.

ЕЛАБОРАЦИЈА ПРОБЛЕМА

Концепт „критичне инфраструктуре“ стар је колико и друштвене заједнице, па се с правом може тврдити да је уједно и пратилац развоја људске цивилизације. Наиме, још у старом Риму, критичну инфраструктуру представљали су првенствено аквадуктии путеви који су били првенствено војног карактера. С друге стране аквадукти су обезбеђивали питку воду становништву, што у датом тренутку није представљало само иновативно технолошко решење, већ и питање здравља и санитарних потреба. На далеком истоку, кинески зид је представљао критичну инфраструктуру, а пружао је заштиту од освајачаи уједно омогућавао несметан економски, војни и културни развој. За Шпанију као колонијалну силу, критичну инфраструктуру сачињавали су између осталог рудници злата у Јужној Америци, као и луке и флота која је транспортовала овај драгоцени метал у земљу.[3] Очигледно је да је критична инфраструктура постојала од настанка потребе за безбедношћу и сигурношћу људских заједница.

Током друге половине 19. века, инфраструктурни ресурси и индустријска постројења која су била од посебне важности за војску као и економски и друштвени развој налазила су се у фокусу пажње креатора политика националних држава. Зато с правом можемо тврдити да је однос према критичној инфраструктури крајем 19. и почетком 20. века, представљало подстицање спровођења национализације у овој области. То је посебно било изражено у Европи где су политичке, војне и економске користи од ширења и стандардизације инфраструктуре биле усмерене на чврсто повезивање са државом или јавним сектором.

У периоду хладног рата, критична инфраструктура је првенствено разматрана као саставни елемент државних и војних планова. У периоду релативног мира 80-тих година прошлог века дошло је и до занемаривања проблематике критичне инфраструктуре. Међутим, треба напоменути да је у истом периоду дошло до постепеног повећања ризика за друштво у целини услед намерних и ненамерних поремећаја критичне инфраструктуре. С друге стране у савременом друштву и начину живота, технички системи, посебно информациони у контроли и управљању снабдевања енергијом, саобраћајем и ресурсима питке воде имају прворазредни значај. При томе треба, напоменути да су процес глобализације и развој информационе технологије у многоме допринели

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

да критична инфраструктура постане комплексан систем, међусобно зависан али и осетљив на различите утицаје. Поједини политички, економски, друштвени као и еколошки догађаји а посебно терористички напади, глобална економска рецесија, елементарне непогоде, нуклеарни инциденти, пожари у појединим деловима света указали су да је човечанство у савремено доба знатно угроженије од различитих катастрофа у односу на ранији период. То је између осталог указало на међузависност критичне инфраструктуре. С друге стране, опстанак, безбедност и просперитет нације или државе, у многоме је повезан са критичним системима који морају бити на адекватан начин организовани, управљани и заштићени. Разлог наведеном је да сви елементи критичне инфраструктуре морају да издрже различите унутрашње и спољне утицаје на начин да буду обезбеђени основни услови за задовољавање потреба друштва и функционисање националних установа[4].

Почетак 21. века је између осталог обележио и поновно враћање на фокус заштите критичне инфраструктуре нарочито на Западу, као последица појачане забринутости за обезбеђивање појединих основних потреба као што су енергија и транспорт. Међутим, уместо ранијег фокуса на опасности од оружаних сукоба великих размера, све више долазе до изражаја „нове“ неизвесности првенствено од све веће сложености и међузависности критичних инфраструктура. Зато се уместо опасности од конвенционалног војног сукоба све више разматрају све присутније сајбер претње у условима међусобно повезаних и умрежених критичних инфраструктура. Као пример наведеном, је појава „миленијумске грешке“, односно проблемом са уношењем и архивирањем података са почетка 2000-те године.[5] И без даљег елаборирања, савремено доба и технолошки развој је између осталог утицао на проширење садржаја и обима критичне инфраструктуре. Међутим и поред тога, значај многих класичних система критичне инфраструктуре остао је непромењен.

ГЕНЕЗА СИНТАГМЕ „КРИТИЧНА ИНФРАСТРУКТУРА“

Иако историја указује, да је критична инфраструктура пратилац развоја људске заједнице, сам појам је релативно новијег датума. У научној и стручној литератури интензивније се употребљава након

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

[5] de Bruijne Mark, van Eeten Michel: „Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment“, Journal of Contigencies and Crisis Management, Vol 15, Issue 1, March 2007, p. 26

терористичких напада у САД у септембру 2001. године. Као последица неистражености, у теорији не постоји потпуна сагласност о садржини тог појма и концепта. С друге стране, евидентно је да питањима дефинисања критичне инфраструктуре у највећој мери одређују законским актима и стратешким документимаодређених институција националних држава, као и органа наднационалних организација попут ОУН, Европске уније, НАТО и ОЕБС-а. Појам "инфраструктура" може се одредити као „основни оквир система или организације". Када је реч о синтагми„критична инфраструктура" постоје различите одреднице, као последица променљивости и вишезначности појма „критичан". Етимолошки посматрано појам критичност потиче од грчког израза κρίσις (криза), који је најчешће коришћен у медицинске сврхе да опише тренутак у току болести у коме се одређује судбина пацијента (преживљавање или смрт).На почетку Хладног рата, појам критичност је уврштен у стратегију цивилне одбране Сједињених Америчких Држава, где је употребљаван у контексту „мапирања рањивости", као начин процене угрожености виталних делова инфраструктуре државе, односно важне техничке инфраструктуре[6]. То је уједно и почетак интензивнијег коришћена за идентификацију организација и институција које су на одређен начин који начин релевантне или прекопотребне за континуитет снабдевања становништва и привреде добрима и услугама.

Све до краја прошлог века, појам инфраструктура се првенствено односио на јавне радове и објекте којим се управља у јавном власништву као што су на пример путеви, мостови, водоводи, аеродроми, морске луке, јавне зграде и слично. У модерно доба критична инфраструктура садржи објекте, мреже, системе и структурефизичке и организационе, који пружају основне услуге припадницима друштвене заједнице. То омогућава континуирано функционисање друштва на одређеном простору. Поред тога, критична инфраструктура је од виталне важности за заједницу или нацију, јер у околностима њеног ометања, оштећења, уништења или неког другог разлога нефункционисања, може остварити негативан утицај на безбедност, економију, национално здравље, добробит становништва и привредног пословања. При томе не треба искључити могућност значајних губитака живота у околностима када недостаје пружање оних услуга које критична инфраструктура омогућава[7].

---

[6] Collier J. Stephen, Lakoff Andrew: "Distributed Preparedness: The Spatial Logic of Domestic Security in the United States", *Environment and Planning D: Society and Space*, Vol. 26, Issue 1, SAGE Journals, Thousand Oaks CA, 2008, pp. 12–16

[7] Pesch-Cronin A. Kelley, Marion E. Nancy, *Critical Infrastructure Protection, Risk Management, and Resilience – A Policy Perspective*, CRC Press, Boca Raton FL, pp. 4-5.

Поред појмовног нејединства у дефинисању, евидентна је дилема и у одређењу садржаја и обима критичне инфраструктуре. С тим у вези издвајају се два најважнија начина. При начин је просто набрајање свих виталних инфраструктура заједнице. То је уједно и пример у једном од првих докумената ове врсте и то Национална стратегија САД за физичку заштиту критичне инфраструктуре и кључних материјалних добара из 2003. године[8]. У односу на претходни, други приступ је сложенији јер представља резултат специфичних карактеристика система, његових релационих својстава у односу на друге системе или ентитете. Пример наведеном је, немачка национална стратегија за заштиту критичне инфраструктуре у којој се дефинише критичност као релативна мера за последицу поремећаја или неуспеха функције у вези са испоруком добара и услуга друштву[9]. Током раног периода хладног рата, појам критичности је укључен у стратегију цивилне одбране Сједињених Држава, где је коришћен у контексту „мапирања рањивости“, као врста процене виталних делова државе, односно важне техничке инфраструктуре[10]. То је уједно и почетак интензивније употребе предметног појма у политичким и другим дебатама ради означавањаи идентификације организација и институција које су на било који начин важне, релевантне или неопходне за континуитет снабдевања становништва и привреде добрима и услугама.

Поред наведног, евидентно је да у стратешким документима и законским актима савремених држава у неким случајевима могу имати извесне разлике у критеријумима који се користе за дефинисање критичности (критеријуми који покривају све инфраструктуре у свим секторима, секторски критеријуми, критеријуми који апострофирају сврху критичне инфраструктуре).[11] Поред тога, треба напоменути да геополитички, геостратешки и географски положај земље утиче на одређивање сектора и подсекторе критичне инфраструктуре, што је евидентно на примеру држава које имају нуклеарни потенцијал или поморских држава и слично.

И поред наведених разлика, заједничко за све је тренд повећања обима и садржаја критичне инфраструктуре, што се између осталог одражава и на дефиниције критичне инфраструктуре које постају све

---

[8] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, United States Government, Washington DC, 2003

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

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

[11] Lazari Alessandro, *European Critical Infrastructure Protection*, Springer International Publishing, Cham CH,2014, p.3.

екстензивније. И без анализирања националних одређења критичне инфраструктуре, постоје поједини специфични случајеви. Тако на пример у Италији „критична инфраструктура подразумева системе, ресурсе, процесе, структуре, укључујући виртуелне, чије уништавање, прекид или чак делимична или привремена недоступност има за последицу значајно слабљење ефикасности и нормалног функционисања земље, као и угрожавање безбедности и економских, финансијских и социјалних система, укључујући централне и локалне органе јавне управе“.[12]

С друге стране у Француској се употребљава појам витална уместо критична са основним значењем основне услуге или инфраструктуре. С тим у вези „витална инфраструктура обухвата сваку установу, постојење или структуру, чија недоступност или уништење као резултат злонамерног деловања, саботаже или терористичке акције могу директно или индиректно да изузову штету, посебно ако је њихова делатност тешко заменљива, озбиљно угрожава одбрамбени или економски потенцијал, националну безбедност, опстанак нације, или озбиљне утичу на здравље или живот становништва“[13]

Знатно једноставније решење је у случају Швајцарске где „критична инфраструктура обухвата процесе, системе и објекте који су неопходни за функционисање економије и благостање становништва“.[14] У Европској унији, под критичном инфраструктуром означава се „имовина, систем или његов део који се налази на територији земље чланице и који је неопходан за одржавање кључних друштвених функција, здравства, безбедности, сигурности, економског или социјалног благостања, а чије би ометање или уништење имало значајан утицај на земљу чланицу”.[15]

Евидентно је да не постоји општеприхваћена дефиниција критичне инфраструктуре, јер је то питање које се пре свега тиче националне регулативе данашњих држава. Поред тога, постоје и различити

---

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

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

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

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

критеријуми идентификације и утврђивања листе инфраструктуре која ће се у одређеној земљи сматрати критичном. Иначе, према документима Европске уније, критичне инфраструктуре морају бити дефинисане и пописане у свим државама чланицама, као и у земљама које претендују да постану пуноправне чланице ЕУ.

У анализи предметног појма, треба напоменути да се често упоредо употребљавају изрази критична инфраструктура и критична информациона инфраструктура, као различити, али међусобно повезани појмови. Наиме, критична инфраструктура укључује и критичну информациону инфраструктуру, која представља њен саставни део. Нефункционисање информационе инфраструктуре може довести до прекида функционисања укупне критичне инфраструктуре, али критична инфраструктура може бити угрожена и због низа других разлога који нису повезани са информационом инфраструктуром[16].

САВРЕМЕНИ ТРЕНД РАЗВОЈА„КРИТИЧНЕ ИНФРАСТРУКТУРЕ“

Савремени концепт критичне инфраструктуре карактерише измењена перцепција претњи и повећане међузависностиизмеђу разних инфраструктурних елемената. То је утицало да критична инфраструктура поприми све већи обим, садржај и сложеност, а потенцијалне претње и угрожавања представљајупрворазредни значајза националну безбедност. Појам критичне инфраструктуре обухвата објекте као што су зграде, путеви и транспортни, телекомуникациони, водоводни и енергетски системи, хитне службе, банкарске и финансијске институције и извори снабдевања као и виртуелни (сајбер) простор. Уопштено посматрано, критичну инфраструктуру чине различити системи који су потребни за несметано функционисање управљања заједницом на свим нивоима.[17]

Првенствено због широког обима који обухватаи разноликости садржаја који су по својој природи мултидисциплинарни, дефинисање појма критична инфраструктура је сложен поступак. Сам појам “инфраструктура” може се дефинисати као “основни оквир система или организације” док се за синтагму “критична инфраструктура” може употребити мноштво дефиниција, с обзиром да је појам „критичан“ променљив и садржи широк спектар елемената.Проблему сложености

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

[17] Kelley A., Pesch-Cronin N., MarionE. (2016). Critical infrastructure protection, risk management, and resilience: a policy perspective, Taylor & Francis Group, 2016, p. 4

доприносе и вештачке мреже и системи који пружају неопходне услуге широком кругу становништва.[18]

Из научногугла посебно је значајан приступ, који дефинише критичност као резултат специфичних особина. У овом случају утврђују се одређена релациона својства система, јер је дати систем критичан у односу на друге системе или целине. Наиме, систем је критичан за други систем када је први неопходан да би се наставило са радом другог. Тако немачка национална стратегија за заштиту критичне инфраструктуре дефинише критичност као релативну меру за последице поремећаја или неуспеха функције у вези с испоруком добара и услуга друштву.[19] У том смислу, критична инфраструктура је инфраструктура која је потребна да би се наставило са радом других већих техничких и (или) друштвених система или који су потребни за обезбеђивање робе или услуга које се сматрају виталним за функционисање модерног друштва.[20]И без даљег навођења, можемо уочити да суштински проблем у дефинисању појма представља појам„критичност“. С тим у вези, значајно је одређење по коме је „одређен систем критичан ако обезбеђује рутинске функције, ако не постоје практичне могућности брзе замене, изненадна дисфункција која узрокује нетривијалне штете и ако је уграђен у интегрисане системе”.[21]При покушају разумевања обима и потенцијалапојма криза, једнако је важно испитати и његове метафоричке ефекте. Појава светске кризе и услови повезани са кризом евоцирају слике радикалне промене, као такавпојам криза постао је у модерној историји синоним за појмове као што су побуна, конфликт или револуција.[22]

Уобичајено је да критична инфраструктура обухвата саобраћај, транспорт, производњу и дистрибуцију енергије, информационе и комуникационе системе, здравствене службе, системе за снабдевање водом и храном, финансијске службе, државну инфраструктуру и слично. У околностима евентуалног делимичног или потпуног отказивања ових инфраструктура долази до угрожавања друштва и у крајњој линијии националне безбедности. То је један од разлога што многе државе настоје

[18] Kelley A., Pesch-Cronin N., MarionE. (2016). Critical infrastructure protection, risk management, and resilience: a policy perspective, Taylor & Francis Group, 2016, p. 4-5

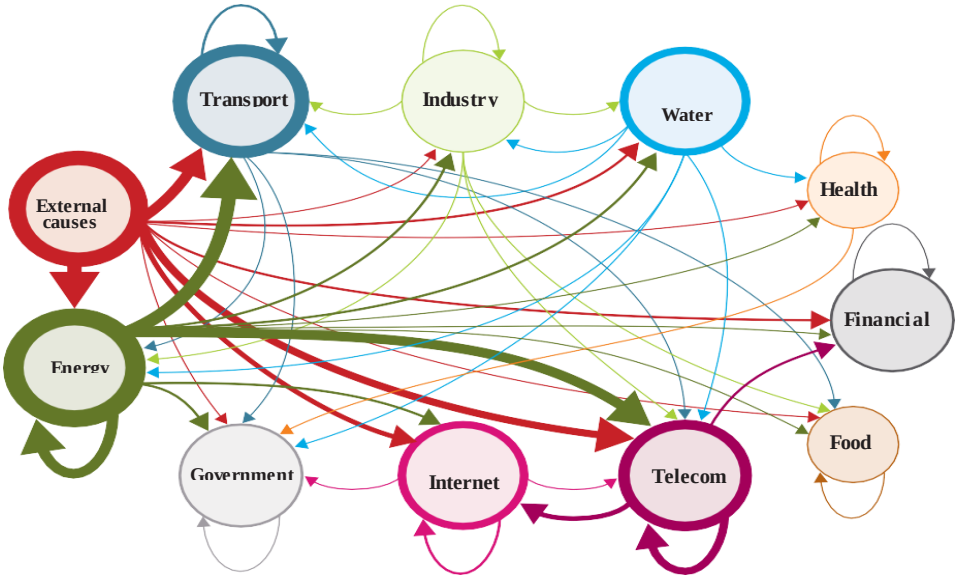
[19] Bundesministerium des Innern. Bundesministerium des Innern Nationale Strategie zum Schutz Kritischer Infrastrukturen. Berlin, 2009, p. 7

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

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

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

да идентификују и анализирају критичне секторе као и подсекторе, процесе и објекте уз употребу различитих методолошких приступа. Међутим, сама сложеност инфраструктурних система је највећи заједнички проблем свих држава које су приступиле идентификовању и изградњи политике заштите критичне инфраструктуре.[23]



Слика бр.1 : Пример повезаности критичне инфраструктуре[24]

КОНЦЕПТ ДРУШТВЕНЕ БЕЗБЕДНОСТИ БАЗИРАН НА ОЧУВАЊУ ФУНКЦИЈЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Концепт друштвене безбедности је универзалан и јединствен. Друштвена безбедност је релевантна за све функције у друштву и то је разлог што је политичку, економску, техничку, регулаторну, правну и социјалну динамику и промене у безбедносном окружењу тешко описати другим термином.[25] Референтни објекат проучавања друштвене безбедности у оквиру савремених студија безбедности су друштво и друштвене групе. С обзиром да се друштвене групе разликују по многим

[23] Lewis T.: Infrastructure Protection in Homeland Security, Defending a Networked Nation, Wiley Interscience, 2006, p. 32

[24] Luiijf Eric et al: The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, TNO, Netherlands, 2016, p. 26

[25] Кековић, З., Кешетовић, Ж.: Друштвена безбедност у Србији, Српска политичка мисао, број 1-2/2008, год.15. vol. 20.,стр.181-200.

карактеристикама, неопходна је стандардизација процеса, процедура и културе управљања кризама.Стандардизација у разним областима функционисања друштва, допринела једа се појам друштвене безбедности изједначава са способности организације да се суочи са претњама и поремећајима.У основи овог организационог приступа је управљање безбед- ношћу на основама друштвено одговорног понашања.

Промена концепта управљања у безбедности подразумева комплексан систем функционално различитих мрежа које укључују различите актере на разним нивоима одговорности.Пракса друштвене безбедности, нпр, на државном нивоу, показује како се најбоље може управљати безбедношћу посредством нетрадиционалних питања безбедности, прецизније, утицајем на безбедносне изазове (еколошке, демографске, техничко-технолошке) на начин којим се штите природни ресурси, умањује штетност по становништво и материјалне ресурсе.[26]

Имајући у виду чињеницу да је неопходна, чак и пресудна потреба синхронизације послова на остваривању функција безбедности друштва, стандарди у области друштвене безбедности су важни завећину функција друштва и организација које их остварују.Више димензионални приступ који је претпоставка истраживања у области друштвенебезбедности захтева фундаменталну културолошку промену у оквиру друштва, укључујући прихватање неизвесности и несавршености на свим нивоима. Сви нивои друштва треба да имају у виду да је ризик неодвојив од сваке одлуке и активности, и да одступање од планских циљева има потенцијал да креира негативан догађај. Руководиоци на свим нивоима управљања друштвеним заједницама требају сходно томе да размотре како ће друштвена заједница реаговати на негативне догађајеу односу на постављене циљеве.

ЗНАЧАЈ И ВАЖНОСТ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ОДНОСУ НА ДРУШТВЕНУ БЕЗБЕДНОСТ

Државне политике, стратегије, доктрине и поједине директиве приступају проблематици критичне инфраструктуре на различите начине, али увек ради успостављања ефикасне инфраструктуре која је од виталног значаја за развој економије и национални прогрес. Адекватно и функционално осмишљена инфраструктура је основни покретач националног просперитета и представља предуслов за економску експанзију и будући раст, што између осталог омогућава националну

[26] Исто

продуктивност, квалитет живота и економску прогресију кроз покретање раста, стварање радних места и слично. Она подстиче раст тако што обезбеђује широку мрежу подршке на коју се ослања целокупнодруштво. Умрежена инфраструктура, као што су на пример транспорт и комуникације, подстиче дугорочни економски учинак, јер пружа корист другим секторима, али доприноси побољшању ефикасности пословања и уједно подстиче стварање ефикасних механизама за координацију и управљање ланцима снабдевања и испоруку производа. Отпорне и поуздане мреже обезбеђују пословно самопоуздање што доводи до повећања пословних инвестиција и раста и стварања нових економских могућности. Улагање у инфраструктуру и начин управљања овим инвестицијама такође може имати значајан утицај на економске циљеве владе. Зато су инвестиције у инфраструктуру неопходне за функционисање економије и доприносе ефикасности пословања, повезаности и пословном расту, што између осталог може довести до повећања поверења у постојећу и будућу инфраструктуру.[27]

Распрострањена и ефикасна инфраструктура представља и кључ за осигурање ефикасног функционисања привреде, јер је иста важан фактор у одређивању локације инвестицијских улагања и одређивању врста економских активности, као и сектора који се могу развијати у одређеној држави. Поредтога, добро развијена инфраструктура смањује и ефекат удаљености између региона, интегришући национално тржиште и повезујући га са другим тржиштима, уз истовремено смањење трошкова, што је од посебног значаја у савременим економским односима. По својој природи, инфраструктура се везује за структуре које формирају основну базу, потребну за остваривање одређених активности. Инфраструктуре одржавају виталне функције друштва и чине свакодневни живот предвидљивим, сигурним и здравим, али и обезбеђују ресурсе за стварање и обнављање свакодневних активности. У обликовању динамике свакодневног животног тока, оне утичу на оно што се сматра нормалним и довољним[28].

---

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

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

Квалитет и поузданост критичне инфраструктуре није само од значаја за економски развој већ и за очување и унапређења поверења грађана и друштва у државне институције. То је уједно и разлог што савремене државе приоритетно инвестирају у критичну инфраструктуру и настоје да дођу до најадекватнијег решења на плану заштите предметних објеката и ресурса. Иако је евидентно да постоје различити приступи овој проблематици свим државама је заједнички примарни циљ, а то је успостављање одрживе, и ефикасне инфраструктуре која ће бити у функцији развоја и друштвеног просперитета. Поремећаји у функционисању критичне инфраструктуре могу утицати и на правовремену испоруку роба и услуга које су од посебног значаја за националну економију, што може у крајњој линији утицати и на губитак пословања и прихода од пореза на погођеном подручјима али и ширих регионалних последица. У околностима катастрофа, евидентни су директни и индиректни економски утицаји и поремећаји који се манифестују у секторима радне снаге, трговине, производње, транспорта ланаца снабдевања, што може угрозити друштво у целини.Учестале или тешко надокнадиве штете са продуженим периодом опоравка за пословне субјекте и привреду у целини доприноси проширењу и повећању губитака на националном нивоу, што указује на повећану важност јачања отпорности критичне инфраструктуре унутар државе. С друге стране савремена друштва су све више зависна од критичних инфраструктурих система који пружају основне услуге и подржавају економски просперитет друштва и државе у целини. Када се критична инфраструктура угрози или поремети, самостановништво осећаутицај тих претњи и последица угрожавања. Због тога улагања у отпорност инфраструктуре и изградња комплексних система на националном нивоу могу смањити дужину и обим поремећаја у функционисању критичне инфраструктуре.[29]

Критична инфраструктура је окосница друштвене безбедности и од суштинског је значаја за друштвени просперитет. Отпорна и сигурна инфраструктура је од виталног значаја за економски просперитет, јер не само да подупире ефикасно пословање компанија и пружање услуга, већ подупире дугорочно поверење и планирање на националном и регионалном нивоу, а тиме и осигурање сталног и стабилног нивоа друштвене безбедности. Обезбеђивање отпорности и безбедности може стога деловати и као директанподстицај у регионалну или секторску економију, а такође и као катализатор за даљи економски раст и

[29] Lazari A.lessandro, *European Critical Infrastructure Protection*, Springer International Publishing, Cham CH, 2014, p.3.

инвестиције. Критични инфраструктурни системи се граде како би обезбедили услуге за неколико генерација и током неколико деценија. Међутим, када дође до прекида у пружању услуга критичне инфраструктуре, посебно у подручијима као што су енергетска, транспортна и комуникациона мрежа, то потенцијално може имати директне негативне економске утицаје, пре свега везано за трошкове санације штете на физичкој структури, као и индиректне економске утицаје на друштво, укључујући прекид пословања у глобалном ланцу снабдевања и повећање краткорочне и дугорочне незапослености.

Значај критичне инфраструктуре се повећава уколико је држава индустријски развијенија. Са економским развојем се повећава и зависност од несметаног функционисања критичне инфраструктуре, и то не само на сопственој територији, већ и на подручјима суседних држава. На основу анализе савремених трендова у критичној инфраструктури, недвосмислено се може уочити тренд повећања њеног значаја не само за државу и друштво, већ и за свакодневни живот појединца. Такав тренд можемо очекивати и у будућности с обзиром да је модеран начин живота постао неодвојив од садржаја критичне инфраструктуре. Разлог томе треба тражити у чињеници да ће савремени свет и у будућности зависити више-мање од појединих сектора инфраструктуре, а посебно енергетског сектора, комуникација, транспортних система, финансија, интернета и јавних служби. Због тога ће и сваки поремећај у њиховом раду доводити до озбиљних стања и потешкоћа за појединце, друштво и пословне ентитете, као и за функционисање државе у целини. И у кризним и ванредним ситуацијама поједини сектори критичне инфраструктуре имаће посебан значај. То су првенствено јавне услуге које се односе на рад болница, полицијских и ватрогасних служби, снабдевање водом и храном и друго, а такође и комуникационе и информационе мреже, саобраћајни сектор (путеви, пруге, аеродроми и луке) и извори енергије (струја, гас, бензин и друго).[30]

Заштита критичне инфраструктуре представља припремљеност капацитета друштва за ублажавање и одговор, односно опоравак од поремећаја или уништења. Реч је о активностима власника, оператора, произвођача, корисника и регулаторних власти, са циљем очувања перформанси критичних инфраструктура у случају немогућности пружања траженог минимума нивоа услуга, минимизирања насталих

[30] Pashley, V., Cools m. (2013), The Power in creative Thinking in situations of Uncertainities: the Almost Impossible Taks of Protecting Critical Infrstaructures: in National Critical infrastructure protection-Regional perspective, Faculty of Security Sudies, Belgrade (et al.), ISBN 978-86-84069-84-1, p.27-40

штета и скраћења времена опоравка. Заштита критичне инфраструктуре нужно мора бити међусекторска, везано за анализе и процене, размену информација и смањење рањивости.Сходно наведеном, са аспекта друштвене безбедности, неопходно је одржање минимума функција критичне инфраструктуре у циљу обезбеђивања континуитета пословања.

Заједнички циљ којем тежи држава и друштво, када је у питању заштита критичне инфраструктуре јесте израда адекватног механизма који ће спречити стварање услова који могу довести до отказивања одређене инфраструктуре услед несреће или напада на било који елемент система. Сходно томе, политика заштите критичне инфраструктуре представља комплексан склоп различитих стратегија, методологија, планова усмерених ка превенцији ризика и претњи, као и спречавању тежих последица услед непредвиђених кризних ситуација. Комплексни проблеми у овом подручју захтевају мултидисциплинарне анализе и примену наменски израђених алата кризног менаџмента ради ефикаснијег идентификовања потенцијалних ризика и претњи.

ЗАКЉУЧНА РАЗМАТРАЊА

Појам друштвене безбедности, може имати више различитих значења и конотација, зависно од угла посматрања. У студијама безбедности он се најчешће односи на стабилност колективног идентитета. У том смислу, друштвена безбедност је моћ и вештина друштва да истраје у свом основном оквиру под измењеним условима и могућим или стварним претњама. Више него посебно, то је питање одрживости, без прихватљивих услова за еволуцију, традиционалних образаца језика, културе, удружења религијског и националног идентитета и обичаја. Концепт друштвене безбедности је веома модеран у теорији међународних односа, нарочито са аспекта одрживости друштва. Овај концепт безбедности је усредсређен на националне и етничке колективитете, и њихову способност да сачувају и успоставе функције друштва у циљу нормалног живота и рада. Главни референтни објекат друштвене безбедности представља одрживост друштва у свим условима. Ирелевантно је очекивати да се друштво развија у идеалним условима. Стога је обезбеђење критичних функција, од изузетног значаја за опстанак и развој друштва. У данашњем свету, иако то није одувек било тако, најмоћнији колективни идентитет је национални идентитет. Национални идентитет, наглашава потребу друштвених група за одрживошћу националних вредности. Пракса показује да је такав приступ исправан, јер су скоро сви негативни догађаји показали да се у заштиту прво стављају

властити капацитети. Тек у неком следећем кораку долази до ангажовања партнерских капацитета, што увек не тече глатко.

Актуелни тренд у савременом свету огледа се у преображају у коме друштва у разним деловима света постају боље повезана и више зависнакао последица развоја технике и технологије, нових начина медијског комуницирања, тржишне економије, брзине транспорта и начина деловања мултинационалних компанија. С друге стране, традиционална култура као национални контекст изгубила је своју некадашњу димензију и доживела је радикалан преображај. Процес који је попримио планетарне размере и у коме су и животни стилови промењени, назван је глобализацијом и подразумева обликовање света као глобалне целине. Глобализација је остварила утицај на све елементе друштвеног живота али и на све становнике земљине кугле, при чему су научни приступи овом феномену били и остали супротстављени. Супротстављеност, са друге стране, подразумева да контрола над критичном инфраструктуром остаје у рукама њених власника, иако би глобализација требала да омогући равноправну расподелу могућности. Управо, моменат располагања критичном инфраструктуром могућност управљања истом и капацитети за враћање функција у условима криза, представљају суштинску одредницу одрживог развоја друштвених заједница у будућности.

ЛИТЕРАТУРА

1. Baylis, J., Wirtz, J., Gray, C., Cohen, E. (2007), Strategy in the Conteporary World, Oxf ord, New York.
2. Borodzicz, E. (2005), Risk, Criis and Security Manageent, John Wiliey&Sons Ltd.:Chichester, West Susex.
3. *Bundesministerium des Innern Nationale Strategie zum Schutz Kritischer Infrastrukturen*, Bundesministerium des Innern,Berlin, 2009, S.7.
4. Collier S.J., Lakoff A. (2008), Distributed Preparedness: The Spatial Logic of Domestic Security in the United States. In: *Environment and Planning D: Society and Space*, 26 (1), 12-16.
5. *Council Directive 2008/114/EC of 8 Decembar 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Official Journal of the European Union L, pp. 345-375, 23.12.2008.
6. Koselleck et al. (1982), Krise und Kritik. In: Geschichtliche Grundbegriffe. Historisches Lexikon zur politisch-sozialen Sprache in Deutschland (Vol. 3), Klett-Cotta, Stuttgart, p. 619.

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

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

9. Кековић, З., Кешетовић, Ж.: Друштвене безбедност у Србији, Српскаполитичкамисао, број 1-2/2008, год.15. vol. 20.

10. Keković, Z., Vučić, S., Despotović, R., Komazec, N. (2013), Compliance of education programs with the need of Protection National Critical Infrastructure: inNational Critical infrastructure protection-Regional perspective, Faculty of Security Sudies, Belgrade (et al.), ISBN 978-86-84069-84-1, p.201-216.

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

12. Kelley A., Pesch-Cronin N., MarionE. (2016). Critical infrastructure protection, risk management, and resilience: a policy perspective, Taylor & Francis Group, 2016, p. 4.

13. Kelley A., Pesch-Cronin N., MarionE. (2016). Critical infrastructure protection, risk management, and resilience: a policy perspective, Taylor & Francis Group, 2016, p. 4-5.

14. Nádai L., Padányi J. (2016), *Critical Infrastructure Protection Research*, Springer International Publishing Switzerland p. 1.

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

16. Pesch-Cronin A. Kelley, Marion E. Nancy, *Critical Infrastructure Protection, Risk Management, and Resilience – A Policy Perspective*, CRC Press, Boca Raton FL, pp. 4-5.

17. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, United States Government, Washington DC, 2003.

18. Lazari Alessandro, *European Critical Infrastructure Protection*, Springer International Publishing, Cham CH, 2014, p.3.

19. Lewis T. (2006), Infrastructure Protection in Homeland Security, Defending a Networked Nation, Wiley Interscience, p. 32.

20. Luiijf Eric et al : The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, TNO, Netherlands, 2016, p. 26.

21. Lukitsch K., Müller M., Stahlhut C. Criticality in (2018), Engels I., J. (2018).*Key Concepts for Critical Infrastructure Research*, Springer, Wiesbaden, p. 12.

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

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

24. Zaballos G. Antonio., JeunInkyung, *Best Practices for Critical Information Infrastructure Protection (CIIP), Experiences from Latin America and the Caribbean and Selected Countries*, Inter-American Development Bank, Washington DC, 2016, p. 3-4.

25. Presidency of the Council of Ministers, *Civil Protection Agency*,dostupno na: http://www.protezionecivile.gov.it/tools/footer/glossary?p_p_id=DpcGlossario_WAR_DpcGlossario100SNAPSHOT&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_DpcGlossario_WAR_DpcGlossario100SNAPSHOT_letter=C&_DpcGlossarioWAR_DpcGlossario100SNAPSHOT_action=listByLetter,

26. Радоман, J.: Секуритизација енергије као увод у енергетску безбедносну дилему, Безбедност Западног Балкана 4/07, ЦЦВО, Београд.

27. Таталовић, Синиша, (2006), Национална и међународна сигурност, Политичка култура, Загреб.

CRITICAL INFRASTRUCTURE AND SOCIAL SECURITY

Dr. Branislav Milosavljević[31]
Dr. Nenad Komazec[32]

Abstract: Negative events that undermine the security of social communities in recent decades have resulted in massive suffering of civilians, material goods and the environment. Modern society is facing numerous challenges and threats related to vulnerabilities of a technical-technological and socio-demographic nature. Their destructive nature is most often the result of the combined action of technical, social and economic factors. Regardless of the variety of causes and consequences, some common characteristics describe most of the dangers that come from natural disasters, terrorist attacks, technical-technological accidents and other disasters that affect the modern world. Psychological action, complexity, interdependence and multidimensionality are their common features, which have brought crisis management issues into the very priorities of world and national security policy of various countries.

Many crises confirm the rule that security threats are of such a nature that vulnerability to endangered infrastructure can be discussed. Approaches are different but there are joint efforts of individuals, organizations, the private sector and governments to prepare, prevent, respond to and recover the fundamental functions of the state and social values. According to Keković and Kešetović, the division into state and social functions is irrelevant here, since all the capacities of the society are engaged in all key phases of a situation that has the potential to cause a crisis. The same authors further believe that this essentially holistic approach to crisis management emphasizes the interoperability of key actors in crisis prevention and response and, what sets it apart from many similar concepts, the combined bottom-up and top-down approach in identifying security threats, hazards and responses to them. It is evident that critical infrastructure is a significant factor in social security.

Key words: critical infrastructure, social security, risk, protection

[31] University of Defense, Institute for Strategic Research, Belgrade, Serbia.
[32] University of Defense, Military Academy, Belgrade, Serbia.

Review paper

THE ROLE OF CORPORATE SECURITY IN THE PROTECTION OF CRITICAL INFRASTRUCTURE

Marjan Gjurovski, PhD[1]
Gjorgji Alceski, PhD[2]

Abstract: One of the main features of corporate security is the protection of the interests of the company from all types and forms of endangerment. However, many of the corporations have a part of determining the objects that are of vital interest to the state, i.e. belonging to the category of critical infrastructures. There is the need for a different approach that is shaped according to changed security conditions. The field of competencies, based on the national interest, is changing and it is different from the standard measures i.e. ways of security, this is so the measures that are already in place should be focused on both, the corporate needs and the national security system.

The constant terrorist attacks on the corporations of vital interest show that terrorism does not recognize state borders nor the political systems or areas on which it is directed to. The tragic past events directed at corporations are defined as critical infrastructures and represent a clear indicator to continuous improvement of security, extending the corporate security interest both, to the state and even to the global security interest.

The increase development of the national security through corporations with a clearly defined security policy and co-operation is grounded over subjects that have a precise task in dealing with security challenges that arise from the complex sources of endangerment, and give a new impulse to the transformation of security awareness of both, the security and the other qualified staff. For those reasons, this paper has the purpose to raise the awareness into achieve a standardized level of security in all corporations that have the status of critical infrastructures with direct cooperation and coordination between the state security sector and the private security sector, which this key factor in the overall security system.

Keywords: security corporate security, national security, critical infrastructures, coordination

[1] Faculty of Security – Skopje, University "St.Kliment Ohridski"-Bitola. E-mail: marjan.gjurovski@uklo.edu.mk

[2] Dep. Airport Manager, TAV Macedonia Airport St. Paul The Apostle Ohrid. E-mail: Gjorgi.Alceski@tav.aero

THE IMPORTANCE OF NATIONAL CRITICAL INFRASTRUCTURE AS AN ESSENTIAL STATE INTEREST

The need to keep track with contemporary security trends, especially in the segment of "critical infrastructures", or the so-called "vital facilities", "facilities of special interest to the state and security", etc., as terms used in our country, is the foundation of security in modern societies. The complexity of contemporary threats, reflected through the corporations that operate the critical infrastructures, implies that they have a direct impact on national security and the efficient functioning of the state systems.

The determination of the need for security, as an essential interest of the state, is expanded with concepts of reference facilities whose security must be guaranteed. Hence, the infrastructures that bear such importance for society, where their non-functioning or limited functioning may create serious consequences and problems, are defined as "critical infrastructures" and need to be treated both on national and international level.[3] As critical infrastructure has become an important segment of national security, critical infrastructure protection has started to develop as well and it is listed among the top priorities of every state. In the context of contemporary global security threats, critical infrastructure protection is a priority issue of the national security of every state.[4]

The complexity of the issue of critical infrastructure security is directly linked with the national security strategies of a number of states, where it acquires a broader vital dimension that includes economic, business, political and environmental issues. National security no longer refers solely to military strategies, but rather tries to eliminate non-military threats by detecting the real threats and efficiently eliminating them. It often presupposes the creation of national security strategies through the corporations that are considered critical infrastructures, as a delicate and comprehensive process which constitutes an integral part of the security concept of each state.

Generally, there are a number of definitions of critical infrastructure. The generally accepted definition of critical infrastructure across the European Union is presented in Directive 114/2008. Here, the European Commission defines critical infrastructure' as a system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a

[3] http://zastita.info/hr/clanak/2013/2/denis-caleta-(ics)-slovenska-iskustva,311,10204.html,Преземено 14.03.2014

[4] О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год. Стр.84

result of the failure to maintain those functions[5]. The analysis of the term critical infrastructure perceived through the need for its adequate protection, indicates that there are minor differences in the national definitions of the states, which highlight systems, assets, properties, products, etc. as crucial for normal functioning of the state in terms of its economic, social, health and security needs. Based on the overall analyses of the notion of "critical infrastructure", viewed through the prism of security and the offered Western indicative lists of critical infrastructures, and guided by the European Union, we may formulate the following definition: *Critical infrastructures refer to facilities, assets, installations, products, services and all systems that are directly or indirectly linked with the normal functioning of the state and whose disruption would cause serious consequences to national security, economy, health, state functionality, social and other consequences*.

In that context, we would fully accept the areas identified by the European Commission, inter alia, energy, information and communications technologies, water, food, finances, public and legal protection, public administration, transport, chemical industry, research[6], with all their capacities and activities, products or services. On the other hand, viewing national security as a state of continuing accomplishments, development, welfare and optimal protection of national and state values and interests, the companies that operate critical infrastructures are assigned an exceptional place within the national security system. National security is necessary, inter alia, to accomplish, maintain and promote the security of the citizens, the national security system and the supranational security mechanism, as well as the absence (individual, group and collective) of fear of being threatened, and the collective feeling of peace, certainty and control of the development of future occurrences and events important to societal life and the state.[7]

NON-MILITARY RISKS AND THREATS TO NATIONAL SECURITY REFLECTED THROUGH THE CORPORATIONS DESIGNATED AS CRITICAL INFRASTRUCTURES

Non-military risks and threats to national security, which are ever more present in everyday life, asymmetric threats focusing on the new forms of action and the examples of the past imply that critical information

[5] EU Directive 2008/114/23.12.2008 EN Official Journal of the European Union L 345/75"

[6] Green paper on a European Programme for critical infrastructure protection Brussels, 17.11.2005 COM(2005) 576 final Annex II

[7] Саша В. Мијалковић- НАЦИОНАЛНА БЕЗБЕДНОСТ - треће, измењено и допуњено издање КРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКА АКАДЕМИЈА Београд, 2015 стр.82

infrastructures, electrical energy infrastructures, oil and natural gas transportation, civilian aviation, water resources and other critical infrastructures have been the target of terrorist attacks. The attacks on critical infrastructures, regardless of whether they are triggered by political, religious, separatist or other types of organizations or they involve terrorism, industrial espionage, hacker attacks are real threats that are directly linked to national security. The omissions of the security services and the preparedness of the terrorists to manipulate, or break into the security protection systems of the corporations determined as critical infrastructures, increase the danger of future illegal acts.

It is evident that national security should be considered on three levels through several areas of human activity. The levels of consideration are individual, state (national) and international, whereas the spheres of human activity include at least the military, political, economic, social and environmental areas. State level is the most important since it determines the other two levels: in contemporary world, the standard unit of security is the sovereign territorial state. The areas important for national security are military, including the offensive and defensive capabilities of the state; economic, that is, the access to natural resources, the market and the finances that determine the acceptable level of welfare; the social, that determines the existence and evolution of traditions, culture, language, national identity and customs and environmental protection that includes the care for the biosphere on which all human activities are dependent.[8] Critical infrastructure is the backbone of every nation as it is linked with national security, economy, industry and health[9].

With respect to the threats to the critical infrastructures, they may be man-made, as a result of terrorism or other criminal activities, or natural, as a consequence of weather conditions, such as storms, volcanic eruptions, floods and other environmental disasters. Furthermore, critical infrastructures may be jeopardized by diseases or pandemics that affect large numbers of critical personnel.[10]

[8]https://kupdf.com/download/nacionalna-bezbednost-knjiga_58ac2d4b6454a70654b1e90d_pdf 96 Buzan, B.:
People, States & Fear – An Agenda for International Security Studies in the Post-Cold War Era , стр. 19–20. Саша Мијалковиќ : Национална безбедност 2017год. стр. 37
[9]http://www.dhs.gov/what-critical-infrastructure Accessed on 26.03.2015г.
[10]Critical Infrastructure Security and Protection: The Public-Private Opportunity White Paper by CoESS – Confederation of European Security Services © December 2010.

CORPORATE SECURITY AS A SECURITY FACTOR OF NATIONAL SECURITY

Considering the fact that in many Western countries the largest portion of critical infrastructures is privately owned, there is a need for active involvement of the state in this type of security. In Germany, four fifths of the critical infrastructures are in private hands. In the USA, about 85% of the critical infrastructures are privately owned, but reality shows that market powers are not sufficient by themselves to incite the required investment in protection. The complexity of this security concept arises from the need to implement a number of measures and activities that extend throughout different areas of expertise and activities, all united under national security. Critical infrastructure consisting of numerous sectors is a system of elements that are most often on the territory of one state and crucial to the maintenance of the vital functions, health, security, safety, economic and social welfare of the population and its disruption or destruction would significant consequences in a given state as a result of its inability to preserve these functions. [11]

If we draw a parallel between the basic principles of corporate security for protection of the company's interests against all types and forms of threats and making profit on the one hand, and the need for national security, in terms of critical infrastructures that permeate all pores of national security, on the other hand, it is evident that their roots are stemming from the national values and their ensuing state interests. Many scientists view National security on three levels (individual, state/national and international), including important areas of human activity, *inter alia*, the level of technical – technological development, the educational and age structure of the population, the influence of the state on the decisions made by the international organizations, the power and potential of the states, etc.[12]

All offered definitions or considerations of the term national security refer to the connection between critical infrastructures and national security. Therefore, the complexity of this security concept stems from the need for implementation of plethora of measures and activities that encompass various areas of expertise and activities, all united under the area of security.

---

[11] О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год. Стр.35

[12] More details in: Art J. Robert "The Fungibility of Force" in Art J. Robert, Waltz N. Kenneth (eds), The use of Force – Military Power and International Politics, Rowman & Littlefield Publishers Inc., Oxford 2004., pp.8-15 . – Корпорациски Безбедносен Систем О. Бакрески, Д. Триван, С. Митевски Скопје 2012

NATIONAL CONCEPTS IN FUNCTION OF THE SECURITY OF CI THROUGH THE CORPORATIONS OF VITAL INTERESTS

If we consider the need to protect critical infrastructure in the US by managing risks it is evident that it is wide-ranging, composed of partnerships among owners and operators; Federal, State, local, and territorial governments; regional entities; non-profit organizations; the academia, etc.

Managing the risks from significant threat and hazards to physical and cyber critical infrastructure requires an integrated approach to:

- Identify, deter, detect, disrupt, and prepare for threats and hazards to the Nation's critical infrastructure;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur[13].

The success of this integrated approach depends on the overall spectrum of capabilities, expertise and experiences in infrastructures and their concerned parties.[14]

Although the US and the EU differ in their positions on the risks and threats to general national security and the critical national goods, they recently established a common determination on two levels that define:

- The resources that constitute critical infrastructure, and
- The measures required for their protection[15].

If we make an overview of the security concepts through a legislative framework, we will see that many contemporary countries regulate this area by directives, strategies, laws, etc., in line with their national interests, designed to enhance the security and persistence of their critical infrastructures in the face of today's threats. The CIP concept, viewed through the prism of providing a framework for a consistent national approach to protection of the state, government and business, designs security concepts that will enable the corporations, that is, the owners – operators of critical infrastructures to deal with the potential risks to the infrastructure or the relevant sector.

CI protection is largely decentralized in the EU member states. In each state, a significant part of the infrastructure is in private ownership and

---

[13] NIPP 2013 Partnering for Critical Infrastructure Security and Resilience Homeland Security - USA

[14] Ibid, p. 7

[15] Zastita kriticne infrastructure i osnovni elementi uskladivanja sa direktivom saveta Evrope 2008/114/ES, Mirko Škero Bezbedno-informativna agencija Vladimir Ateljević Vlada Republike Srbije, Kancelarija za evropske integracije - Visoke studije bezbednosti i odbrane стр.197.

therefore, there must be cooperation with the state institutions. The level and degree of participation of privately-owned corporations in the protection of critical infrastructures are different. In certain countries, the representatives of the private sector are actively or systematically involved in the policy creation process, whereas in others, the private sector is involved only if necessary and mostly for the purpose of implementing the minimum protection standards set up by the state sector. There are many efforts in the EU to consider CIP for each sector separately.[16] As a result, experts describe the EU work on protecting CI as assisting the states in clearly defined sectors in conditions of relevant sectoral coordination.[17] The problem of the cooperation between the EU and member states for CIP may lie in some states' position that certain data must be kept within national frames only.[18]

In Norway, the concept of "a vulnerable society" has become a major part of both public and political debates, following a report by a government commission headed by former Prime Minister Kåre Willoch.[19] The Willoch commission listed several new challenges regarding societal vulnerability and proposed a set of measures in its Report, which constituted the foundation of Norways's White Paper. These included technological changes, increased complexity in society, increased cost- and efficiency pressure, reduced manning in public services and outsourcing of public services to commercial enterprises.[20] These challenges, together with the emergence of "new" threats like terrorism, organized crime and climatic changes, represent a fundamentally changed context for the organizations responsible for the maintenance and protection of critical infrastructures. France follows the doctrine for defense and national security and its approach focusing on "operators of vital importance" means that the inaccessibility of those operators will strongly undermine the economic or military potential and nation's security and resilience. Each operator identifies the critical components in its production system and is

[16] Eriksson, P., Barck-Holst S., Critical Infrastructure Protection policy in the EU and in Sweden –Comparative analysis, FOI, Stockholm, 2005.

[17] Larsson, R., *Tackling Dependency: The EU and its Security Challenges*, Swedish Defense Research Agency, 2007, стр. 9-24.

[18] Jarlsvik, H., Castenfors, K., *Security and Preparedness in the EU*, Stockholm, 2004, стр.64.

[19] Project description: Critical infrastructures, public sector reorganization and societal safety (CISS) https://www.sintef.no/globalassets/project/samrisk/ciss/critical-infrastructures-and-societal-safety.pdf посетена 03/12/2016.О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.

[20] Report on Safety and Security of Society. Report no. 17 to the Storting (2001-2002). Government Norway: https://www.regjeringen.no/en/dokumenter/Statement-on-Safety-and-Security-of-Soci/id420173/посетена на 6/12/2016.О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.

obligated to offer them as points of vital interest that require special protection.[21]

In the legal code of the Czech Republic, the CI issues ensue from the legal regulations and fall under four steps:

1. Selection of CI within individual sectors.
2. Applying the definition of critical infrastructure.
3. Applying the definition of European critical infrastructure (ECI).
4. Applying the cross-cutting criteria.[22]

With respect to the legal regulation for CI protection, the Republic of Croatia has advanced in comparison with the other states of former Yugoslavia, by regulating CI protection, or more specifically, the management and protection of CI is regulated by the Law on Critical Infrastructures, adopted in 2013,[23] which is based on EU Directive 114 of 2008. In addition to adopting this law, the Republic of Croatia has passed two additional bylaws: the Decision designating the sectors in which the central state administration bodies identify national critical infrastructures,[24] and the List determining the order of critical infrastructures sectors and the Rulebook on the risk analysis methodology in managing critical infrastructures.[25] With the Law on Critical Infrastructures, the Republic of Croatia regulates national and European critical infrastructures, the sectors of national critical infrastructures, the management of critical infrastructures, the risk analysis development, the security plan of the owners, the security coordinator of critical infrastructures, the procedures for handling sensitive and classified information and the mechanism for supervising the implementation of the law.[26]

The Federation and local governments are required jointly to enhance and implement critical infrastructure protection in their respective areas of responsibility. This purpose is served by a structured implementation. This procedure comprises the following work packages, which are implemented in parallel, and is based on the co-operative approach adopted by the Federal

[21]Secrétariat Généraldela Défenseetdela Sécurité Nationale: http://www.sgdsn.gouv.fr/site_rubrique70.html, посетена 06.12.2016.

[22] International jurnal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal – Issue 7, Volume 5, 2011.

[23] Zakon o kritičnim infrastrukturama, (Narodne novine 56/2013).

[24] Odluku o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura, (Narodne novine 108/2013).

[25] Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura, (Narodne novine 128/2013).

[26] Закон о критичним инфраструктурама NN56 13, http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, посетена на 14/11/2016.

Administration with the involvement of the other major players, i.e. operators and the relevant associations:

1. definition of general protection targets;
2. analysis of threats, vulnerabilities, and management capabilities;
3. assessment of the threats involved;
4. specification of protection targets, taking account of existing protective measures; analysis of existing regulations and, where applicable, identification of additional measures contributing to goal attainment.

For the implementation of the protection strategy, an extensive set of instruments is available in the form of

- programmes and plans (e.g. the National Plan for information infrastructure protection and the related implementation plans as a strategic concept for IT infrastructure protection;
- specific recommendations for action (e.g. the national Baseline Protection Concept as a basic guidance to physical critical infrastructure protection; the Risk and Crisis Management Guide for Critical Infrastructure Operators, or the national special protection concepts as detailed recommendations for action for the protection of individual CI sectors;
- standards, norms and regulations (e.g. the BSI Information Security Standards as a basic recommendation for action addressed to critical infrastructure operators; or the regulations of the German Gas and Water Supply Association on risk management in the field of drinking water supply.[27]

On account of the chosen co-operative approach that must be given priority, suitably institutionalized platforms involving the state and public authorities, companies and associations are required in view of the procedural steps and instruments that serve to implement the politico-strategic framework.

These security partnership platforms may be organized as: round tables; on federal level; on federal states level; on local government level; joint round tables of the afore-stated entities[28].

CI security, viewed through the prism of national guidelines for protection of CI from terrorism, adopted by the Committee for fight against terrorism of Australia and New Zealand, provides a framework for a national, consistent approach on the protection of CI for the state, the government and the businesses. The Strategy is designed to aid the owners and operators of CI in their dicussions with their jurisdictions (including the Government) about protecting the CI from terrorism. It defines that the treatment of individual CI assets will depend on an assessment of the criticality of the asset in question,

[27] National Strategy for Critical Infrastructure Protection (CIP Strategy) Federal Republic of Germany
Federal Ministry of the Interior Berlin, 17th June 2009
[28] Ibid.

the nature of the security environment and the risk profles for that asset or relevant sector[29].

The term critical infrastructure has not yet been adopted in the framework of the National legislation of the Republic of Macedonia, however, it does not mean that the objects of special significance or the vital facilities in the Republic of Macedonia have not been determined or defined. The Republic of Macedonia has continuity in defining these facilities, in terms of foreseen security measures and delegated duties and responsibilities, however, they are not harmonized in accordance with the guidelines of the European Union. In this regard, the terms are not clearly specified, that is, critical infrastructures are not covered in accordance with the recommendations of the Union. One of the more important steps in this direction was made with the adoption of the Decision on determining the legal entities that are obligated to have private security. This Decision was adopted by the Government of the Republic of Macedonia in 2013, and pursuant to Article 44 of the Law on Private Security ("Official Gazette of the Republic of Macedonia" No. 166/12) and the Law on Amending the Law on Private Security ("Official Gazette of the Republic of Macedonia" No. 164/13), which stipulates the time of their entry into force. According to Article 44 of this Law, the Government of the Republic of Macedonia determines which legal entities are obligated to have private security, if the performance of their activity is related to handling radioactive substances or other hazardous substances for people and the environment, objects of particular cultural and historical significance, as well as in other cases when it is in the interest of security, that is, defense of the Republic of Macedonia.

It must be noted that the regulations treating critical infrastructures include the legal regulations on protection and rescue, as well as crisis management.

CONCLUSION

Corporate security may be defined as one of the most important processes in the organizations as it has a significant role in the functioning of the systems. The strategic planning and operational measures stemming from corporate security must provide answers to the numerous threats and risks the companies face, especially in the segment of critical infrastructure. This process

[29]https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf Превземено 11.11.2015година

requires much more attention and awareness at the highest level of company management[30].

The key personnel in corporate security must take dominant positions, primarily due to the dependence of the state on these companies determined as critical infrastructures. It is the the responsibility of the state to protect the public and ensure a certain level of social functionality and secutity. However, the fact that part of CI is state-owned, whereas part is in orivate ownership (domestic or foreign companies) and that some owners do not share the same values and positions with respect to the protection of the CI system calls for a multifaceted approach of the state and the operators.

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that have institutional knowledge and specialized expertise about the sector.[31] Therefore, security policy, which is a complex and interdependent set of measures, plans, activities and programs, should be directed towards upgrading the existing regulations and practices in view of seeking and defining the possibilities and conditions for applying advanced practices, procedures and systems and implementing them in the development of security. The practical application of certain standards and procedures that ensue from the final operationalization of the offered solutions should be the priority of each state, which requires a new approach to security by activating advanced security systems that follow the technological achievements non-stop, 24 hours a day. There is no dilemma that equipping the security services in accordance with the latest sophisticated achievements in this area will ensure unobstructed execution of the assigned tasks, adequate to contemporary risks and threats.

Corporations, defined as CI, should develop legislation-based security programs or plans that will be approved, accepted and coordinated with all national security stakeholders, especially with the Ministry of Interior and the Ministry of Defense and other relevant members of the national security system. On the other hand, the national security bodies should develop guidelines for the critical infrastructures to adapt their security systems in terms of personnel and technical equipment, so as to guarantee the implementation of standard measures and activities within their scope of work.

---

30 http://www.asadria.com/index.php/teme/kolumne/276-kriticna-infrastruktura-i-znacaj-osiguravanja-njenog-neprekidnog-djelovanja - Denis Caleta - Kritična infrastruktura i značaj osiguravanja njenog neprekidnog djelovanja, Превземено на 17.09.2015г.

31 Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House Office of the Press Secretary February 12, 2013

BIBLIOGRAPHY

1. О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.
2. Саша В. Мијалковић- Национална безбедност - треће, измењено и допуњено издање Криминалистичко-полицијска академија Београд.
3. О. Бакрески, Д. Триван, С. Митевски Скопје 2012 Корпорациски Безбедносен Систем.
4. http://zastita.info/hr/clanak/2013/2/denis-caleta-(ics)-slovenska-iskustva,311,10204.html
5. Директива на ЕУ2008/114/23.12.2008 EN Official Journal of the European Union L 345/75”
6. Green paper on a European Programme for critical infrastructure protection Brussels, 17.11.2005 COM(2005) 576 final Annex II
7. Critical Infrastructure Security and Protection: The Public-Private Opportunity White Paper by CoESS – Confederation of European Security Services © December 2010.
8. NIPP 2013 Partnering for Critical Infrastructure Security and Resiliencehomeland security - USA
9. Zastita kriticne infrastructure I osnovni elementi uskladivanja sa direktivom saveta Evrope 2008/114/ES Mirko Škero Bezbedno-informativna agencija Vladimir Ateljević Vlada Republike Srbije, Kancelarija za evropske integracije - Visoke studije bezbednosti i odbrane Eriksson, P., Barck-Holst S., Critical Infrastructure Protection policy in the EU and in Sweden –Comparative analysis, FOI, Stockholm, 2005.
10. Larsson, R., Tackling Dependency: The EU and its Security Chalenges, Swedish Defense Research Agency, 2007, Jarlsvik, H., Castenfors, K., Security and Preparedness in the EU, Stockholm, 2004,
11. Project description: Critical infrastructures, public sector reorganization and societal safety(CISS)https://www.sintef.no/globalassets/project/samrisk/ciss/critical-infrastructures-and-societal-safety.pdf посетена 03/12/2016. О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.
12. Report on Safety and Security of Society. Report no. 17 to the Storting (2001-2002). Government Norway: https://www.regjeringen.no/en/dokumenter/Statement-on-Safety-and-Security-of-Soci/id420173/ посетена на 6/12/2016. О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.

13. Secrétariat Général de la Défense et de la Sécurité Nationale: http://www.sgdsn.gouv.fr/site_rubrique70.html, посетена 06.12.2016.

14. International jurnal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal – Issue 7, Volume 5, 2011.

15. Zakon o kritičnim infrastrukturama, (Narodne novine 56/2013).

16. Odluku o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura, (Narodne novine 108/2013).

17. Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura, (Narodne novine 128/2013).

18. http://www.asadria.com/index.php/teme/kolumne/276-kriticna-infrastruktura-i-znacaj-osiguravanja-njenog-neprekidnog-djelovanja - Denis Caleta - Kritična infrastruktura i značaj osiguravanja njenog neprekidnog djelovanja, Превземено на 17.09.2015г.

19. Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House

20. Office of the Press Secretary February 12, 2013

ANALYSIS OF THE ENERGY INFRASTRUCTURE IN THE REPUBLIC OF NORTH MACEDONIA

Tatjana Gerginova[1], PhD

Abstract: The author will analyze the need for protection of critical infrastructure within the private security sector in Macedonia. In the introductory part of the paper, the author will give a review of DIRECTIVE 2008/114/EC on Identification and determination of European Critical Infrastructure on procedure - which emphasizes the involvement of the private security sector in the protection of critical infrastructure and determines that the Public-Private Partnership is the key link in the implementation of policies for the protection of critical infrastructure.

Assuming that in the field of protection of critical infrastructure, the energy and transport sector will be a priority for the Republic of Northern Macedonia in the process of integration into the European Union, in this paper, the author will analyze the situation in the energy sector.

In the end, the author will give recommendations for the construction of an efficient system for protection of critical infrastructure. With this paper, the author intends to contribute to the creation of appropriate solutions for achieving the protection of critical infrastructure as a top priority and interest of a nation state.

Keywords: critical infrastructure protection, public-private partnership, energy infrastructure

INTRODUCTION

The modern dynamic development of the world has contributed to the critical infrastructure being more and more present in everyday life. The term critical infrastructure is related to telecommunications, energy security, as well as oil and gas pipelines, water supply, economy, transport and the like.

"Critical infrastructure" is defined as an important component of the national security of each country because the threat to such facilities / infrastructure calls into question the general functioning of the state as well as the normal course of life and safety of citizens. "Critical infrastructure" is

[1] Faculty of Security-Skopje, University "Sv. Kliment Ohridski"-Bitola, Macedonia. E-mail: tanjagerginova@gmail.com

defined as the sum of all facilities, systems, networks and functions, vital for the survival of the state, the destruction of which will negatively affect security, national security, public health and the like.

The European Critical Infrastructure Protection Program creates a procedure for identifying and assessing Europe's critical infrastructure and learning how to better protect it.[2]

This procedure is established for the energy and transport sectors in the Directive on the Identification and Designation of European Critical Infrastructure - Measures to assist in the protection of infrastructure, including expert groups designated by the European Union and the establishment of the Critical Infrastructure Warning Information Network (CIWIN) - Internet-based communication system for exchange of information, studies and best practices.- financing of over 100 critical infrastructure protection projects from 2007 onwards.

These projects focused on a variety of issues, including national and European information exchange and alert systems, the development of ways to assess the interdependence between electronic and electricity transmission networks, and the creation of a "good practice" handbook for policy makers.[3]

This is followed by the preparation of the so-called "Green Paper on the European Critical Infrastructure Protection Program".[4] The Green Paper was adopted on November 17, 2005.

The Green Paper is defined as a "policy document". However, the Green Paper of the European Program for Critical Infrastructure Protection provides an indicative list for identifying critical infrastructure by sectors, as well as a proposed list of framework definitions of key terms.

The most important pillar of the European Critical Infrastructure Protection Program is the adoption of Council Directive 2008/114 / EC.

All Member States have implemented the Directive by establishing a process for the identification and designation of critical European infrastructure in the energy and transport sectors. In the Directive itself, critical infrastructure is defined as: "property, system or part thereof which is located in the Member States and is essential for the maintenance of vital social functions, health,

---

[2] European Commission website, available at https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

[3] Poposka, Vesna., (2019). International-legal aspects of protection of the critical infrastructure, Doctoral dissertation defended at the Military Academy Mihailo Apostolski - Skopje, University "Goce Delchev" Stip.

[4] Green Paper on the European Critical Infrastructure Protection Program (2005) available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576

Green Paper on a European Programme for critical infrastructure protection, 2005, Brussels, Annex II;

safety, security, economic and social well-being of the people, and the disruption or destruction of which would have a significant effect on a Member State as a result of the failure to maintain those functions".[5]

The Directive specifically recognizes "European Critical Infrastructure" (ECI) as critical infrastructure whose disruption or destruction would have cross-border effects in the Member States, and which should be referred to as such in a joint procedure.[6]

European critical infrastructure means "critical infrastructure located in the Member States whose disruption or destruction would have a significant impact on at least two Member States.

In order to improve the protection of critical infrastructure, the European Commission in 2012 establishes a working document for the revision of the European Program for Critical Infrastructure Protection, which sets out a global plan for the improvement of critical infrastructure in all EU member states and all relevant sectors of economic activity. The program is the result of a regular exchange of information between all members of the European Union and it is not limited to terrorism, but also includes natural disasters, crime in order to identify all the dangers in all sectors.

In the energy and transport sectors, Directive 2008/114 / EC has been implemented by the EU Member States since 12 January 2011, with a view to extending its application to other critical infrastructure sectors. Prior to accession to the European Union, all new members of the Union are required to implement this Directive in their national legislation. The document is conceived as the first measure to identify, determine and assess the necessary protection of critical infrastructure and this obligation and responsibility is assigned to states and owners of critical infrastructure. The Directive requires a single approach to the protection of critical infrastructure with implementation in three stages: 1) Identification of potential critical infrastructure; 2) Determining the critical infrastructure; 3) Protection of critical infrastructure.

The Directive emphasizes the involvement of the private sector in the protection of critical infrastructure (supervision, risk management, continuity planning, disaster recovery).

---

[5] DIRECTIVE 2008/114/EC – identification and designation of European critical infrastructures and assessment of the need to improve their protection available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0013

[6] Poposka, Vesna., (2019). International-legal aspects of protection of the critical infrastructure, Doctoral dissertation defended at the Military Academy Mihailo Apostolski - Skopje, University "Goce Delchev" Stip, p. 81

ESTABLISHMENT OF AN INTEGRATED SYSTEM FOR SECURING THE ENERGY SECTOR IN THE EUROPEAN UNION

The European Union today pursues an energy policy that has established an integrated system for securing the energy sector in the member states. The Directive of the European Council is a concrete European document for the identification and determination of the European critical infrastructure, but also the need to improve protection. The main guidelines of this directive are:[7] protection of terrorist threats is a priority for anyone managing critical infrastructure; - protection from all dangers arising from human or technological threats as well as threats coming from natural disasters; the primary and final responsibility for the protection of critical infrastructure is given to the Member States of the European Union and to the owners and operators of these infrastructures; critical infrastructure operators should develop security plans that are in line with European Union Directives based on threat and security risk assessment; accelerate the improvement of critical infrastructure security and the development of general methodologies for categorizing hazards, risks and vulnerabilities of critical infrastructure; it is necessary to protect classified data in accordance with Union acts; critical infrastructure owners and operators should follow proven practices in establishing security mechanisms in energy and transport, as defined by EU members; each EU Member State should designate a security officer authorized to coordinate with the other Member States.

The governments of the member states of the European Union are making great efforts in order to establish functional legislation and to prevent the abuse of the energy sector.

PROTECTION AND PROVISION OF ENERGY INFRASTRUCTURE IN THE REPUBLIC OF NORTH MACEDONIA

The protection and provision of critical infrastructure in the Republic of North Macedonia should be focused on several key activities, namely: • energy sector; • information technologies; • water systems; and • air traffic.

In Macedonia, in the field of critical infrastructure protection, the priority is the energy and transport sector. Therefore, the author further analyzes the situation in the energy sector.

[7] Bakreski, Oliver., Milosevska, Tanja., Alcheski, Gjorgji., (2017), Protection of critical infrastructure. Skopje: Chamber of the Republic of Macedonia for Private Security, p. 42

In Macedonia, from a strategic point of view, the most important are the companies: ELEM (Power Plants of Macedonia) and AD MEPSO (Macedonian Electricity Transmission System, Operator), which with all their capacities are a pillar of the energy system. When it comes to oil infrastructure, AD OKTA has priority in protection, because it has a significant role in the sale, supply and distribution of oil derivatives in the Republic of North Macedonia.

The modern concept for protection of the energy infrastructure of the developed countries is relatively new and different from the traditional - defense-focused - way of providing energy infrastructure. It is comprehensive and integrated into the concept of critical infrastructure protection and has an inextricable link with national security. This means that in addition to state institutions, all relevant structures from the private sector that manage energy infrastructure are included.

Energy infrastructure is the basis of all fundamental processes for the functioning of modern society.[8] Prolonged disruption of this sector would lead to huge consequences, so that many of the activities for the normal functioning of the state would be impossible. Energy infrastructure is divided into three interconnected segments, including: electricity, oil and natural gas. Each of these sources requires a unique set of activities. Energy critical infrastructure may be owned by state, federal, local and private entities as well as some other users, such as large industrial and financial institutions.[9]

An analysis of the multi-national strategies for protection of the critical infrastructure of the member states of the European Union and NATO will show that the interest in protecting the energy infrastructure from asymmetric threats or natural disasters is one of the key imperatives of modern democracies. Therefore, modern countries and their energy sectors take appropriate measures, but also the responsibility to guarantee the availability of the necessary amounts of energy resources at all times and without interruption that would imply additional security or economic problems.

In conditions of liberalization of energy production and distribution, the safety of privatized energy production plants cannot be ensured only through the public sector. In this way, the problems with the internal insurance that the legal entities have in the production and distribution of energy arise, as well as the problem with the insurance of the transmission parts of the energy plants, which opens additional problems in the relations between the private and public sector.

[8] http://www.dhs.gov/energy-sector, accessed on 15.03.2021

[9] Bakreski, Oliver., Milosevska, Tanja., Alcheski Gjorgji (2017), Protection of critical infrastructure. Skopje: Chamber of Private Security of the Republic of Macedonia, p. 36

The security of the energy infrastructure is a task for which the Government of the Republic of North Macedonia has a primary, but not the only responsibility. On the other hand, the hydro power plants, thermal power plants, the Okta refinery, the Thessaloniki-Skopje oil pipeline, the Deve Bair-Skopje main gas pipeline, etc. are owned or managed by private or mixed companies in which the state has a significant stake. That is why the Government and the energy sector have legal responsibility for the protection of the energy infrastructure of the Republic of North Macedonia.

PROTECTION OF THE ENERGY INFRASTRUCTURE THROUGH THE PROVISIONS OF THE ENERGY LAW

The Law on Energy is a legal act, which confirms the primary responsibility of the Government of the Republic of North Macedonia - achieving security and protection of citizens. Reliable, safe and quality supply of energy and energy consumers, creation of efficient, competitive and financially sustainable energy sector, and protection of the environment from negative impacts during the performance of certain activities in the field of energy, are part of the main objectives of this law.[10]

The Energy Law is the only law that covers the terms: security, protection, energy (types of fuels) and infrastructure. Under the term "safety", the Energy Law defines the ability to ensure the protection of human health and life, protection of the environment and property by taking technical and other types of safety measures in the production, transmission and distribution of energy or fuels. In addition to various types of energy, the Law defines most of the components of the energy infrastructure, such as gas pipeline, oil pipeline, electricity distribution network, power system, energy facility, energy sector, operator, electricity producer, etc.

The law also regulates a number of rights and obligations that energy operators should assume in order to protect the energy infrastructure and security of supply not only to citizens but also to the institutions of the national security system.

According to the Law on Crisis Management, the operators of the transmission and distribution systems of the appropriate type of energy or fuel are obliged to prepare plans for action in crisis situations and submit them to the Ministry of Economy for approval.[11] Furthermore, the distribution system

[10] Law on Energy, 2018, "Official Gazette of the Republic of Macedonia", Skopje, no.96 from 28.5.2018

[11] Law on Crisis Management, 2005. "Official Gazette of the Republic of Macedonia", 29/2005

operators are obliged to adopt and publish distribution rules which, among other things, regulate: the technical and other conditions for safe and secure operation of the distribution systems; measures, activities and procedures in case of disturbances and accidents; prescribed safety measures, etc. The law also stipulates strict security measures that potential investors in the energy sector must take as a precondition for obtaining authorization to build energy facilities. These measures relate to the safety and security of the energy system, facilities and related equipment, the protection of public health and safety, and the protection of the environment.

In Macedonia, there are adequate legal bases and obligations for protection of energy i.e. critical infrastructure, but the Republic of North Macedonia significantly lags behind in terms of the type and effectiveness of legal regulations for protection of critical infrastructure of the European Union and NATO member states.

As a candidate country for full EU membership, Macedonia needs to follow the steps taken by the Union and its members to protect critical infrastructure. Therefore, the Government of the Republic of North Macedonia must first define the critical infrastructure, and then proceed to the development and adoption of a Program for protection of the national critical infrastructure as a basis for developing an effective strategy for its protection.

The program should be the result of constructive cooperation that must be established and maintained between the private sector - including energy operators - and the competent government institutions at the state and local levels, not only in crisis but also in peacetime.

The main goal of that cooperation is to create an operational and effective national framework for joint action and construction of flexible and stable critical infrastructure, following the example of the organization of bodies and organs in the crisis management system. The development of a draft strategy for protection of critical infrastructure, in which the competent government institutions, operators and companies from the private sector, as well as experienced experts in the field of critical infrastructure security will participate, is the next step in the process of adopting an effective protection strategy. of the energy, ie critical infrastructure.[12]

If we make an Analysis of the Law on Crisis Management, the Law on Protection and Rescue and the Law on Energy, - it can be concluded that public enterprises, companies, industrial facilities and energy operators, voluntarily or contractually can participate in prevention, early warning and dealing with natural and safety risks and hazards.

[12] Mitreska, Marina., Mileski, Toni., Mikac, Robert., (2019). Critical Infrastructure-Concept and Security Challenges, Skopje

Furthermore, an operational framework for cooperation is needed, so that the institutions of the national security system and the management of energy operators can be able to effectively implement and coordinate measures and activities for protection of energy infrastructure. Energy operators must have sufficient information necessary for relevant safety assessments on the basis of which they will plan and implement the necessary infrastructure protection measures.

Therefore, the creation of a joint integrated approach in function of the security of the energy infrastructure should be equally important and a legal imperative, both for the Government and the energy operators.[13]

CONCLUSION

Directive 2008/114 / EC has been applied in the energy and transport sectors by the EU Member States since 12 January 2011, with a view to extending its application to other critical infrastructure sectors. Prior to accession to the European Union, all new members of the Union are required to implement this Directive in their national legislation.

In the Republic of North Macedonia it is necessary to scientifically define the terms "critical infrastructure" and "protection of critical infrastructure". It is necessary to prepare a comprehensive list of critical infrastructure that should be protected. Furthermore, it is necessary to make a security risk assessment, to determine the sectors of the protected critical infrastructure and to determine sect oral and cross-sect oral criteria on the basis of which it will be determined which facilities, systems and processes will enter the protected critical infrastructure.

By organizing a comprehensive public debate, it is necessary to initiate legal regulation of the protection of critical infrastructure with a special Law on Protection of Critical Infrastructure.

Furthermore, the Law on Protection of Critical Infrastructure needs to define the following terms:[14]

---

[13] Ćaminski, B., (2017). Geopolitical significance and protection of the energy infrastructure of the Republic of Macedonia from asymmetric threats. Doctoral dissertation. Defended at the Faculty of Philosophy, March. 2017;

[14] These terms are already defined in the Law on Critical Infrastructure of the Republic of Croatia

See more: Zakon o kriticnim infrastrukturama, (Narodne novine 56/2013), http://www. zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, accessed on 15.04.2021

▪ European Critical Infrastructure - means critical infrastructure of interest to at least two Member States or one Member State, located in the territory of another Member State;

Furthermore, this Law needs to define the term "National Critical Infrastructures" as systems, networks and facilities of national importance whose interruption of operation or interruption of the procurement of goods or services may have serious consequences on national security, human health and life, property and the environment, security and economic stability, and the continued functioning of government.

▪ Protection of critical infrastructure means activities that aim at achieving functionality, continuous operation and delivery of services / goods to critical infrastructure as well as prevention of endangerment of critical infrastructure;

▪ Risk analysis (means considering possible manifestations of threats to assess vulnerability and possible assessment of disruptions in the functioning of critical infrastructure or to assess its destruction);

▪ Cross-sect oral metrics (benchmarks) - denote a set of general metrics according to which the risk is assessed for individual critical infrastructure systems and networks in all sectors;

▪ Critical Infrastructure Security Coordinator is a person who acts on issues related to the protection of critical infrastructure between the owner / manager and the central bodies of the state administration responsible, responsible for a certain critical infrastructure sector;

▪ Sensitive data - are critical infrastructure data that are marked as classified data in accordance with special regulations;

▪ Contact point - is a central body of the state administration that communicates on behalf of the state with the competent authorities of the European Union and other countries in order to exchange information on critical infrastructures and implement identified activities to achieve their protection and ensure continuity of operation;

▪ Sector metrics (benchmarks) means a set of specific metrics according to which the risk for the composition and network of critical infrastructure in a given sector is assessed;

▪ The owner / manager security plan is a plan that ensures confidentiality, integrity and availability with organizational, personnel, material, information-communication and other solutions, as well as permanent and step-by-step security measures necessary for the continuous functioning of the critical infrastructure;

▪ Critical infrastructure management is the provision of working conditions and continuous functioning of the critical infrastructure;

▪ Owners / managers are legal entities responsible for critical infrastructure management;

The preparation of a draft strategy for protection of critical infrastructure, in which the competent government institutions, operators and companies from the private sector, as well as experienced experts in the field of critical infrastructure security will participate, is the next step in the process of adopting an effective protection strategy of the energy i.e. critical infrastructure.

The focus of the protection of critical infrastructure is precisely the energy facilities that are necessary for the functioning of political, social, economic and security processes in society. General energy security is defined as the physical, technical and electronic protection of energy production, network, transport, facilities and equipment and personnel employed in energy companies.[15] Creating a common integrated approach to the security of energy infrastructure should be an equally important, legal imperative for both the Government and energy operators.

In order to build an efficient system for protection of energy infrastructure, the author gives the following recommendations:

-establishing awareness of the energy sector through timely information and appropriate exchange of information between the public and private sector;

- implementation of the principle of protection (such as exchange of information, creation of partnership between the private and public sector, etc.);

-clear definition of the role and responsibilities of the public and private sector in order to improve the coordination between the partners; - application of appropriate principles for risk management with implementation of physical and informational measures, in order to improve the readiness, security, resilience (flexibility); - conducting effective emergency and disaster planning, including training and exercises to improve response in such situations; - understanding the importance of interdependence and cooperation with other sectors and implementing knowledge in planning and operations; strengthening public trust between partners, in order to strengthen the ability of sectors to cope with risks and implement effective measures for security and post-crisis recovery.[16]

---

[15] Vrsec M., Managing Corporate Security in the Energy Sector: Energetics as a Vital (Critical) infrastructure for the Functioning of State, Economy and Civil Society. Counter – terrorism Challenges regarding the Processes of critical infrastructure: Ljubljana: Seprember, 2011, p.124 - 125

[16] Energy Sector-Specific Plan An Annex to the National Infrastructure Protection Plan 2010, Homeland Security – United States Department of Energy.

-the owners and operators of the critical infrastructure should follow the proven practices in establishing the security mechanisms in energy and transport, which are defined by the members of the European Union; - each member of the European Union should designate a security officer authorized to coordinate with the other member states;

In order to achieve adequate security of the energy sector, the Government should propose measures for security and protection precisely because of the direct dependence of the state on the energy sector. In order to improve the provision of critical infrastructure, it is necessary to develop simple methodologies for establishing and categorizing hazards (security threats, risks and vulnerabilities within critical infrastructures). Owners and operators of critical infrastructure, including the energy sector, need to follow good practice in establishing security systems regulated in accordance with European Union acts by establishing a cooperation officer who will be in charge of coordinating with other countries but will provide and advice to state critical infrastructure operators.

REFERENCES

1. Bakreski, Oliver., Milosevska, Tanja., Alcheski Gjorgji (2017), Protection of critical infrastructure. Skopje: Chamber of Private Security of the Republic of Macedonia

2. European Commission website, available at https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

3. Energy Sector-Specific PlanAn Annex to the National Infrastructure Protection Plan2010, Homeland Security – United States Department of Energy.

4. Vrsec M., (2011). Managing Corporate Security in the Energy Sector: Energetics as a Vital (Critical) Infrastructure for the Functioning of State, Economy and Civil Society. Counter – terrorism Challenges regarding the Processes of critical infrastructure : Ljubljana

5. Green Paper on the European Critical Infrastructure Protection Program (2005) available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576

6. DIRECTIVE 2008/114/EC – identification and designation of European critical infrastructures and assessment of the need to improve their protection available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0013

7. Law on Energy, 2018, “Official Gazette of the Republic of Macedonia”, Skopje, no.96 from 28.5.2018

8. Law on Crisis Management, 2005. “Official Gazette of the Republic of Macedonia”, 29/2005

9.Law on Protection and Rescue, “Official Gazette of the Republic of Macedonia”, 93/2012

10. Zakon o kriticnim infrastrukturama, (Narodne novine 56/2013), http://www. zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, accessed on 15.04.2021

11. Mitreska, Marina., Mileski, Toni., Mikac, Robert., (2019). Critical Infrastructure-Concept and Security Challenges, Skopje

12. Poposka, Vesna., (2019). International-legal aspects of protection of the critical infrastructure, Doctoral dissertation defended at the Military Academy Mihailo Apostolski - Skopje, University "Goce Delchev" Stip.

13. http://www.dhs.gov/energy-sector, accessed on 15.03.2021

Pregledni rad

STEPEN UGROŽENOSTI KRITIČNE INFRASTRUKTURE TERORISTIČKIM AKTIVNOSTIMA

Nikola Terzić, MSc [1]
Milan Baltić[2]

Apstrakt: Skupstina Crne Gore je na šestoj sjednici drugog redovnog zasijedanja u 2019. godini usvojila predlog Zakona o određivanju i zaštiti kritične infrastrukture. Sa ciljem što uspješnije zaštite iste u narednom periodu Ministarstvo unutrašnjih poslova će ići korak dalje te napraviti nacionalni dokument koji će analizirati kritičnu infrastrukturu sa aspekta bezbjednosti i dati preporuke sa ciljem zaštite kritične infrastrukture od terorizma. Ovaj rad predstavlja nastojanje doprinosa autora toj ali i svim ostalim aktivnostima koje će se preduzimati u buduće postujući nacionalne ali i međunarodne standarde bezbjednosti jer su mir i normalno funckionisanje života u jednoj društvenoj zajednici osnovna mjera i putokaz oko kojeg nema dileme i oko kojeg se ne pregovara. Terorističke aktivnosti su takve djelatnosti u koliko ne djelujete korak ispred njih unaprijed ste izgubili rat.

Ključne reči: Crna Gora, Kritična infrastruktura, terorizam, procena rizika.

UVOD

Kritična infrastruktura obuhvata sisteme, mreze, objekte, odnosno njihove djelove koji se nalaze na teritoriji Crne Gore, čiji prekid funkcionisanja, odnosno prekid isporuka roba ili usluga preko tih sistema, mreza, objekata moze imati ozbiljne posledice po nacionalnu bezbjednost, zdravlje i zivot ljudi, imovinu, zivotnu sredinu, bezbjednost gradjana, ekonomsku stabilnost odnosno djelatnosti od javnog interesa.

Zastita kritične infraksturkture predstavlja skup aktivnosti i mjera koje imaju za cilj da spiječe nastanak poramećaja u radu, oštećenje ili uništenje kritične infrakstrukture u slučaju prijetnje obezbijede fukncionisanje i otpornost

[1] Savjetnik Ministra unutrašnjih poslova Crne Gore.
[2] Koordinator Odjeljenja za koordinaciju i nadozor u oblasti kritične infrakstrukture, Ministarstvo unutrasnjih poslova Crne Gore.

kritične infakstrukture i smanje tj dovedu na minumun posledice do kojih moze doći.

Savremeni terorizam predstavlja ozbiljnu prijetnju kako međunarodnoj bezbjednosti čije totalno otklanjanje ne nadzire se u skorije vrijeme, tako i nacionalnoj bezbijednosti država koje su obuhvaćene terorističkim aktima. U opštem smislu pojam „ugrozavanje„ znači nečije organizovano djelovanje usmjereno ka izazivanju promjena na ciljanu vrijednost (čovjek, predmet, društvo, drzave...) nezavisno od toga da li je branjeno ili nezaštićeno.

Ugrozenost Crne Gore terorizmom podrazumijeva prije svega i pouzdanu ocjenu stanja zastićenosti drzave i društva u određenom trenutku od teritorijalne opasnosti. Riječ je o uobičajenoj periodičnoj i vanrednoj ocjeni stanja zastićenosti vitalnih društvenih i drzavnih interesa i vrijednosti od ispoljenih (postojećih) i mogućih (potencijalnih) djelatnosti terorista. Ustanovljavanje ugrozenosti bezbjedenosti energetskih objekata kao dio kritične infrakstrukture je odgovoran i rizičan zadatak koji iziskuje profesionalnu odgovornost i veliki stepen stručnosti nosioca tih i takvih aktivnosti. Bezbijednost kritične infrastrukture obuhvata sveukupnost međusobno zavisnih mreža i sistemi koji obuhvataju prepoznatljive industrije, institucije (uključujući ljude i procedure), i mogućnosti distribucije koje obezbeđuju pouzdan protok proizvoda i usluga neophodnih za odbranu i ekonomsku sigurnost zemlje, čiji primeri uključuju snabdevanje električnom energijom, transport, komunikaciju, energije i vode, upravljačke infrastrukture i sl., je predmet povećanja pažnja vlada zbog sve veće prijetnje od terorizma u svetu.[3]

Pošto su kritične infrastrukture sastavni dio normalnog funkcionisanja društva, njihovo eventualno ugrožavanje je povezano sa ogromnim rizikom po normalno funkcionisanje života u jednoj društvenoj zajednici. Kritične infrastrukture su složeni sistemi koji se sastoji od različitih komponenti podsistema, a njihove funkcionalnosti zasnovane su na operacijama podsistemi unutar kritičnih infrastruktura. Složenost kritičnih infrastruktura ih čini ranjivim, od raznih oblika ugrožavanja (poput prirodnih nesreća ili nekih manjih kvarova) što ponekad rezultira značajnim gubicima po društvo.[4] S obzirom na visok nivo štete koju kvarovi na kritičnim infrastrukturama mogu nanijeti ljudskim životima, ekonomiji, nacionalnoj bezbijednosti i normalnom funkcionisanja društva, tačna procena ugroženosti kritičnih infrastruktura na

[3] Yao, X., Wei, H., Shohet, M. I., Skibniewski J. M., Assessment of Terrorism Risk to Critical infrastructures: The Case of Power-Supply Substation, Applied sciences, no. 10/71621, MDPI, Basel, 2020, pp. 1.

[4] Zimmerman, R. Social implications of infrastructure network interactions. J. Urban Technol. no. 8, 2001, pp. 97.

opasnosti od terorizma su od velike važnosti, kao i razvoj strategija koje bi mogle zaštititi kritične infrastrukture od takvih opasnosti ili smanjiti gubitke.[5]

PRAVNI OKVIR BEZBIJEDNOSNE ZAŠTITE KRITIČNE INFRASTRUKTURE U CRNOJ GORI

Donošenje Zakona o određivanju i zaštiti kritične infrastrukture predviđeno je Programom pristupanja Crne Gore Evropskoj uniji za period 2018-2020. godine.[6]

Predlog zakona o određivanju i zaštiti kritične infrastrukture[7] pripremila je međuresorska radna grupa koju su, pored predstavnika Ministarstva unutrašnjih poslova, činili i predstavnici: Ministarstva odbrane, Ministarstva ekonomije, Ministarstva održivog razvoja i turizma, Ministarstva javne uprave, Ministarstva zdravlja i Uprave policije. Prilikom izrade ovog zakona izvršeno je usaglašavanje sa Direktivom Savjeta Evropske unije od 8. decembra 2008. o utvrđivanju i označavanju Evropske kritične infrastrukture i procjeni potrebe poboljšanja njene zaštite[8], te je Predlog zakona u maju upućen Evropskoj uniji na mišljenje.

Takođe, zakon je bio i na javnoj raspravi tokom koje su svi zainteresovani imali priliku da se upoznaju sa predmetnim tekstom i daju svoje sugestije. Uzimajući u obzir činjenicu da je Crna Gora punopravan član NATO-a, na Predlog zakona i NATO je dao svoje mišljenje čiji su predlozi i sugestije uvrštene u tekst Predloga zakona, čime se Crna Gora pokazala kao ozbiljan partner i partner koji teži da dobru praksu Evropske unije i NATO-a prenese u svoje nacionalno zakonodavstvo, i time ispuni ne samo standarde iz oblasti zaštite kritične infrastrukture već generalno sve standard iz oblasti bezbjednosti i zaštite. Važno je istaći da crnogorski pravni sistem do sada nije poznavao propis koji uređuje oblast kritične infrastrukture, prema tome ovaj zakon je prvi kojim se ista uređuje.

---

[5] Rinaldi, S. M, Peerenboom, J. P., Kelly, T. K., Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag., no. 21, 2001, pp. 11.

[6] Program pristupanja Crne Gore Evropskoj uniji 2018-2020. godine, dostupan na: https://www.eu.me/wp-content/uploads/2018/03/16_II_18_PPCG_2018_-_2020.pdf, pristupljeno 31.05.2021. godine.

[7] Kompletan tekst predloga zakona dostupan je na: https://www.paragraf.me/nacrti_i_predlozi/nacrt-zakona-o-kriticnoj-infrastrukturi.pdf, na dan 31.05.2021. godine.

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

Zakonom uređeni su način određivanja kritične infrastrukture, njena zaštita i druga pitanja od važnosti za kritičnu infrastrukturu.

Naime, kritična infrastruktura je veoma specifična, a prevashodno iz razloga što obuhvata više resora, te je prilikom određivanja iste, potrebno voditi računa o tome da se obuhvati svaka oblast društva na koju se ona odnosi. Navedene oblasti nazvane su sektorima kritične infrastrukture, i to su oblasti: energetike, saobraćaja, snabdijevanja vodom, zdravstvo, finansije, elektronske komunikacije, informaciono-komunikacione tehnologije, zaštita životne sredine, funkcionisanje državnih organa,kao i druge oblasti od javnog interesa.

Kada je u pitanju određivanje kritične infrastrukture, kroz tekst Zakona na detaljan način uređen je postupak izvještavanja i dostavljanja predloga za određivanje kritične infrastrukture između operatora kritične infrastrukture, ministarstava nadležnih za određeni sektor i Ministarstva unutrašnjih poslova, koje u krajnjem, objedinjene predloge za određivanje kritične infrastrukture dostavlja Vladi, koja svojim aktom, koji je određen stepenom tajnosti, određuje kritičnu infrastrukturu.

Određivanje kritične infrastrukture vrši se na osnovu međusektorskih i sektorskih kriterijuma, te naprijednavedenom postupku prethodi još jedan akt Vlade kojim se propisuju sektorski kriterijumi za svaku oblast, odnosno sektor ponaosob. Međusektoski kriterijumi predviđeni su samim zakonom (član 8), imajući u vidu da svaki sektor, da bi predstavljao kritičnu infrastrukturu mora da ispunjava najmanje jedan međusektorski kriterijum.

Nadalje, za upravljanje kritičnom infrastrukturom zaduženi su operatori kritične infrastrukture, te je svaki operator dužan je da iz reda zaposlenih najkasnije šest mjeseci po određivanju kritične infratrastrukture odredi koordinatora kritične infrastrukture. Imajući u vidu da koordinator obavlja veoma važne zadatke u članu 20 zakona predvidjeno je osposobljavanje za koordinatora za zaštitu kritične infrastrukture, kao i polaganje stručnog ispita.

Kada je u pitanju zaštita kritične infrastrukture predvidjeno je da će se ista vrštiti primjenom fizičke i tehničke zaštite shodno Zakonu o zaštiti lica i imovine[9], gdje već postoje privredna društva, druga pravna lica i preduzetnici koji vrše poslove zaštite. Takođe, napominjemo da je Zakonom o zaštiti lica i imovine omogućeno da ministarstva, organi državne uprave, lokalne samouprave i službe koje obrazuje država mogu da obrazuju svoju unutrašnju službu zaštite.

Posebno je važno istaći da su iz odredaba zaštite kritične infrastrukture propisane ovim zakonom izuzeti Ministarstvo odbrane, Vojska CG, Agencija za nacionalnu bezbjednost, Uprava policije, kao i kritična informatička infrastruktura, s obzirom da se njihova kritična infrastruktura štiti posebnim

[9] Zakon o zaštiti lica i imovine Crne Gore ("Sl. list CG", br. 43/2018).

zakonima (Zakon o odbrani[10], Zakon o vojsci[11], Zakon o Agenciji za nacionalnu bezbjednost[12], Zakon o unutrašnjim poslovima[13] i Zakon o informacionoj bezbjednosti[14]).

Takođe, navedeni organi nijesu dužni da odrede koordinatora za zaštitu kritične infrastrukture, kao ni da izrađuju bezbjednosni plan shodno ovom Zakonu. Ovu mogućnost izuzeća omogućava i Direktiva Evropske komisije sa kojom je zakon usaglašavan.

Kritična infrastruktura se štiti na osnovu posebnog plana zaštite koji je Zakonom nazvan bezbjednosni plan, pa su operatori, najkasnije godinu dana po određivanju kritične infrastrukture, dužni da izrade bezbjednosni plan i na isti pribave saglasnost Ministarstva unutrašnjih poslova, kao i da prilikom upravljanja kritičnom infrastrukturom vode računa o bezbjednosnom planu.

Nadalje, uzimajući u obzir delikatnost i specifičnost oblasti kritične infrastrukturu bilo je potrebno i predvidjeti ko će biti zadužen u slučaju nastanka poremećaja u radu, odnosno oštećenja ili uništenja kritične infrastrukture, te će u ovim situacijama, rukovođenje i koordinaciju sprovođenja mjera i aktivnosti u skladu sa ovim zakonom, preduzimati koordinacioni tim obrazovan u skladu sa Zakonom o zaštiti i spašavanju[15]. Ovo je propisano iz razloga jer Koordinacioni tim obrazovan u skladu sa Zakonom o zaštiti i spašavanju čine svi predstavnici koji bi učestvovali i u zaštiti kritične infrastrukture.

Takođe, kao posebno poglavlje zakona predviđena je evropska kritična infrastruktura, čije odredbe će se primjenjivati tek kada Crna Gora postane članica Evropske unije, što je u prelaznim odredbama i definisano.

---

[10] Zakon o odbrani Crne Gore ("Sl. list RCG", br. 47/2007 i "Službenom listu CG", br. 86/2009 - drugi zakon, 88/2009, 25/2010 - drugi zakon, 40/2011 - drugi zakon, 14/2012, 2/2017, 46/2019 i 74/2020 - drugi zakon).

[11] Zakon o vojsci Crne Gore ("Sl. list CG", br. 51/2017 i 34/2019).

[12] Zakon o Agenciji za nacionalnu bezbjednost ("Sl. list RCG", br. 28 od 5. maja 2005, "Sl. list Crne Gore", br. 20 od 15. aprila 2011).

[13] Zakon o unutrašnjim poslovima Crne Gore ("Sl. list CG", br. 44/2012, 36/2013, 1/2015 i 87/2018).

[14] Zakon o informacionoj bezbijednosti Crne Gore („Sl. glasnik RS", br. 6/2016, 94/2017 i 77/2019).

[15] Zakon o zaštiti i spašavanju Crne Gore ("Sl. list Crne Gore", br. 013/07 od 18.12.2007, 005/08 od 23.01.2008, 086/09 od 25.12.2009).
032/11 od 01.07.2011, 054/16 od 15.08.2016)

ANALIZA ZAŠTITE KRITIČNE INFRASTRUKTURE KROZ PRIZMU MOGUĆNOSTI TERORISTA I PROTIV TERORISTIČKE MOGUĆNOSTI CRNE GORE

U poslednjih desetak godina načinjeni su značajni koraci da se elementi kritične infrastrukture analiziraju sa aspekta rizika i pripreme za događaje koji mogu omesti njihov rad kroz izradu planova zaštite, tako da se ublaži ugroženost sistema na svim nivoima (regionalni, nacionalni i lokalni). Ipak, strategije koje su usmjerene ka uspešnoj prevenciji krajnje negativnih scenarija (terorističkih napada ili prirodnih katastrofa većih razmera), iako veoma efikasne, ne moraju da potvrđuju da je izvršena optimalna alokacija resursa koji su potrebni za zaštitu.[16] Rizičnost zadatka procjena i sama zastita kritične infraksture je u tome što postoji mogućnost da neki od faktora bude potcijenjen ili precijenjen, a takvo postupanje moze da ima ogromne i nesagledive posledice po bezbjednost naše zemlje i ukupne kolektivne bezbjedosti.

Procjena ugrozenosti kritične infraksturure u Crnoj Gori predstavlja svojevrsnu instrukciju i upustvo o postupanju svim drzavnim i drustvenim subjektima koji se bave zastitom ovih objekata od terorističkih aktivnosti.

Kvalitetno razmatranje i shvatanje procesa ugrozavanja i sama procjena ugrozenosti kritične infraksturture od terorističkih aktivnosti kao preduslov uspjesne odbrane od agresije terorista predstavlja i obuhvata aktivnosti brojnih i raznovrsnih činilaca, činjenica i okolnosti.

Analizom samog Ustava Crne Gore[17], Krivičnog zakonika[18] ali i cjelokupnog pravno normativnog okvira nesumnjivo stičemo utisak da Crna Gora drzava članica NATO saveza i drzava kandidat za članicu EU , nastoji da se kvalitetnim zakonodavnim okvirom suoči sa terorizom nezavisno od faze ispoljavanja izazov ili prijetnja.

Prilikom procjene ugrozenosti kritične infrakstruture terorističkim aktivnostima mora se prije svega uzeti u obzir nivo uspješnosti nacionalnog sistema bezbjednosti u suočavanju sa terorističkim aktivnostima i djelovanjem u fazi izazov ili prijetnja te u konačnom rezultat stanja nacionalne bezbjednosti u opste.

Sama analiza kada je u pitanju kritična infraksturutra treba da obuhvati obvezne elemente ili analizu i to:

---

[16] Škero, M., Ateljević, V., Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope 2008/114/ES, Vojno delo, god. 67, br. 3, Ministarstvo odbrane Republike Srbije, Beograd, 2015, str. 195.

[17] Ustav Crne Gore ("Sl. list CG", br. 1/2007 i 38/2013 - Amandmani I-XVI).

[18] Krivični zakonik Crne Gore ("Sl. list RCG", br. 70/2003, 13/2004 - ispr. i 47/2006 i "Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011 - dr. zakon, 40/2013, 56/2013 - ispr., 14/2015, 42/2015, 58/2015 - dr. zakon, 44/2017, 49/2018 i 3/2020).

a) preventivnu odbranu kojom odvraća nosioce od preduzimanja terorističkih djelatnosti;

b) aktivnu odbranu sa ciljem sprečavanja terorista da realizacijom ne smrtonosnih djelatnosti steknu sposobnost za primjenu smrtonosnih djelatnosti, kao i suzbijanje smrtonostnih aktivnosti.

Prilikom same procjene mora se voditi računa o principima i to, zakonitosti, preventivnosti, informisanosti, centralizovanosti i sl.

Angazovanje kapaciteta obezbjeđenja objekata kritične infrastrukture mišljenja smo treba koncipirati na principu uobičajenog obezbjedjenja (redovno i svakodnevno), za uspješnu prevenciju u odnosu na terorističke aktivnosti ili neobičajeno (vanredno), kada je prevencija zakazala. Ono što je prvi krug obezbeđenja je zaštita okruženja objekta i postiže se kombinacijom sistema protivprovalne zaštite i videonadzora sa inteligentnomvideo analitikom. Potom, neophodno je utvrditi dozvolu pristupa – ulaza ili prolaza – isključivo ovlašćenim osobama. Pristup se omogućava ili sprečava automatskim delovanjem sistema za ranu detekciju i dojavu požara. Kada dođe do potrebe za zaštitom, visokokvalitetan i pouzdan alarmni glasovni sistem predstavlja valjano rešenje za brzu i neophodnu evakuaciju.Bitno je naglasiti da se integracijom sistema video nadzora, protivpožarne zaštite, kontrole pristupa i evakuacionog ozvučenja, poboljšava efikasnost i smanjuje potrebno vreme za evakuaciju ljudi iz objekta.[19]

Misija MUP a je da kroz niz aktivnosti da značaj opstoj terorističkoj preventivi te da na taj način odvrati potencijalne teroriste od terorističkih djelatnosti, a da tek nakon toga imamo spremne planove protiv terorističkih akcija i operacija sa ciljem onesposobljavanja terorista.

Kao elementi za ustrojstvo analize terorističkih potencijala mogu poslužiti sledeći karakteristike: a) motivi koji pokreću članove, b) organizovanost i hijerajhiska struktura, c) broj članova; d) obim i oblici podrske stanovništva gdje se priprema sami teroristički akt, e) izvor finasiranja, f) personalne i karakterne osobine vodje i članova, g) sredstva za samo izvodjenje terorističke aktivnosti, h) iskustva terorista, i) važni datumi iz proslosti koji ih ,,obavezuju,, i sl.

Dakle, kvalitetna analiza mogućih oblika ugrožavanja kritične infrastrukture od terorističkih napada zahteva prethodno dobro poznavanje fenomena terorizma, terorističkih grupa koje deluju na datom prostoru, kao i samog *modusa operandi* terorističkih organizacija. Terorizam, kao metod djelovanja političkih ekstremista, je u najširem smilu riječi samo jedan od

[19] Kekić, D., Čudan, A., Direktiva Saveta o utvrđivanju i označavanju evropske kritične infrastrukture i proceni potrebe unapređenja njene zaštite, Evropsko zakonodavstvo, Institut za međunarodnu politiku i privredu, br. 71/20, Beograd, 2020, str. 23.

načina primene nasilja u cilju ostvarenja određenih političkih interesa, kako unutar države, tako i u okvirima međunarodne zajednice. Prema zvaničnoj američkoj definiciji FBI (eng. *Federal Bureau of Investigation*) pod terorizmom se smatra nezakonita primjena sile ili nasilja prema ljudima ili imovini da bi se zastrašila vlada, civilno stanovništvo ili neki njegov dio, a u svrhu postizanja političkih ili društvenih ciljeva.[20]

U najširem političkom smislu, terorizam je naziv za metod političke borbe za koju je karakteristična sistematska upotreba nasilja radi zastrašivanja protivnika i slamanja njegovog otpora.[21] U krivično-pravnom smislu teorizam predstavlja krivično delo koje se sastoji u napadu na život, tjelo ili slobodu drgoga, otmicu ili uzimanje talaca, uništenje državnih ili javnih objekata, saobraćajnih sistema, infrastrukture ukjlučujući i informacijske sisteme, neporketne platforme u epikontinentalnom pojasu, opšteg dobra ili privatne imovine koje može da ugrozi život ljudi, izrada, posjedovanje, nabavljanje, prevoz, snapbdevanje ili upotrebz oružja, eksploziva, nuklearnog ili radioaktivnog materijala ili uređaja, nuklearnog, biološkog ili hemijskog oružja, istraživanje i razvoj nuklearnog, biološkog ili hemijskog oružja, ispuštanje opasnih materija ili prouzrokovanje požara, ekspeksplozije ili poplave ili preduzimanje druge opšteopasne radnje koja može da ugrozi život ljudi, ometanje ili obustavu snabdijevanja vodom, električnom energijom ili drugim energentom koje može da ugrozi život ljudi a u namjeri da ozbiljnog zastrašivanja građana ili radi prinuđivanja Crne Gore, strane države ili međunarodne organizacije da što učini ili ne učini, ili da ozbiljno ugrozi ili povrijedi osnovne ustavne, političke, ekonomske ili društvene strukture Crne Gore, strane države ili međunarodne organizacije (član 447 stav 1 KZ). Terorizam, kao metod djelovanja političkih ekstremista, ogleda se u preduzimanju različitih akata fizičkog nasilja ili drugih oblika ugrožavanja života i zdravlja ljudi koje najčešće karakteriše neselektivnost pri izboru objekta napada i neposrednih žratvi, pri čemu se izaziva strah i osjećaj nesigurnosti u određenoj društvenoj zajednici i stvaraju uslovi za postizanje političkih ciljeva.[22] Dakle kao osnovni elementi terorističkog djelovanja, javlja se, pre svega, nasilje prema konkretnim neposrednim objektima (uglavnom ljudima). Oblici nasilja kojima politički ekstremisti pribegavaju prilikom terorističkog delovanja su veoma različiti i obuhvataju podmetanje i aktiviranje eksplozivnih sredstava na javnim mjestima, rušenje važnih političkih, kulturnih, istorijskih,

[20] Aleksić, Ž., Škulić, M., Žarković, M., Leksikon kriminalistike, 2004, str. 357.

[21] Savić, A., Delić, M., Ilić, P., Osnovi državne bezbednosti, Obrazovno istraživački centar RDB MUP RS, Beograd, 1998, str. 85.

[22] Ivanović, R. A., Soltved, P. L., Mirno rešavanje konflikata i izgradnja poverenja u multikulturalnim sredinama u svrhu borbe protiv radikalizma i nasilnog ekstremizma, MONITOR, Novi Pazar, 2020, str. 60.

verskih ili privrednih objekata u jednoj zemlji, vršenje otmica, uzimanje talaca, vršenju ubistava i sl. Drugi oblici ugrožavanja života i zdravlja ljudi terorističkim aktivnostima ogledaju se u upotrebi različitih sredstava, počev od raznih hemijskih, zapaljivih, biološkobakterioloških (bakterije, virusi i gljivice) i radioloških sredstava koja dovode do uništenja, oštećenja, paljenja, trovanja i oboljenja, privremenog ili trajnog onesposobljavanja ljudi, biljnog i životinjskog sveta,[23] tzv. bioterorizam. Nasilje koje se ispoljava terorirstičkim djelovanjem je brutalno, bezobzirno i amoralno, tj. prevazilazi potrebe čina, i u suprotnosti je sa opšteprihvaćenim moralnim i društvenim vrijednostima, odnosno usmereno je na objekte koji naročito pogađaju psihu ljudi, npr. nezaštićene građane, djecu i sl. Akti nasilja, odnosno drugi vidovi ugrožavanja života i zdravlja građana preduzimaju se (mada ne uvek), neselektivno. Naime, žrtve terorističkog delovanja, danas su uglavnom nedužni građani koji su se u momentu napada slučajno zatekli na tom mestu. Dok su u ranijem periodu teroristi za objekt napada u većini slučajeva birali ljude koji su simbol odrijeđene države, odnosno odrijeđene politike (šefove država, premijere, ministre, diplomatske predstavnike, kao i članove njihovih porodica i članove uže familije) ili objekte od posebne istorijske, ekonomske, političke, duhovne ili druge važnosti za jednu društvenu zajednicu (zgrada skupštine, sedišta ministarstava, ambasade, istorijska i verska zdanja, i sl).[24] Bilo da su žrtve istaknuti pojedinci ili obični građani, primarni cilj terorista je obezbeđenje reakcije države. Zbog toga se ističe da žrtva kod terorizma nije individualno određena, već simbolično. Ubijanjem žrtve u toku realizacije terorističkog akta, teroristi u stvari ciljaju na državu.[25] Teroristi pribegavaju ovakvoj taktici izvođenja napada, zbog toga što nakon ovakvih napada, nužno sledi reakcija države na čijoj teritoriji je akt izvršen, odnosno prema kojoj je izvršen, u smislu preduzimanja aktivnosti na osiguranju mira i bezbijednosti pojedinaca, društvenih grupa, organizacija i institucija koje mogu biti objekt napada terorista.

Vršenjem napada teoriističke organizacije, teže najpre privlačenju pažnje javnosti, odnosno publicitetu, koji prati svaki teroristički akt, kao i izazivanju straha kod stanovništva, što im dalje omogućava javno iznošenje svojih motiva i realizaciju, odnosno ostvarenje političkih ciljeva i zahtjeva.[26]

Dakle, prije svega, teroristički akt je akt prenošenja određene poruke s obzirom da sam po sebi ne može da proizvede skoro nikakve društvene promene. Poruka govori o ciljevima delovanja, kao i o namerama izvršioca

[23] Šipraga, J., Aleksić, Ž., Kriminalistička metodika, Viša škola unutrašnjih poslova, Beograd, str. 27.
[24] Ivanović, R. A., Soltved, P. L., op. cit., str. 61.
[25] Simonović, B., Kriminalistika, Pravni fakultet, Kragujevac, 2004, str. 655-656.
[26] Stajić, Lj., Osnovi bezbednosti , Policijska akademija, Beograd, 2004, str. 249.

terorističkog akta, ma ko on bio. Zato teroristi preuzimaju odgovornost za izvršeno djelo. Porukom se naglašava i pretnja da će se sa takvim akcijama nastaviti ako se ne postupi po zahtevima terorista, što u krajnjoj liniji izaziva strah.[27] Izazivanju straha dodatno doprinosi i velika brojnost i raznovrsnost objekata terorističkog napada. Naime, teroristi u odabiru objekta koji će biti meta terorističke akcije imaju čitavu lepezu objekata. Stoga je, veoma teško unapred otkriti sledeću metu napada teorориста i preduzeti adekvatne mere za zaštitu tog objekta.

Izazivanje straha predstavlja ključnu karakteristiku terorističkog djelovanja. Naime, teroristi svojim delovanjem nastoje da aktima nasilja, pre svega, ukažu stanovništvu da država nije u stanju da im garantuje, odnosno jemči ličnu bezbednost, i tako izazovu strah, nesigurnost i nepoverenje koji će zatim prevazići rušilačke posljedice samog čina nasilja. Stoga se može reći da strah ne predstavlja nusproizvod terorističkog delovanja, već ciljani efekat, odnosno efekat koji se želi postići, a zatim upotrebiti kao sredstvu za ostvarenje ideoloških, odnosno političkih ciljeva. Za ostvarenje ovog efekta koriste se sredstva masovne komunikacije (društvene mreže, internet, televizija, radio, štampa i sl.), putem kojih terorirsti javno preuzimaju odgovornost za konkretne terorističke akte, i ujedno stanovništvu predočavaju pretnju daljim aktima nasilja, a vladajućem režimu zahtev za ostvarenje političkog cillja.

Izazivanje straha, nesigurnosti i nepovjerenja kod stanovništva u većem obimu za posljedicu može imati njihov pritisak na samu vlast da udovolji zahtevima terorista. Iz svega navedenog zakjlučujemo da neposredne posledice terorističkih akcija su, pre svega, lišavanje života ili ugrožavanje telesnog integriteta ljudi, zatim razaranje ili oštećenje različitih materijalnih i duhovnih vrednosti, zagađivanje životne sredine u većem obimu.[28] Međutim, iza svega toga stoji nastojanje unošenja trajnog nemira i straha u jednu zemlji, tj. krajnja posledica terorizma ogleda se u izazivanju straha radi iznuđivanja ustupaka i postizanja odgovarajućih političkih ciljeva.

Posebnu opasnost terorističkog delovanja predstavlja dalekosežnost i veoma teška otklonjivost posledica realizovanih terorističkih akcija, tj. izazivanog straha. Koliko su dalekosežne i duboke posledice koje prizvodi terorirstičko delovanje unutrašnjih ekstremista možda se najbolje može prikazati konstatacijom profesora Paula Vilkinsona (Paul Wilkinson) koji kaže: „Da se borba protiv terorizma može poistovetiti sa ulogom golmana, tj. da možete napraviti sto briljijantnih odbrana, ipak, jedini šut koji će ljudi pamtiti

[27] Ibid, str. 249.

[28] Korać, H., Ivanović, R. A., Begović, A., Prevencija kriminaliteta, Internacionalni univerzitet u Novom Pazaru, Beograd, 2011, str. 220.

biće onaj koji vam je promakao. Što znači da su posljedice uspešno izvedenih terorističkih akcija u psihološkom smislu (strah) teško neutrališu.[29]

UMJESTO ZAKLJUČKA

Iz svega navedenog možemo zaključiti da zbog ciljeva i *modusa operandi* terorističkih grupa, al i važnosti koju kritična infrastruktura ima za jednu društvenu zajednicu, kao i njenu ranjivost, koja se pre svega ogleda u dalekosežnim posledicama, ista se itekako nalazi u fokusu djelovanja terorista u smislu objekta napada. U prilog ovome govori postojanje dokaza da je Al Qaida bila zainteresovana za ranjivosti američkih javnih i privatnih komunalnih preduzeća. Naime, otkrivanje u Avganistanu računara koji sadrže programe strukturne analize za brane, u kombinaciji sa povećanjem web prometa koji se odnosi na sisteme supervizorske kontrole i prikupljanja podataka (eng. *Supervisory control and data acquisition-SCADA*), navelo je Nacionalni centar za zaštitu infrastrukture (eng. *National Infrastructure Protection Center - NIPC*) Sjedinjenih Američkih Država da izda informativni bilten upozorenja na sajber teroristička pretnje ovim sistemima. U skladu sa navedenim, u ovom radu, u smislu ugroženosti kritične infrastrukture terorističkim napadima želimo prije svega da ukaženo na vulnerabilnost, industrijskih sistema upravljanja koji obuhvataju sisteme nadzorne kontrole i prikupljanja podataka (SCADA) i sisteme za distribuirano upravljanje (eng. *Systems and distributed control systems* - DCS). SCADA sistemi se često koriste za daljinsko nadgledanje velikog geografskog područja i za prenos komandi do udaljenih sredstava, kao što su ventili i prekidači. Na primer, mogu se naći u vodovodima i naftovodima, gde prate brzine protoka i pritiske. Na osnovu podataka koje ovi sistemi pružaju, računarski programi ili operateri u centralnom kontrolnom centru uravnotežuju protok materije. Distribuirani sistemi upravljanja su sistemi za upravljanje procesima, koji se obično nalaze u jednom proizvodnom kompleksu, a karakteriše ih mreža računara. DCS generalno pruža obrađene informacije ili niz komandi sa centralne lokacije. Na primer, u hemijskom postrojenju, DCS može istovremeno pratiti temperaturu niza reaktora i kontrolisati brzinu mešanja reaktanata, istovremeno izvršavajući optimizaciju procesa u realnom vremenu i izveštavajući o toku reakcije. Napad na DCS može izazvati veliku štetu na jednom objektu, ali ne može uticati na više od jedne lokacije. Naime, ovi sistemi za upravljanje procesima mogu biti međusobno povezani u jednoj industriji. To može biti slučaj u infrastrukturi koja prenosi i obrađuje materiju. Na primer, infrastruktura nafte i gasa sadrži

[29] Ivanović, R. A., Soltved, P. L., op. cit., str. 61.

lokacije za obradu i preradu, kao i skladišne objekte i distributivne sisteme. Lokacije za obradu i preradu mogu koristiti DCS na diskretnim lokacijama. Objektima za distribuciju i držanje može upravljati SCADA sistem koji prikuplja podatke i izdaje komande različitim geografskim lokacijama sa jedne lokacije. Tehnologije industrijskog sistema upravljanja često se koriste u kritičnim infrastrukturnim industrijama kako bi omogućile jednom kontrolnom centru da upravlja sa više lokacija. Industrijski sistemi upravljanja su prvobitno implementirani kao izolovane, odvojene mreže. Na njih se gledalo kao na sigurne sisteme koji štite udaljene lokacije od fizičkog provaljivanja i ugrožavanja. Na primjer, uspostavljanje sistema daljinskog upravljanja u branama navodno zaštićenim od nezakonitog ispuštanja pregrađene vode, jer nisu bili dostupni ručno upravljani ventili i prekidači.

Uzevši u obzir napred navedeno možemo zakjlučiti da posljedice napada na industrijske sisteme kontrole kritične infrastrukture mogu biti različiti. Ovde treba istaći da se u oblasti studija bezbednosti uglavnom pretpostavlja da bi uspešan sajber napad na ovakve sisteme prouzrokovao malo ljudskih žrtava, ili ih uopšte ne bi bilo, ali bi zato mogao rezultirati gubitkom infrastrukturne usluge dok je kontrolor zauzet uspostavljanjem kontrole i popravljanjem štete, što zapravo predstavlja veliku opsasnost, i mogućnost za nove napade, i ljudske žrtve. Na primer, uspešan sajber napad na javnu telefonsku komunikacionu mrežu mogao bi lišiti korisnike telefonskih usluga, i dok se tehničari bave resetovanjem i popravljanjem telefonske mreže, napad na kontrolne sisteme postrojenja za hemijski ili tečni prirodni gas mogao bi da dovede negativnih materijalnih i ljudskih posledica znatno širih razmjera. Ovde treba imati na umu, kada su u pitanju kritične infrastrukture da događaji sa manjom verovatnoćom uključuju katastrofalne kvarove infrastrukture, gde kvar jednog dela infrastrukture dovodi do kvara drugih delova, izazivajući široko rasprostranjene efekte. Do takvog kvara može doći usled sinergijskog efekta infrastrukturnih industrija jedna na drugu. S tim u vezi, sasvim opravdano stručnjaci upozoravaju na tzv. kaskadni efekat, gde terorista može da manipuliše sistemima upravljanja i izazove katastrofalan kvar unutar infrastrukture. Kaskadni efekti mogu da imaju veoma štetno dejstvo, uzrokujući rasprostranjene prekide u radu komunalnih usluga.

Scenario koji izaziva najveći stepen zabrinutosti stručnjaka je kombinovana upotreba sajber napada na kritičnu infrastrukturu zajedno sa fizičkim napadom. Ova upotreba sajber-terorizma mogla bi rezultirati pojačanjem efekata fizičkog napada. Primer za to može biti konvencionalni bombaški napad na zgradu u kombinaciji sa privremenim uskraćivanjem električne ili telefonske usluge. Posledična degradacija reagovanja u vanrednim situacijama, sve dok rezervni električni ili komunikacioni sistemi ne budu uspostavljeni i upotrebljeni, mogla bi povećati broj žrtava i javnu paniku.

Uzevši u obzir sve navedeno kao značajno pitanje u zaštiti kritične infrastrukture od mogućih terorističkih napada postavlja se pitanje modeliranja rizika od ovakvog vida ugroženosti, što zahteva znanje iz dveju oblasti: procenjivanje ranjivosti infrastrukture i procenu potencijalnih spoljnih pretnji po nju. Ranjivost se može analizirati modelovanjem odgovora različitih komponenti infrastrukture suočavanjem sa pretnjom i procenom rizika po čitavu infrastrukturu u svetlu posledica napad na svaku komponentu, interakcije među komponentama i kombinovani uticaj direktnog i indirektno oštećenje ukupne funkcionalnosti infrastrukture. Procena ugroženosti kritične infrastrukture je gotovo uvek veoma složena, jer će različite komponente ove infrastrukture verovatno pokazivati različite reakcije na isti događaj. Međutim, uticaji opasnosti na kritičku infrastrukturu se mogu podeliti na dva osnovna tipa: direktne gubitke na funkcionalnosti komponente u sistemu i indirektne efekte koji proizilaze iz interakcija između ili između više komponenti. Dok se direktni efekti mogu direktno proceniti na osnovu stepen oštećenja komponenti i troškovi popravke, procena indirektnih efekata je znatno teža. U stručnoj literaturi, koja se bavi ovom oblašću može se naići na različite predloge modela procenu ranjivosti kritične infrastrukture.

Međutim, ovde treba istaći, da u mnoštvu tih modela, treba praviti razliku između procene ranjivosti kritične infrastrukture prirodnim nepogodama i procene ranjihovisti kritične infrastrukture terorooristčkim napadom. Ovo pre svega, zbog toga što za razliku od prirodnih nepogoda, teroristički napadi nisu samo nasumični događaji sa velikom verovatnoćom pojavljivanja koje se mogu relativno dobro proceniti (npr. period ponavljanja poplava ili zemljotresa). U slučaju analize rizika od terorističkih napada, najizazovniji problem je utvrđivanje vjerovatnoće njihovog pojavljivanja, koje (za razliku od prirodnih katastrofa) mogu biti povezane ne samo sa istorijatom prethodnih pojava, već i sa trenutnim nivoom zaštite kritične infrastrukture. Dakle, za procenu rizika od terorističkog napada na kritičnu infrastruktutur je od ključne važnosti zaštitna strategija jedne države kada je u pitanju kritična infrastruktura. Ovakav pristup može dovesti do razotkrivana vjerovatnoće terorističkih napada na kritičnu infrastrukturu, na način da na taj rizik utiču faktori kao što su ranjivost kritične infrastrukture, zaštita kritične infrastrukture, vidljivost kritične infrastrukture, posljedice događaja, mogućnosti napadača i istorijat djelovanja teroristčke organizacije. U tom smislu smanjenje vjerovatnoće napada i poboljšanje odvraćanja mogu se ostvariti većom robusnošću (povećavanjem cjene napada) i većom otpornošću (smanjenjem posljedica napada).

LITERATURA

1) Aleksić, Ž., Škulić, M., Žarković, M., *Leksikon kriminalistike*, 2004.

2) Ivanović, R. A., Soltved, P. L., *Mirno rešavanje konflikata i izgradnja poverenja u multikulturalnim sredinama u svrhu borbe protiv radikalizma i nasilnog ekstremizma*, MONITOR, Novi Pazar, 2020.

3) Kekić, D., Čudan, A., *Direktiva Saveta o utvrđivanju i označavanju evropske kritične infrastrukture i proceni potrebe unapređenja njene zaštite*, Evropsko zakonodavstvo, Institut za međunarodnu politiku i privredu, br. 71/20, Beograd, 2020, str. 22-37.

4) Korać, H., Ivanović, R. A., Begović, A., *Prevencija kriminaliteta*, Internacionalni univerzitet u Novom Pazaru, Beograd, 2011.

5) Rinaldi, S. M., Peerenboom, J. P., Kelly, T. K., *Identifying, understanding, and analyzing critical infrastructure interdependencies*. IEEE Control Syst. Mag., no. 21, 2001, pp. 11–25.

6) Savić, A., Delić, M., Ilić, P., *Osnovi državne bezbednosti,* Obrazovno istraživački centar RDB MUP RS, Beograd, 1998.

7) Simonović, B., *Kriminalistika*, Pravni fakultet, Kragujevac, 2004.

8) Stajić, Lj., *Osnovi bezbednosti* , Policijska akademija, Beograd, 2004.

9) Šipraga, J., Aleksić, Ž., *Kriminalistička metodika*, Viša škola unutrašnjih poslova, Beograd, 1986.

10) Škero, M., Ateljević, V., *Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope 2008/114/ES*, Vojno delo, god. 67, br. 3, Ministarstvo odbrane Republike Srbije, Beograd, 2015, str. 192-207.

11) Yao, X., Wei, H., Shohet, M. I., Skibniewski J. M., *Assessment of Terrorism Risk to Critical infrastructures: The Case of Power-Supply Substation*, Applied sciences, no. 10/71621, MDPI, Basel, pp. 1.

12) Zimmerman, R. *Social implications of infrastructure network interactions*. J. Urban Technol. 2001, 8, pp. 97–119.

DEGREE OF CRITICAL INFRASTRUCTURE VULNERABILITY TO TERRORIST ACTIVITIES

Nikola Terzić, MSc [30]
Milan Baltić[31]

Abstract: At the sixth session of the second regular session in 2019, the Parliament of Montenegro adopted the proposal of the Law on Designation and Protection of Critical Infrastructure. In order to protect them as successfully as possible in the coming period, the Ministry of Interior will go a step further and create a national document that will analyze critical infrastructure from the security aspect and make recommendations to protect critical infrastructure from terrorism. This paper represents the author's contribution to this and all other activities that will be undertaken in the future, respecting national and international security standards, because peace and normal functioning of life in a community are a basic measure and guide that is not dilemma and which is not to be negotiated. Terrorist activities are such activities insofar as you do not act a step ahead of them you have lost the war in advance.

Keywords: Montenegro, Critical Infrastructure, Terrorism, Risk Assessment.

[30] Adviser to the Minister of Interior of Montenegro.
[31] Coordinator of the Department for Coordination and Supervision in the Field of Critical Infrastructure, Ministry of Interior of Montenegro.

OSVRT NA ZAKON O BEZBJEDNOSTI KRITIČNIH INFRASTRUKTURA U REPUBLICI SRPSKOJ

Dr Dragiša Jurišić[1]

Apstrakt: Kritična infrastruktura i njeno razmatranje je relativno novi diskurs, u području bezbjednosti. U kontekstu savremenih prijetnji od terorizma ali i onih nastalih uslijed klimatskih promjena, definisanje i zaštita kritične infrastrukture su od velikog značaja za uspješno funkcionisanje savremenih država. BiH, kao država, ima obavezu da se pozabavi ovim pitanjem, ali je do sada samo Republika Srpska donije Zakon o bezbjednosti kritičnih infrastruktura i time stvorila preduslove za njeno definisanje, procjenu i poduzimanje mjera zaštite. Zakon je donesen 2019.godine ali se po njemu sporo postuapa pa ostaje pitanje njegove primjenjivosti i potrebe za određenim izmjenama ili dopunama kroz predviđene metodologije, uputstva i procjene. U ovom radu je prije svega izvršena analiza postojećeg Zakona o bezbjednosti kritičnih infrastruktura, date su određene sugestije na njegov sadržaj ali i određene preporuke kako bi sam Zakon bio primjenjiviji i kako bi ispunio svoju svrhu u budućnosti.

Ključne riječi: Kritična infrastruktura, Zaštita kritične infrastrukture, zakon, zaštita, Republika Srpska, BiH

UVOD

Savremeni svijet je povezan u svim segmentima. Teorija Edvarda Lorensa[2] da bi lepršanje krila leptira u jednom dijelu svijeta moglo da utiče na klimatske promjene hiljadama kilometara daleko, danas više nego ikad ima svoje uporište u stvarnom svijetu i događajima koji ga prate. Povezanost sistema, višeslojnost odnosa, kao i multipliciranje uticaja i opasnosti, jasno zahtjevaju sistemski pristup u prepoznavanju, procjeni i zaštiti infrastrukture koja je ključna za normalan život i rad ljudi i njihov opstanak na nekom prostoru. Kako je sva infrastrukture na određeni način povezana i umrežena, svi su zainteresovani da ona funkcioniše.

[1] Bezbjednosni istraživački centar, Banja Luka

[2] Edward N. Lorenc, Deterministic Nonperiodic Flow, Journal of The Atmospheric Sciences, Volume 20, 1963, str.130, https://www.astro.puc.cl/~rparra/tools/PAPERS/lorenz1962.pdf, preuzeto 18.06.2021.

Prateći trendove u svijetu, pitanje kritične infrastrukture i njene zaštite je počelo da se razmatra i u Bosni i Hercegovini (BiH). Prvi zakon je donesen na nivou Republike Srpske i to je Zakon o bezbjednosti kritičnih infrastruktura. S obzirom da je to prvi takav pokušaj u BiH i Republici Srpskoj (RS) da se determiniše, procijeni i zaštiti kritična infrastruktura, ovaj rad ima za cilj da analizira taj Zakon i ukaže na određene nedorečenosti i potrebu da se pojedini njegovi dijelovi revidiraju ili dopune.

Rad je koncipiran u pet poglavlja. Na početku će biti riječi o kritičnoj infrastrukturi u BiH a nakon toga će se obraditi pitanje kritične infrastrukture u Republici Srpskoj. Zaštita kritične infrastrukture u Republici Srpskoj, njena procjena i zakonski okvir su težište ovog rada, nakon čega su izvučeni određeni zaključci.

KRITIČNA INFRASTRUKTURA U BIH

U svijetu i u zemljama u okruženju postoje mnogi radovi koji razmatraju temu kritične infrastrukture (KI). U poslednjih deset godina, ovo pitanje je postalo veoma važan dio bezbjednosti. Ljudi su postali svjesni da ne mogu da štite sve i uvijek, i da moraju odlučiti, koja infrastruktura je od ključnog značaja za njih i zašto. Zaštita kritične infrastrukture (ZKI) je tema u kojoj se prepliću politika, biznis, tehnologije i rizik. Svi su svjesni važnosti KI, ali još uvijek ne postoji jedinstvena, opšte prihvaćena, lista ili definicija KI, i to dovodi do različitog pristupa kada je riječ o ZKI-e, njenom definisanju i načinu njene zaštite.

BiH ima sličan problem, a organizacija države čini rešavanje tog pitanja složenijim. Najvažnija stvar je definisanje odnosa države prema KI i izrada liste KI. Svaki entitet, i Brčko Distrikt BiH su odgovorni za svoju listu KI, ali definicija bi trebalo da bude zajednička. Takođe, postoji potreba za jasnim razumjevanjem, ko će štititi koju KI. U skladu sa propisima EU[3], KI mora biti definisana i sačinjena njena lista u svim državama članicama, kao i u zemljama koje hoće da postanu članice. Što znači da BiH mora pristupiti rešavanju ovog pitanja što prije.

Sistem zaštite i spasavanja u BiH je veoma složen, i dalje u fazi razvoja. On ima više nivoa, a treba da bude osnova za upravljanje KI. U rukama je entiteta i osnove, pa ZKI takođe treba da budu u njihovim rukama. S druge strane, BiH ima infrastrukturu koju koriste institucija BiH. Neke od tih

[3] Direktiva Vijeća 2008/114/EZO utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite,Službeni list Europske Unije L 345/75, 2008, https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114&from=en, preuzeto 22.03.2021.

infrastruktura su: međunarodni aerodromi, granični prelazi, kasarne, neke državne institucije i državni funkcioneri. Na državnom nivou postoji nekoliko organizacija koje imaju posao da štite ove infrastrukture. To su granična policija, bezbednosna agencija za istrage i zaštitu (SIPA), Direkcija za koordinaciju policijskih tijela BiH i Oružane snage BiH. Te institucije nisu prepoznale tu infrastrukturu kao KI, pa se ona ne definiše kao takva, ali u skladu sa Zakonom o državnoj agenciji za istrage i zaštitu (SIPA)[4] i njegovom promenom 2009. godine, Savjet ministara BiH odlučuje koji objekti treba da budu zaštićeni, a u tom Zakonu je i spisak osoba koje treba da budu zaštićene. Zaštita ambasada i međunarodnih institucija predviđeno je u skladu sa međunarodnim obavezama koje je potpisala BiH[5]. Takođe, prema Zakonu o odbrani BiH, Predsedništvo BiH će odlučiti koji od objekata su važni za odbranu, a na predlog Ministarstva odbrane. Za razliku od nekih drugih država i vojski u svijetu, gdje zaštitu nekih vojnih instalacija vrše privatne kompanije, svu vojnu infrastrukturu u BiH čuvaju i štite vojne snage, odnsono OS BiH.

Prema Strategiji BiH za prevenciju od terorizma (2006-2009)[6], KI mora biti definisana, ali se to nije dogodilo, a u novoj Strategiji (2010-2013)[7] postojao je isti zadatak, ali opet to nije učinjeno. Poseban podcilj, Strategije BiH za prevenciju i borbu protiv terorizma 2015-2020[8], je zaštita kritične infrastrukture. Predviđeno je da će se utvrdit obaveza usvajanja minimalnih standarda za zaštitu kritične infrastrukture i drugih objekata od značaja, kao i unapređenje procedura za procjenu realnog rizika i ugroženosti. Na žalost sam akcioni plan ovog dokumenta ne donosi ništa novo, odnosno nema aktivnosti usmjerenih direktnom pitanju definisanja i zaštite kritične infrastrukture, kao ni planove za donošenje zakona o zaštiti KI na nivou BiH jer je to jedan od preduslova za ulazak u EU.

---

[4]Zakon o državnoj agenciji za istrage i zaštitu, "Službeni glasnik BiH", br. 27/2004, 63/2004, 35/2005, 49/2009 i 40/2012

[5]Bečka konvencija o diplomatskim odnosima od 18. aprila 1961.godine, "Službeni list SFRJ" - dodatak, 2/64

[6]Ministarstvo bezbjednosti BiH, Strategija Bosne i Hercegovine za prevenciju i borbu protiv terorizma (2006-2009), Sarajevo, 2006.

[7]Ministarstvo bezbjednosti BiH, Strategija Bosne i Hercegovine za prevenciju i borbu protiv terorizma (za period od 2010–2013. godine), Sarajevo, 2010., http://www.psa.gov.ba/Popisi_i_dokumenti/Propisi/Strategije/Strategija%20BiH%20za%20prevenciju%20i%20borbu%20protiv%20terorizma.pdf, preuzeto 14.04.2021.

[8] Savjet Ministara BiH, Strategija Bosne i Hercegovine za prevenciju i borbu protiv terorizma 2015.- 2020, Sarajevo, 2015., http://www.vijeceministara.gov.ba/akti/prijedlozi_zakona/default.aspx?id=20285&langTag=hr-HR, preuzeto 14.04.2021.

Takođe, u Strategiji za uspostavljanje CERT (Computer Emergenci Response / Spremnost tima) u BiH[9], kao kratkoročni zadatak je bio identifikacija KI koja bi trebala da bude zaštićena. Na listi srednjoročnih zadataka je dato da BiH mora procjeniti bezbjednost KI i poboljšati rad na smanjenju rizika i da edukuju administratore KI. Strategija BiH za prevenciju i borbu protiv terorizma 2015-2020[10], posebnim setom mjera predviđa aktivnosti na zaštiti kritične cyberinfrastrukture, odčijeg ključnog značaja za ovaj proces uspostave CERT-a u BiH.Ministarstvo odbrane BiH razvilo je vlastitu strategiju cyber obrane[11] s ciljem uspostavljanja bezbjednog cyber okruženja samo za informacijske sisteme unutar svog Ministarstva. Ova je strategija razvijena bez usvajanja službene državne strategije za cyber bezbjednost. Međutim, sudionici predviđaju da će strategija Ministarstva pomoći poboljšanju opštegnivoa cyber bezbjednosti unutar zemlje.[12]

Trenutno na državnom nivou ne postoji registar ili katalog incidenata na nacionalnom nivou kojim centralno upravlja Savjet ministara, niti postoji nacionalno koordinaciono telo, kao što je Tim za reagovanje na incidente računarske bezbjednosti (CERT), u cilju efikasne koordinacije reagovanja i upravljanja incidentima u cyber bezbjednosti. Takođe, ne postoje obavezni zahtjevi za izvještavanje o cyber incidentima. Na entitetskom nivou, prvi CERT je osnovan 2015. godine, stvaranjem Odjeljenja za informacionu sigurnost pri Agenciji za informaciono društvo Republike Srpske.[13] Preporuke koje su date BiH a vezano za cyber kritičnu infrastrukturu kroz dokument Pregled cyber bezbjednosnih kapaciteti BiH (Cybersecurity Capacity Review Bosnia and Herzegovina)[14] iz 2019.godine su:

- razviti i sprovesti nacionalnu procenu rizika s ciljem identifikovanja KI na državnom nivou;

---

[9] Savjet Ministara BiH, Strategija uspostave CERT-a u Bosni i Hercegovini (CERT- Tim za odgovor na računarske incidente - Computer Emergency Response/Readiness Team), Sarajevo, 2011, http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=en-US, preuzeto 15.05.2021.

[10] Savjet Ministara BiH, Strategija Bosne i Hercegovine za prevenciju i borbu protiv terorizma 2015.- 2020, Sarajevo, 2015., http://www.vijeceministara.gov.ba/akti/prijedlozi_zakona/default.aspx?id=20285&langTag=hr-HR, preuzeto 14.04.2021.

[11] OSCE, Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini, Sarajevo, 2019, https://www.osce.org/files/f/documents/4/8/438386.pdf, preuzeto 15.05.2021.

[12] Eva Nagyfejeo and Sarah Puello Alfonso,Cybersecurity Capacity Review Bosnia and Herzegovinahttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658404, SSRN, 2019, posjećeno 09.04.2021.

[13] Isto

[14] Isto

- obavljati redovne, detaljne revizije KI u pogledu cyber bezbjednosti i distribuirati liste revizije KI relevantnim zainteresovanim stranama. Obavestite one koji posjeduju tu KI o njihovioj odgovornosti;
- uspostaviti mehanizam za redovno otkrivanje ranjivosti i razmjenu informacija između vlasnika KI i Savjeta ministara BiH. Uspostaviti redovan dijalog između taktičkog odnosno izvršnog i strateškog nivoa u vezi sa praksama cyber rizika i podstaći komunikaciju između operatora informacionih tehnologija;
- utvrditi interne i eksterne strategije komunikacije KI sa jasnim kontaktnim tačkama;
- uspostaviti postupke i procese zaštite podataka i upravljanja rizikom u okviru KI, podržane odgovarajućim tehničkim bezbjednosnim rješenjima, koja obavještavaju izrađivače planaova odgovora na incidente, o cyber incidentima.
- uspostaviti zajedničke procese za mjerenje i procjenu sposobnosti vlasnika imovine KI da otkriju, identifikuju, reaguju na njih i oporavljaju se od cyber prijetnji.

Očigledno je da spisak KI u BiH ne postoji. Samo u nekim zakonima, na državnom ili entitetskom nivou, moguće je naći spisak imovine koja pripada nekoj od infrastruktura. U Zakonu o šumama u RS je lista šumske infrastrukture (objekata, šumskih puteva, transportnih sredstava i dr.), i isto je u Federaviji BiH (FBiH). Isto je i sa željezničkom infrastrukturom u Zakonu o železnici FBiH ili sa infrastrukturom u Zakonu o prostornom planiranju i korišćenju zemljišta FBiH.

U dokumentu Procjena ugroženosti BiH od prirodnih ili drugih nesreća[15], nije moguće naći definiciju KI, ali jedan od naslova nosi naziv „O transportnim i drugim objektima i instalacijama KI“. U skladu sa tim podnaslovom u KI, u BiH spadaju:

- putne i željezničke komunikacije i čvorišta, riječne komunikacije, te aerodromi;
- vodoopskrbni objekti;
- termo-energetska i hidro-energetska postrojenja i instalacije, transformatorske stanice i dalekovodi;
- naftovodi i gasovodi;
- benzinske stanice;
- objekti i instalacije hemijske i petrohemijske industrije;
- poštanski i telekomunikacijski sistemi;

[15] Procjena ugroženosti Bosne i Hercegovine od prirodnih ili drugih nesreća, Savjet ministara, Sarajevo, 2011.str.4-5.

- objekti farmaceutske industrije;
- objekti prehrambene industrije;
- objekti površinske i podzemne eksploatacije rude i minerala.

U Procjenama ugroženosti entiteta od prirodnih ili drugih nesreća, slične oblasti su uzete u razmatranje, ali se na tom nivou nigdje ne pominje KI, niti se bilo koja struktura razmatra kao takva. Navedeni spisak u Procjeni na nivou BiH, uz određene dopune, te precizno definisanje KI i donošenje Zakona o KI u entitetima, a onda i na nivou BiH, su koraci koje je potrebno poduzeti kako bi BiH ozbiljno pristupila ZKI.

KRITIČNA INFRASTRUKTURA U REPUBLICI SRPSKOJ

Kada je u pitanju KI u Republici Srpskoj situacija je nešto bolja nego na nivou BiH i na nivou FBiH. Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj[16] pokrenuo je ovo pitanje sa mrtve tačke. Ovim Zakonom je ujedno i definisana KI u Republici Srpskoj, pa u skladu sa članom 2 ovog Zakona: "Kritične infrastrukture su sistemi, mreže i objekti od posebne važnosti, čije uništavanje ili ugrožavanjemože izazvati ozbiljan poremećaj u slobodnom kretanju ljudi, prevozu robe i pružanju usluga, negativno uticati na unutrašnju bezbjednost, zdravlje i živote ljudi, imovinu, životnu sredinu, spoljnu bezbjednost, ekonomsku stabilnost, te neprekidno funkcionisanje republičkih organa."

Kao prvo definicija je usmjerena ka sistemima, mrežama i objektima čime se sa jedne strane dala širina izbora KI u tim oblastima a sa druge strane se opet izbor ograničava samo na ove elemente. U tom kontekstu, institucije, javne službe kao i vaspitanje i obrazovanje nisu uključene, bar ne direktno, kao KI, kao ni određeni prirodni resursi poput rijeka kao ni otpad i sl.

Kao drugo, mora se uvesti i termin onesposobljavanje ili prekid u radu KI, jer će se to najčešće dešavati. Uništavanje KI je moguće kada se radi o manjim objektima i sl., ali to su veliki kompleksi koji se najčešće onesposobljavaju ili se u njima prouzrokuje prekid rada a ne uništavaju se.

Kao drugo, definicija se završava sa potrebom "neprekidnog funkcionisanja državnih organa." Time se zanemaruju KI na nivou jedinica lokalne samouprave (JLS) na čijoj teritoriji se ove infrastructure nalaze i na koje su jedinice lokalne samouprave, po pravilu, najviše oslonjene i čiji prekid u funkcionisanju na njih diretno i prvo utiče.

U tom kontekstu potrebno je u budućnosti djelovati amandmanski na ovaj Zakon i u istom unaprijediti samu definiciju koja bi glasila: *Kritične*

[16] Službeni glasnik RS, br.58/19,

infrastruktura je ona čijim uništavanjem, onesposobljavanjem, ugrožavanjem ili prekidom u radu se može izazvati ozbiljan poremećaj u slobodnom kretanju ljudi, prevozu robe i pružanju usluga, negativno uticati na unutrašnju bezbjednost, zdravlje i živote ljudi, imovinu, životnu sredinu, spoljnu bezbjednost, ekonomsku stabilnost, te neprekidno funkcionisanje republičkih organa i/ili organa jedinica lokalne samouprave.

Generalno gledano Republika Srpska se opredjelila za sektorski pristup u definisanju KI. Odnosno određeni su sektori iz kojih se određuje KI i to osnovnih 12 sektora ali se ostavlja mogućnost da se na prijedlog Ministarstva unutrašnjih poslova Republike Srpske, mogu odrediti i drugi sektori iz kojih će se razmatrati kritične infrastrukture.

U skladu sa Zakonom o bezbjednosti kritičnih infrastruktura u RS, član 3, navode se sledeći sektori i njihovi podelementi:

- industrija, energetika i rudarstvo (proizvodnja, uključujući ulazne resurse, objekte, sisteme za prenos, skladištenje, transport proizvoda, energenata i energije, sisteme za distribuciju),
- informaciono-komunikaciona infrastruktura (elektronske komunikacije, prenos podataka, informacioni sistemi, pružanje audio, i audio i video medijskih usluga),
- saobraćaj (drumski, željeznički i vazdušni saobraćaj i saobraćaj unutrašnjim plovnim putevima),
- zdravstvo (zdravstvena zaštita, proizvodnja, transport i nadzor nad lijekovima),
- komunalne djelatnosti (objekti komunalne infrastrukture, a naročito u oblasti proizvodnje i isporuke vode, prečišćavanja i odvođenja otpadnih voda, proizvodnje i isporuke toplotne energije, zbrinjavanja otpada iz stambenih i poslovnih prostora i slično),
- vodoprivreda (regulacioni i zaštitni vodni objekti),
- hrana i piće (proizvodnja i snabdijevanje hranom i pićem, sistem sigurnosti hrane i pića, robne zalihe),
- finansije (bankarstvo, berze, investicije, sistemi osiguranja i plaćanja),
- proizvodnja, skladištenje i prevoz opasnih materija (hemijski, biološki, radiološki i nuklearni materijali),
- javne službe,
- vaspitanje i obrazovanje,
- kulturna i prirodna dobra (vjerski objekti, spomenici kulture, prostorne kulturno-istorijske cjeline, arheološka nalazišta, znamenita mjesta, umjetnička djela i istorijski predmeti, arhivska građa, filmska građa, stara i rijetka knjiga, kao i zaštićena prirodna dobra propisana Zakonom o zaštiti prirode).

Kao što se može vidjeti i iz ovih sektora,važeća definicija iz Zakona nije najbolje pokrila sve navedene elemente a pored toga jasno je da dio ovih segmenata najveći uticaj ima na jedinice lokalne samouprave. I pored toga, u najvećem broju sektora i podelemenata ovdje se može govoriti o onesposobljavanju ili prekidu rada a ne o uništenju, čime predložena definicija dobija na svom značaju i sadržajnosti te usklađenosti sa predloženim sektorima.

S obzirom da je cijeli Zakon koncipiran tako da se bavi isključivo KI od republičkog značaja i zadaci vezani za imenovanje KI iz tih sektora su dati u nadležnost republičkih organa uprave nadležnih za te sektore. Na žalost u zakonu nije jasno napravljena tabela ko za koji sektor KI odgovara i ko tačno podnosi prijedlog da nešto bude KI. To u svakom slučaju treba urediti detaljnijim aneksom ko je u kojem sektoru stvarni nosilac obaveza vezanih za imenovanje KI, a ko sarađuje i na kom nivou.

Nakon što provjeri infrastrukturu koja je imenovana Ministar unutrašnjih poslova RS riješenjem potvrđuje identifikovanu KI. Nakon što se iz svih sektora dostave prijedlozi za KI isti Ministar donosi riješenje za listu sektora kritičnih infrastruktura prema njihovom značaju za opšte funkcionisanje RS, odnosno sektore KI rangira prema njihovj kritičnosti (član 5. Zakona). Zakonom je predviđeno da Vlada RS, na prijedlog Ministra unutrašnjih poslova, utvrdi postupak provjere subjekata i objekata KI imenovanih od strane republičkih organa uprave. Ovaj akt za sada nije još uvjek urađen i ne postoje smjernice za ovu vrstu provjera.

Rješenje o određivanju KI Ministar dostavlja subjektima KI i republičkom organu uprave u čijoj je nadležnosti objekat KI, na sprovođenje. Ovim rješenjem se navode subjekti KI koji su odgovorni za upravljanje i zaštitu KI u svim uslovima (član 7. Zakona).

Ministarstvo unutrašnjih poslova RS bi trebalo jednom godišnje, Vladi RS i odboru Narodne skupštine RS nadležnom za bezbjednost, da podnese izvještaj o broju KI po sektorima, stepenu njihove ugroženosti, te sprovođenju mjera njihove zaštite (član 6. Zakona).

ZAŠTITA KRITIČNE INFRASTRUKTURE U REPUBLICI SRPSKOJ

U skladu sa članom 4. Zakona o bezbjednosti kritičnih infrastruktura u RS “zaštita kritične infrastrukture podrazumijeva sve aktivnosti kojima je cilj da obezbijede funkcionalnost, neprekidno djelovanje i isporuku robe i usluga kritične infrastrukture, te da spriječi ugrožavanje kritične infrastructure.”

Ovim Zakonom je predviđeno da Ministarstvo unutrašnjih poslova, “u saradnji sa nadležnim republičkim organom uprave, iz čije nadležnosti je pojedina kritična infrastruktura, redovno prati i procjenjuje prijetnje, predlaže

operativne i druge mjere za procjenjivanje kritičnosti, kao i mjere za upravljanje i zaštitu kritičnih infrastruktura."[17]

Republički organi uprave iz čije nadležnosti je pojedina KI i Ministarstvo unutrašnjih poslova, odgovorni su, ne samo za određivanje pojedinih sistema ili njihovih dijelova kao KI, upravljanje KI, već i za njihovu zaštitu.

U članu 8. Navedenog Zakona pominje se "Metodologija" koju donosi Ministar unutrašnjih poslova RS ali se ne navodi u vezi čega je navedena metodologija. Za nju se kaže da se označava odgovarajućim stepenom tajnosti a sledeći paragraph istog člana pominje "sektorske mjere" koje određuje republički organ uprave nadležan za sektor u kome je KI. Iako nije jasno povezana "metodologija" i sektorske mjere, pretpostaviti je da se radi o Metodologiji izrade sektorskih mjera za zaštitu KI! Na žalost to u samom zakonu nije jasno navedeno pa se samo može pretpostvljati.

Interesantno je da se predviđa stavom (4) člana 8. Zakona da "republički organi uprave mogu konsultovati strukovna udruženja za svaki pojedinačni sektor". Na žalost nije jasno definisano kako će ta udruženja dobiti dozvolu za pristup stepenovanom dokumentu "Metodologije" i koje preduslove trebaju da ispune ta strukovna udruženja da bi bila angažovana.

Za svaki sektor KI određuje se bezbjednosni koordinator i njjegov zamjenik a određuje ga republički organ uprave. Pored toga, u skladu sa članom 14. „odgovorni subjekti kritične infrastrukture (kao pravna lica) dužni su da odrede lice koje je direktno odgovorno za upravljanje i zaštitu objekata kritične infrastrukture."

Zakonom o bezbjednosti kritičnih infrastruktura u Republici Srpskoj je predviđeno da se u roku od šest mjeseci donese podzakonski akt kojim se utvrđuje postupak provjere subjekata i objekata kritične infrastrukture. Pored toga predviđeno je istim Zakonom da se za 18 mjeseci od dana stupanja na snagu Zakona, od strane rukovodioca republičkih organa uprave, donesu sektorske mjere, a dvet mjeseci nakon usvajanja tih sektorskih mjera treba se donijeti određena „metodologija". Ni u članu 24. Zakona nije naveden naziv metodologije te se samo može pretpostavljati o čemu se radi. Tek šest mjeseci nakon donošenja „Metodologije", republički organi uprave dužni su predložiti KI iz sektora njihove nadležnosti i nivo njihove kritičnosti. Ostaje nejasno o kom se nivou radi kada u Zakonu nikakvi nivoi KI nisu predviđeni.

U skladu sa navedenim rokovima i vremenom donošenja Zakona o bezbjednosti kritičnih infrastruktura Republike Srpske, prva imenovana KI u RS se može očekivati sredinom 2022.godine. S obzirom na dinamiku donošenja podzakonskih akata, ovo zvuči optimistički.

[17] Član 6. Zakon o bezbjednosti kritičnih infrastruktura, Službeni glasnik RS, br.58/19.

OKVIR PROCJENE KRITIČNE INFRASTRUKTURE U REPUBLICI SRPSKOJ

Zakonom o bezbjednosti kritičnih infrastruktura u Republici Srpskoj[18], u članu 9. ulazi se usferu analize rizika KI sa aspekta njenog prekida rada. I u ovom slučaju se predviđa postojanje Metodologije i sektorskih mjera, ali se ne daje odgovor o kakvoj metodologiji je riječ. Pretpostaviti je da se radi o Metodologiji za analizu rizika prekida rada KI.

Prema istom članu pri Analizi rizika svih KI, procjenjuju se direktna i indirektna šteta. Kao direktna šteta, procjenjuju se:

- ljudski gubici (procjenjuje se mogući broj smrtno stradalih ili povrijeđenih zbog prekida rada pojedine kritične infrastrukture),
- ekonomski gubici (procjenjuju se prema važnosti ekonomskog gubitka ili smanjenja kvaliteta proizvoda ili usluga, uključujući i mogući uticaj na životnu sredinu),
- uticaj na javnost (procjenjuje se prema uticaju na povjerenje javnosti, fizičke patnje i narušavanje svakodnevnog života, uključujući i gubitak osnovnih, te javnih usluga).

Pored direktnih, procjenjuju se i indirektne štete i to:

- dugoročan uticaj na integritet pojedinaca i zajednice (procjenjuje se prema važnosti podataka sa stanovišta funkcionisanja zajednice, ostvarivanja ljudskih prava i sloboda),
- dugoročna ekonomska šteta (procjenjuje se prema važnosti podataka za zaštitu kolektivnih vrijednosti i onemogućavanja podrivanja ličnih i kolektivnih ekonomskih interesa),
- dugoročan uticaj na kvalitet životne sredine (procjenjuje se prema važnosti i transparentnosti podataka o sistemima i opasnostima koje mogu bitno uticati na kvalitet životne sredine).

Ovu analizu rizika trebalo bi da radi nadležni republički organ uprave u saradnji sa Ministarstvom unutrašnjih poslova kao i sa odgovornim subjektom KI. Pored analize oni rade i sektorske planove obezbjeđenja rada KI. Treba istaći da u Zakonu nije predviđena saradnja sa jedinicama lokalne samouprave na čijoj teritoriji se nalazi KI a predviđena je konsultacija sa strukovnim udruženjima za svaki pojedinačni sektor, ali uz saglasnost Ministarstva unutrašnjih poslova Republike Srpske.

Treba istaći da je Zakonom predviđeno da se pri procjeni rizika i potrebnog stepena zaštite uzima u obzir i djelovanje pojedinog sektora ili mreže kritične infrastrukture na druge kritične infrastrukture. Ova analiza rizika je osnova za izradu bezbjednosnog plana.

[18] Službeni glasnik RS, br.58/19

Kako stoji u članu 12. Zakona, „bezbjednosni plan obezbjeđuje povjerljivost, potpunost i raspoloživost organizacionih, kadrovskih, materijalnih, informaciono-komunikacionih i drugih rješenja, te stalnih bezbjednosnih mjera potrebnih za neprekidno funkcionisanje kritične infrastrukture.“ Ovaj plan obuhvata mjere zaštite i obezbjeđenja nastavka funkcionisanja KI i izrađuju ga subjekti KI. Predviđeno je da već postojeći dokumenti, koji su izrađeni na osnovu nekih drugih sektorskih propisa, mogu biti sastavni dio ovih bezbjednosnih planova. Za izradu ovog Plana zakonodavac je dao godinu dana od dobijanja rješenja o određivanju KI.

U istom članu 12. u paragrafu 5. stoji da „nadležni republički organ uprave u čijoj nadležnosti je kritična infrastruktura utvrđuje vrijednost dokumenata izrađenih na osnovu drugih sektorskih propisa kojima su regulisane mjere zaštite.“ Ostaje nejasno na koju vrijednost se to odnosi, ali se da pretpostaviti da se misli o značajnosti tih drugih dokumenata i mogućnosti njihovog korištenja u planu bezbjednosti, u cjelini ili nekih njihovih dijelova.

Na bezbjednosni plan saglasnost daje nadležni organ republičke uprave u čijoj nadležnosti je KI. Da bi se dobila saglasnost potrebno je da je plan urađen u skladu sa „Metodologijom“ i sektorskim mjerama. Treba istaći da ovaj bezbjednosni plan nije javno dostupan jer posjeduje određenu bezbjednosnu klasifikaciju, kako je to već ranije naglašeno.

Pored mjera zaštite i obezbjeđenja nastavka funkcionisanja KI, a koje predviđa član 12. Zakona, bezbjednosni plan, po članu 13. obuhvata i sljedeće:

- „određivanje važnih dijelova ili objekata mreže kritičnih infrastruktura,
- sprovođenje analize rizika zasnovane na scenariju velikih prijetnji, ranjivosti svakog objekta, sistema, mreža i funkcionalnosti i mogućim posljedicama u redovnom radu, te u slučaju prestanka rada ili korištenja kritične infrastrukture, uključujući i rizik od napuštanja lokacije kritične infrastrukture,
- identifikaciju, izbor i određivanje svih potrebnih mjera i postupaka za smanjenje ranjivosti i obezbjeđenje djelovanja svih utvrđenih kritičnih dijelova ili objekata mreže ili sistema, i to:
- stalnih bezbjednosnih mjera i postupaka koji se kontinuirano primjenjuju (tehničkih, organizacionih, komunikacionih mjera, mjera i postupaka ranog upozoravanja i jačanja svijesti) i koji određuju nužne troškove u bezbjednosti,
- postepenih bezbjednosnih mjera i postupaka koji se aktiviraju u zavisnosti od jačanja prijetnji.“

Ovi planovi se trebaju revidirati bar jednom godišnje, odnosno u Zakonu u članu 13. stoji da se isti „analiziraju tokom prve godine od dana određivanja kritične infrastrukture, a nakon toga se analiziraju redovno jednom

godišnje.“ Nakon analize bi trebala ići revizija ali na žalost to tako nije predviđeno Zakonom.

Članom 16. Zakona je predviđeno i imenovanje štaba za krizne situacije u slučaju uništavanja ili oštećenja dijelova KI oragna republičke uprave. Ostaje pitanjevezano za nadležnosti štabova za krizne situacije i štabova za vanredne situacije, koje predviđa Zakon o zaštiti i spasavanju u vanrednim situacijama (član 8.)[19], a posebno kad do oštećenja KI dođe usled prirodnih i drugih nepogoda. Ovim zakonom taj segment mora biti bolje obrađen i definisan te usklađen sa postojećim Zakonom o zaštiti i spasavanju u vanrednim situacijama.

PROCJENE UGROŽENOSTI

Dokument Evropske komisije „Procjena rizika i smjernice za mapiranje u upravljanju vanrednim situacijama“[20] predstavlja jedan od dokumenata koji daje osnovne smjernice procjena rizika za sve zemlje članice MCZEU. Prema ovom dokumentu „Uporedivost metoda procjene rizika bi trebalo da doprinesu vrijednosti pojedinačnih napora država članica i da omoguće procjene rizika da se spoje (zajedničke procjene rizika) među regionima ili državama članicama koje se suočavaju sa zajedničkim rizicima. Uporedive metodologije bi takođe omogućile šire i bolje uvažavanje uticaja katastrofa sa kojima su se suočile neke ali ne i sve države članice.“ Pored toga, zajednička terminologija i zajedničko razumijevanje pojmova ćeznačajno olakšati doslijednost iuporedivost.Ovaj dokument predviđa da sve strane uključene u Proces procjene rizika treba da:

a) se dogovore o kriterijumima bodovanja na početku procesa procjene,

b) evidentiraju upotrebljene metode i njihov nivo neizvjesnosti,

c) obrate pažnju na opravdanje za uključivanje ili isključivanje specifičnih rizika,

d) evidentiraju rezultate dodijeljene svakom riziku i njihovo opravdanje,

e) osmisle protokol za korišćenje stručnog mišljenja.

Pregled prirodnih i antopoloških rizika u EU a u skladu sa ovim dokumentom[21] ističe određene oblasti na koje treba obratiti pažlju tokom procjene rizika i bez kojih se valjana procjena rizika ne može napraviti, a to su:

[19]Službeni glasnik RS, br: 121/12

[20] Risk Assessment and Mapping Guidelines for Disaster Management, SEC (2010) 1626 final, European Commission, Brussels, 2010

[21] Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final, European Commission, Brussels, 2017

- međuzavisnosti država, snaga, ali i samih različitih vrsta opasnosti,
- kaskadni efekti u kojima jedna opasnost pokreće drugu,
- prekogranični i regionalni rizici i
- uticaj klimatskih promjena.

Uticaj opasnosti kroz ovaj dokument se prije svega odnosi na uticaj na ljude, ekonomiju i ekologiju kao i na političko/društveno stanje u zajednici. Ovo su osnovne tri vrijednosti koje se štite procjenom rizika i u odnosu na njih je predviđena procjena uticaja a time i rizika po iste. Za ove vrijednosti se rade skale i iste mogu biti kvalitetivne i kvantitativne. Preporuka je da se za uticaj na ljude koristi procjena broja poginulih, povrijeđenih, evakuisanih ili oboljelih. Kada se govori o ekološkom i ekonomskom uticaju onda bi se skale trebale kreirati u skladu sa štetama u eurima dok bi skla za političko/društveni uticaj trebala biti polu-kvantitativna. Ovaj uticaj se može predstaviti i kao šteta nastala kroz određenu opasnost. Treba istaći da se kroz segment političko/društvenog stanja u zajednici definiše i uticaj opasnosti na KI i sve zemlje u okruženju koriste ovu, kao jednu od varijabli, za opis ovog uticaja. Najčešće se kao norma procjene uticaja prirodnih opasnosti na KI koriste nekoliko segmenta a to su postotak šteta u budžetu (Hrvatska i Srbija) ili dužina trajanja prekida u funkcionisanju KI (Finska i Slovenija) , broj ljudi na koje taj poremećaj utiče (Slovenija i Srbija) i sl. Nažadlost JLS same bez ikakve metodologije procjewuju šta je KI za njih i rade procjene. Sada na osnvu sektorske podjele u Zakonu o bezbjednosti kritičnih infrastruktura imaju osnovnu smjernicu.

Prema osnovnim dokumentima EU, koji su vezani za procjenu rizika od prirodnih i drugih opasnosti, u procjeni rizika se mora u obzir uzeti ne samo učestalost odnosno vjerovatnoća i posljedice u smislu novčanih i ekonomskih gubitaka, nego se moraju uzeti u obzir i pitanja savremenog čovjeka a to su: klimatske promjene, naseljenost, infrastruktura ali i migranti, pad biodiverzitet, pad otpornosti na mikrobe, pad otpornosti na antibiotike, uticaj gradnje na izgled okruženja, uticaj eksploatacija ruda na okruženje, uticaj eksploatacije šljunka na riječnia korita, cyber opasnosti, terorizam. Naša svjesnost svih ovih opasnosti natjeraće nas da se njima bavimo ali postoje i opasnosti kojih nismo još svjesni ili im ne pridajemo značaj jer smatramo da se kod nas ne dešavaju pa i nisu bitne: erupcije vulkania, havarije na nuklearnim elktranama, sunčeve pjege i sl. Svako ko se ozbiljno bavi procjenama rizika mora razmotriti realnost ovih opasnosti i identifikovati rizike u skladu sa nivoom procjne (lokalni, regionalni, državi, međudržavni). Kako god je od ovih upasnosti ugrožena teritorija tako je i sva KI na istoj ugrožena i mora biti njena ugroženost procjenjena.

Postojeće procjene ugroženosti od prirodnih i drugih nesreća u BiH trebaju se usaglasiti sa osnovnim direktivama EU a posebno iz razloga što BiH

teži ka članstvu u evropskom mehanizmu civilne zaštite, a isto tako i buduća metodologija procjene ugroženosti KI. Postojeće metodologije za procjenu ugroženosti od prirodnih i drugih opasnosti na svim nivoima trebaju se revidirati i koncipirati tako da se u njima nalaze jasni kriterijumi za određivanje vjerovatnoće i posljedica po štićene vrijednosti. Pored toga nove metodologije treba da sadržive veličinu i izgled matrica rizika (5X5) kao i nivoe rizika (četiri nivoa rizika) usklađene sa evropskim direktivama. Kod procjena ugroženosti KI na isti način bi trebalo pristupiti izradi metodologije a posebno sa aspekta učešća procjene KI u procjeni ugroženosti jedinica lokalne samouprave od prirodnih i drugih opasnosti. Pored toga potrebno je definisati i koji rizici su prihvatljivi a koji ne i u skladu sa tim usmjeriti dalje proces planiranja i izrade Planova zaštite i spasavanja. Metodologije treba dopuniti i sa sadržajem i izgledom te načinom izrade reperezenatativnih scenarija za najvjerovatnije neželjene događaje ali i scenarija za događaje sa najgorim mogućim posljedicama. Ovo bi trebao biti i model procjene ugroženosti KI, jer izrada scenarija i riziko-bazirano dimenzioniranje predstavljaju osnovu procjene rizika od prirodnih i drugih opasnosti a time trenutnio i jedini način procjene KI na nivou lokalne samouprave. Time bi se omogućio jedinstven pristup procjeni ugroženosti od najvišeg do najnižeg nivoa vlasti u BiH a samim tim bi se omogućila komparacija i izrada procjena u skladu sa EU standardima. U slučaju da BiH ove godine postane članica MCZEU, već sledeće godine će biti dužna da uputi svoju Procjenu ugroženosti usklađenu sa evropskim standardima.U Zakonu o bezbjednosti kritičnih infrastruktura Republike Srpske[22], nisu predviđeni nivoi rizika za KI. Nadati se da će biti u „metodologiji“ i da će biti usklađeni sa drugim dokumentima.

Posebno treba istaći da je pitanje KI sastavni dio ovih navedenih procjena i iste se ne mogu realizovati kvalitetno bez procjene KI. Ta procjena u opštinama odnosno jedinicama lokalne samouprave će se moći kvalitetno realizovati kada se izvrši imenovanje KI i kada se bude usmjerio fokus prema određenoj KI u jedinicama lokalne samouprave. Treba istaći da se KI nalazi u sistemu procjene u dijelu ugroženih vrijednosti a to je političko/društveno stanje i ne prestavlja samosatalanelement procjene. Novim Zakonom o bezbjednosti kritičnih infrastruktura treba da se definiše i Metodologija procjene KI što u svakom slučaju treba uskladiti sa načinom procjene KI u Zakonu o zaštiti i spasavanju u vanrednim situacijama. Time bi se dobila jedna jedinstvena slika stanja ugroženosti kritične infrastrukture a i metodološki bi KI bila tačnije i pravilnije procjenjena na nivou jedinica lokalne samouprave.

[22] Službeni glasnik RS, br.58/19

ZAKLJUČAK

Iz svega navedenog može se izvesti nekoliko značajnih zaključaka. Kao prvo Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj je pionirski pokušaj da se ova materija reguliše te je potrebno kao prvo podržati taj napor da se to uradi. Sa druge strane potrebno je dati i određenu konstruktivnu kritiku postojećeg zakonskog rješenja kako b se sa ovom problematikom pokušalo krenuti, od početka na zdravim osnovama.

Zakon nije prepoznao evropsku, međuentitetsku i međudržavnu infrastrukturu te je time na samom početku stvoren prostor za manipulacije, ali i siva zona, nejasna legislativa kod imenovanja kritične infrastrukture, njene procjene posebno a onda i zaštite. Kroz određene uredbe koje slijede i metodologije, ova problematika se može jasnije definisati i stvoriti preduslovi za kvalitetnu procjenu.

Sama definicija koja je data u Zakonu, kao što je već navedeno, ne pokriva sve sektore i ne obuhvata sve okolnosti u kojima se može naći kritična infrastruktura. Iako je malo vjerovatno da će se Zakon mjenjati zbog definicije, treba navedene sugestije imati u vidu tokom procjena kritične infrastrukture.

Vrlo je bitno istaći da postoji potreba za većom saradnjom sa jedinicama lokalne samouprave kada je u pitanju imenovanje kritične infrastrukture a posebno kod njene procjene i zaštite. U samom Zakonu su jedinice lokalne samouprave nekako skrajnute dok mnogo veću pažnju dobijaju razna strukovna udruženja koja se mogu uključiti u ovaj proces, ali nema jasno navedenih strukovnih udruženja ni načina na koji oni mogu postati učesnici u procjeni rizika i imenovanju kritične infrastrukture a posebno jer su to stepenovana dokumenta koja se izrađuju i po kojima se radi.

Pored toga u jednom dijelu Zakona pominju se i štabovi za krizne situacije, a nije jasno ko ih i kada formira s obzirom da jedinice lokalne samouprave imaju obavezu formiranja štabova za vanredne situacije, u skladu sa Zakonom o zaštiti i spasavanju u vanrednim situacijama. Odnosi ovih štabova su nejasni i potrebno je uraditi posebnu obradu ovog problema jer kritična infrastruktura nije u međuprostoru nego na teritoriji jedinica lokalne samouprave. Time i njihovi štabovi imaju odgovornost, jer štite građane i teritoriju. O ovoj problematici se moralo malo više povesti računa kao i o metodologijama. Metodologije procjene ugroženosti od prirodnih i drugih opasnosti tretiraju već kritičnu infrastrukturu u pojedinim segmentima te je potrebno konsultovati te metodologije tokom izrade metodologija procjene rizika i prekida rada kritične infrastrukture da ne bude kao sa planovima zastite od poplava koje imaju jedinice lokalne samouprave i planovima zastite od poplava koje pravi JU Vode RS i oni „ne pričaju“. Ili kod plana zaštite od

požara gdje je jedan sadržaj u zakon o zaštiti od požara a drugi u urebi o načinu izrade procjene ugroženosti od prirodnih i drugih nepogoda RUCZ.

Na kraju, postojanje i donošenje ovog zakona je pohvalno ali je potrebno bilo malo više konsultovati struku i uvažiti njeno mišljenje pri njegovoj izradi.

LITERATURA

1. *Bečka konvencija o diplomatskim odnosima od 18. aprila 1961.godine*, "Službeni list SFRJ" - dodatak, 2/64
2. *Direktiva Vijeća 2008/114/EZ O utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite*, Službeni list Europske Unije L 345/75,2008, https://eurlex.europa.eu/legalcontent/HR/TXT/PDF/?uri=CELEX:32008L0114 &from =en , preuzeto 22.03.2021.
3. Edward N. Lorenc, *Deterministic Nonperiodic Flow*, Journal of The Atmospheric Sciences, Volume 20, 1963, https://www.astro.puc.cl/~rparra/tools/PAPERS/lorenz1962.pdf, preuzeto 18.06.2021.
4. Eva Nagyfejeo and Sarah Puello Alfonso, *Cybersecurity Capacity Review Bosnia and Herzegovina*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658404, SSRN, 2019, posjećeno 09.04.2021.
5. *Ministarstvo bezbjednosti BiH, Strategija Bosne i Hercegovine za prevenciju i borbu protiv terorizma (2006-2009)*, Sarajevo, 2006.
6. *Ministarstvo bezbjednosti BiH, Strategija Bosne i Hercegovine za prevenciju i borbu protiv terorizma (za period od 2010–2013. godine)*, Sarajevo, 2010., http://www.psa.gov.ba/Popisi_i_dokumenti/Propisi/Strategije/Strategija%20BiH%20za%20prevenciju%20i%20borbu%20protiv%20terorizma.pdf,preuzeto 14.04.2021.
7. OSCE, *Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini*, Sarajevo, 2019, https://www.osce.org/files/f/documents/4/8/438386.pdf,preuzeto 15.05.2021.
8. *Overview of Natural and Man-made Disaster Risks the European Union may face*, SWD(2017) 176 final, European Commission, Brussels, 2017
9. *Procjena ugroženosti Bosne i Hercegovine od prirodnih ili drugih nesreća*, Savjet ministara, Sarajevo, 2011.

10. *Risk Assessment and Mapping Guidelines for Disaster Management*, SEC (2010) 1626 final, European Commission, Brussels, 2010
11. Savjet Ministara BiH, *Strategija uspostave CERT-a u Bosni i Hercegovini (CERT- Tim za odgovor na računarske incidente - Computer Emergency Response/Readiness Team),* Sarajevo, 2011, http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=en-US, preuzeto 15.05.2021.
12. *Zakon o bezbjednosti kritičnih infrastruktura,* Službeni glasnik RS, br.58/19.
13. *Zakon o državnoj agenciji za istrage i zaštitu,* "Službeni glasnik BiH", br. 27/2004, 63/2004, 35/2005, 49/2009 i 40/2012
14. *Zakon o zaštiti i spasavanju u vanrednim situacijama,* Službeni glasnik RS, br: 121/12

REVIEW OF THE LAW ON SECURITY OF CRITICAL INFRASTRUCTURES IN THE REPUBLIC OF SRPSKA

Dr Dragiša Jurišić[23]

Abstract: Critical infrastructure and its consideration is a relatively new discourse, in the field of security. In the context of modern threats from terrorism, but also those caused by climate change, the definition and protection of critical infrastructure are of great importance for the successful functioning of modern states. BiH, as a state, has an obligation to address this issue, but so far only the Republic of Srpska has passed the Law on Critical Infrastructure Security and thus created the preconditions for its definition, assessment and protection measures. The law was passed in 2019, but it is being processed slowly, so the question of its applicability and the need for certain changes or amendments through the envisaged methodologies, instructions and assessments remains. In this paper, the analysis of the existing Law on Critical Infrastructure Safety was performed, certain suggestions on its content were given, as well as certain recommendations in order to make the Law more applicable and to fulfill its purpose in the future.

Keywords: Critical infrastructure, Critical infrastructure protection, law, protection, the Republic of Srpska, BiH

[23] Security Research Center, Banja Luka.

UMREŽENOST ZAKONA O MJERAMA BEZBJEDNOSTI U POSLOVANJU GOTOVIM NOVCEM I DRUGIM VRIJEDNOSTIMA SA ZAKONOM O BEZBJEDNOSTI KRITIČNE INFRASTRUKTURE U REPUBLICI SRPSKOJ

Mr Željko Zorić[1]
Mr Dragana Kosić[2]

Apstrakt: Vođena potrebom podizanja bezbjednosti na viši nivo, posebno sektora u kome se posluje gotovim novcem i drugim vrijednostima, Narodna skupština Republike Srpske usvojila je Zakon o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima 2015. godine. Osnov za usvajanje Zakona o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima pronađen je u međunarodnom standardu ISO 31000 kojim se definišu principi i opšte smjernice za upravljanje rizikom, čime je stvoren pravni okvir koji će omogućiti efikasnu primjenu osnovnih mjera bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima, te doprinijeti smanjenju rizika i zaštiti zaposlenih od izvršenja krivičnih djela i prekršaja kojim se narušava bezbjednost lica i imovine. Učestale krize, praćene neizostavnim štetama, kao i potreba usklađivanja bezbjednosnih tokova sa međunarodnom praksom, uticali su na usvajanje Zakona o bezbjednosti kritične infrastrukture 2019. godine, koji treba da dovede do stepena bezbjednosti koji će uticati na prevenciju kriznih situacija. U radu će biti analizirana praktična primjena Zakona o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima. Prikazaće se uloga i značaj privatnog sektora bezbjednosti u primjeni navedenih zakona odnosno značaj privatno-javnog partnerstva u ostvarivanju sistema bezbjednosti.

Ključe riječi: procjena ugroženosti, mjere zaštite, fizičko i tehničko obezbjeđenje, kritična infrastruktura

UVOD

Razlozi za donošenje Zakona o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima[3] sadržani su u potrebi da se bezbjednost u poslovanju sa gotovim novcem i drugim vrijednostima podigne

[1] Sector Security, direktor Sektora fizičkog obezbjeđenja, e-mail: zeljko.zoric@sectorsecurity.org
[2] Sector Security, generalni direktor, e-mail: dragana.kosic@sectorsecurity.org
[3] Službeni Glasnik Republike Srpske, broj 33/2015.

na viši nivo i da se primjenom odgovarajućih mjera bezbjednosti preventivno djeluje u cilju zaštite lica i imovine.

Neuređenost u oblasti primjene mjera bezbjednosti, često interno uređena dogovorom korisnika usluga s jedne strane, i ponuđača usluga s druge strane, imala je za posljedicu usvajanje neefikasnih sistema, koji su, nerijetko, narušavali privatnost građana stvarajući kod istih averziju prema ponuđačima usluga. Na ovaj način današnja, nasušna potreba, obezbjeđenja lica i imovine, kao novina na ovim prostorima, bila je dovedena u pitanje. Porast krivičnih djela, naročito imovinskih krivičnih djela, doprinosi ozbiljnijem shvatanju potrebe razvoja ove oblasti. Pozitivna iskustva u okruženju, posebno iz Republike Hrvatske i Republike Srbije, uticala su i na pokretanje inicijative da se ukupni bezbjednosni ambijent u Republici Srpskoj dodatno poboljša usvajanjem Zakona o procjeni ugroženosti u poslovanju gotovim novcem i drugim vrijednostima.

Uvažavajući činjenicu da je u oblasti poslovanja gotovim novcem i drugim vrijednostima potrebno primijeniti sve raspoložive mjere kako bi se izvršenje krivičnih djela na štetu zaposlenih, lica i imovine obveznika Zakona o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima svelo na minimum, pristupilo se izradi Zakona o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima, a sve u cilju što efikasnije zaštite lica i imovine, uzimajući u obzir činjenicu da je, sa bezbjednosnog aspekta, predmetna oblast uvijek aktuelna.[4]

Međutim, i pored opravdanih razloga koji su uticali na donošenje Zakona o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima, njegova adekvatna primjena, u praksi, je izostala.[5] Zbog otpora u primjeni istog od strane brojnih subjekata, izostanka sankcije, Zakon o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima nije zaživio u praksi, niti je donio željene rezultate, a što je za posljedicu imalo sve veći broj izvršenih teških krivičnih djela. Nakon toga, pristupilo se izradi Pravilnika o procjeni ugroženosti u poslovanju gotovim novcem i drugim vrijednostima kojim je mnogo jasnije i konkretnije opisana primjena Zakona o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima.[6] Prvi put se Pravilnikom o procjeni ugroženosti u poslovanju gotovim novcem i drugim

[4] Izvod iz obrazloženja Zakona o poslovanju gotovim novcem i drugim vrijednostima koji je usvojen 17. aprila 2015. godine, a objavljen u Službenom glasniku Republike Srpske 30.04.2015. godine.

[5] Više: Zorić Ž., "Cooperation between the private and public security in order to realise security system", V International scientific conference safety and crisis management – theory and practice safety for the future - SeCMan, 2019, Belgrade.

[6] Pravilnik je usvojen 23. decembra 2016. godine, a objavljen u Službenom glasniku Republike Srpske 29. decembra 2018. godine.

vrijednostima definiše procedura izrade Akta o procjeni ugroženosti pozivanjem na standard *BAS ISO 31000.* [7]

Potreba praćenja aktuelnih događanja u neposrednom okruženju i težnji Evropske unije da se identifukuje kritična infrastruktura sa svim mogućim rizicima i načinima odgovora na rizike, doveli su do usvajanja novih zakonskih rješenja u Republici Srpskoj. Na temelju stvarnih potreba 2019. godine usvojen je Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj[8], čime su zaokruženi napori da se bezbjednost shvati kao stvarna potreba, a ne kao imaginarna "priča" o nekome ili nečemu.

ZAKON O MJERAMA BEZBJEDNOSTI U POSLOVANJU GOTOVIM NOVCEM I DRUGIM VRIJEDNOSTIMA

Zakonom o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima su propisane osnovne mjere bezbjednosti za pravna i fizička lica koja posluju gotovim novcem i drugim vrijednostima, određuje se stepen primjene mjera bezbjednosti, način primjene mjera bezbjednosti, transport i prenos gotovog novca i drugih vrijednosti, čuvanje, zaštita i obrada podataka koji su prikupljeni sredstvima tehničke zaštite, nadzor i sprovođenje nadzora. Odredbe propisane Zakonom ne primjenjuju se na objekte, prostorije i zaposlene u pravnim licima ako obezbjeđenje vrši Ministarstvo unutrašnjih poslova Republike Srpske.

Ovakvim određenjem izvršena je diskriminacija između subjekata koji se bave istim ili sličnim poslovima, u smislu implementiranja osnovnih mjera

[7] Ovaj međunarodni standard može da koristi bilo koje javno, privatno ili društveno preduzeće, udruženje, grupa ili pojedinac. Stoga, ovaj međunarodni standard se ne odnosi posebno ni na jednu industriju ili sektor. NAPOMENA: Radi lakšeg snalaženja, različiti korisnici ovog međunarodnog standarda su označeni kao opšti termin "organizacija". Ovaj međunarodni standard se može primjeniti tokom postojanja organizacije i na širok spektar aktivnosti, uključujući strategiju i odluke, operacije, procese, funkcije, projekte, proizvode, usluge i imovinu. Ovaj međunarodni standard se može primjeniti na svaku vrstu rizika, ma kakva je njegova priroda, bilo da ima pozitivne ili negativne posljedice. Iako ovaj međunarodni standard pruža opšte smjernice, on nema za cilj da promoviše jednoobraznost upravljanja rizikom u svim organizacijama. Prilikom dizajna i implementacije planova i okvira za upravljanje rizikom treba uzeti u obzir različite potrebe specifične organizacije, njene posebne ciljeve, kontekst, strukturu, operacije, procese, funkcije, projekte, proizvode, usluge ili imovinu i primjenjenu specifičnu praksu zaposlenih. Ovaj međunarodni standard predviđen je da se koristi za harmonizaciju procesa upravljanja rizikom u postojećim i budućim standardima. On daje zajednički pristup za podršku standardima koji se bave specifičnim rizicima i/ili sektorima, ali ne zamjenjuje te standarde. Ovaj međunarodni standard nije namjenjen za sertifikaciju. Izvor: Institut za standardizaciju Bosne i Hercegovine, http://www.bas.gov.ba/standard/

[8] Službeni Glasnik Republike Srpske, broj 58/2019.

bezbjednosti, odnosno akta o procjeni ugroženosti u poslovanju gotovim novcem i drugim vrijednostima. Naime, nije jasno ko i na koji način vrši inspekcijski nadzor nad subjektima koji su u obavezi da primijene odrebe ovog Zakona, a obezbeđenjem su vezani za Ministarstvo unutrašnjih poslova Republike Srpske. Članom 14. stav 2 ovog Zakona propisano je da inspekcijski nadzor nad sprovođenjem ovog zakona vrše ovlašćena službena lica Ministarstva. Postavlja se pitanje, ako je Ministarstvo unutrašnjih poslova odgovorno i za bezbjednost objekta, kako onda mogu sami sebi vršiti inspekcijski nadzor? Ukoliko je nešto takvo i moguće, postavljaju se i dalja pitanja vezana za objektivnost inspekcijskog nadzora. Znači, inspekcijskim nadzorom koji potiče od subjekta koji i vrši obezbjeđenje objekta i ima obavezu primjene obaveznih mjera zaštite, otvara se prostor za moguću korupciju. Istim Zakonom agencijama koje se bave fizičko-tehničkom zaštitom strogo je zabranjeno da se bave poslovima procjene definisanim pomenutim Zakonom..

Zakonom su propisane osnovne (minimalne) mjere bezbjednosti zaštite lica i objekata u poslovanju gotovim novcem i drugim vrijednostima (Član 4. stav 1. Zakona):

- sredstva tehničkog obezbjeđenja;
- fizičko obezbjeđenje;
- kombinovana primjena mjera tehničkog i fizičkog obezbjeđenja.

Uzimajući u obzir da su propisane osnovne (minimalne) mjere bezbjednosti postavljene suviše široko, zakonodavac je članom 5. Zakona kategorisao subjekte koji imaju obavezu primijeniti mjere zaštite:

I kategorija - banke i njihove organizacione jedinice i pošte i njihove organizacione jedinice;

II kategorija – mjenjačnice, mikrokreditne organizacije, kazina, lutrije, sportske kladionice i slično;

III kategorija – bankomati;

IV kategorija – pravna i fizička lica koja posluju plemenitim metalima ili predmetima od plemenitih metala i dragim kamenjem;

V kategorija – ostala pravna i fizička lica koja posluju gotovim novcem i ostvaruju dnevni promet gotovog novca u iznosu većem od 5.000 konvertibilnih maraka.

Nakon što su propisane osnovne (minimalne) mjere bezbjednosti i izvršena kategorizacija subjekata, Zakonodavac je članom 6. definisao osnovne mjere bezbjednosti:

1) protivprovalni sistemi sa mogućnostima hitnog upozorenja;
2) sistemi hitnog upozorenja u vanrednim situacijama (protivprepadni sistemi);
3) sistemi-video nadzora, neprekidnog ili povremenog, sa mogućnošću čuvanja podataka;

4) ugradnja neprobojnih pregrada i protivprovalnih vrata na dijelu koji odvaja radne prostorije od prostorija koje su dostupne komitentima ili drugim korisnicima usluga i
5) fizičko obezbjeđenje objekata i prostorija.

Stavom 4. ovog Zakona, obveznik zakona dužan je donijeti poseban opšti akt kojim se propisuje primjena osnovnih mjera bezbjednosti. Ovaj stav može dovesti u dilemu primjenu Pravilnika o uslovima i načinu sprovođenja tehničkog i fizičkog obezbjeđenja, kojim je regulisano ko i pod kojim uslovima može da se bavi poslovima predmetne zaštite.[9]

Dilema se odnosi na nejasnoću oko donošenja akta kojim će se definisati osnovne mjere bezbjednosti. Imajući u vidu da je Zakon iznad Pravilnika jasno je da obveznik zakona donosi traženi akt o primjeni osnovnih mjera bezbjednosti. No, da li je obveznik zakona kompetentan da razumije osnovne mjere bezbjednosti, odnosno da li ih mora poznavati? Bilo bi mnogo jasnije i prihvatljivije da se Zakonom reguliše *obaveza* obveznika zakona da sve poslove oko izrade samog akta do implementacije sistema traži od privrednog društva registrovanog za obavljanje poslova zaštite. Ovo iz razloga što obveznik zakona usljed nerazumijevanja fizičko tehničke zaštite, kao i smanjenja troškova implementacije iste može predvidjeti obim zaštite koji ne zadovoljava stvarne potrebe objekta ili prostorija u kojima se obavlja djelatnost.

Članom 8. Zakona nastoji se jasnije definisati primjena osnovnih mjera bezbjednosti u kategorisanim objektima iz člana 5. ovog zakona:

(1) obveznici zakona I kategorije dužni su u objektima u kojima se posluje gotovim novcem obezbijediti osnovne mjere bezbjednosti iz Člana 6, i to: protivprovalni sistem sa mogućnostima hitnog upozorenja, sistem hitnog upozorenja u vanrednim situacijama i sistem video nadzora, neprekidnog ili povremenog, sa mogućnošću čuvanja podataka.
(2) Obveznici zakona II kategorije dužni su u objektima i prostorijama u kojima se posluje gotovim novcem i drugim vrijednostima obezbijediti osnovne mjere bezbjednosti iz Člana 6, i to: protivprovalni sistem sa mogućnostima hitnog upozorenja i sistem video nadzora, neprekidnog ili povremenog, sa mogućnošću čuvanja podataka.
(3) Obveznici zakona III kategorije dužni su u objektima i prostorijama u kojima se posluje gotovim novcem i drugim vrijednostima obezbijediti osnovne mjere bezbjednosti iz Člana 6, i to: sistem video nadzora, neprekidnog ili povremenog, sa mogućnošću čuvanja podataka, te instaliranje alarma otvorenih vrata trezorskog dijela bankomata.
(4) Obveznici zakona IV kategorije dužni su u objektima i prostorijama u kojima se posluje gotovim novcem i drugim vrijednostima obezbijediti

[9] Službeni glasnik Republike Srpske, broj 85 od 11.09.2012.godine.

osnovne mjere bezbjednosti iz Člana 6, i to: protivprovalni sistem sa mogućnostima hitnog upozorenja, sistem hitnog upozorenja u vanrednim situacijama i sistem video nadzora, neprekidnog ili povremenog, sa mogućnošću čuvanja podataka.

(5) Obveznici zakona V kategorije dužni su u objektima i prostorijama u kojima se posluje gotovim novcem i drugim vrijednostima obezbijediti osnovne mjere bezbjednosti iz Člana 6, i to: sistem video nadzora, neprekidnog ili povremenog, sa mogućnošću čuvanja podataka.

PRAVILNICI PROSTEKLI IZ ZAKONA O MJERAMA BEZBJEDNOSTI U POSLOVANJU GOTOVIM NOVCEM I DRUGIM VRIJEDNOSTIMA

Članom 17. Zakona propisano je da ministar unutrašnjih poslova Republike Srpske, u roku od šest mjeseci od od stupanja na snagu Zakona donese propise o:

1) standardu i kvalitetu sredstava za primjenu osnovnih mjera bezbjednosti;
2) procjeni ugroženosti obveznika zakona;
3) transportu i prenosu gotovog novca i drugih vrijednosti.

Kao što je već u uvodu istaknuto, radi se o zakonu koji prvi put pokušava regulisati sektor bezbjednosti primjenom određenih mjera bezbjednosti kod velikog broja kategorisanih obveznika zakona. Zakonodavac je predvidio donošenje određenih pravilnika u roku od šest mjeseci od dana objavljivanja zakona u Službenom glasniku Republike Srpske, a što nije urađeno. Pravilnik o transportu i prenosu gotovog novca i drugih vrijednosti objavljen je u Službenom glasniku Republike Srpske 03.02.2016. godine sa dva mjeseca kašnjenja. Pravilnik o standardu i kvalitetu sredstava za primjenu osnovnih mjera bezbjednosti objavljen je u Službenom glasniku Republike Srpske 18.02.2016. godine sa kašnjenjem vise od dva mjeseca. Pavilnik o procjeni ugroženosti u poslovanju gotovim novcem i drugim vrijednostima objavljen je u Službenom glasniku Republike Srpske 29.12.2016. godine sa kašnjenjem od petnaest mjeseci. Problemi vezani za primjenu zakona, problemi proistekli iz nepreciznih pravilnika, u kombinaciji sa pojačanom kontrolom ministarstva unutrašnjih poslova, a koja se odnosi na primjenu zakona i pravilnika, unijeli su priličnu konfuziju kod obveznika zakona, a što se odražava i na lica koja su angažovana u procesu izrade procjene ugroženosti.

PRIMJENA U PRAKSI ZAKONA O MJERAMA BEZBJEDNOSTI U POSLOVANJU GOTOVIM NOVCEM I DRUGIM VRIJEDNOSTIMA I PRAVILNIKA DONESENIH NA OSNOVU ZAKONA

Prosto rečeno, neozbiljno shvatanje značaja Zakona od strane donosioca istog, imalo je za rezultat kašnjenje u donošenju pravilnika i do petnaest mjeseci. Takva nemarnost uticala je i na stav većine kategorisanih subjekata da izbjegnu implementaciju zakonom predviđenih osnovnih mjera bezbjednosti. Kada je neko, u ministarstvu, shvatio značaj zakona i pravilnika, kao i njihove upotrebe u praksi, sa stanovišta podizanja bezbjednosti na viši nivo preventivnim djelovanjem kod napred navedenih kategorisanih subjekata, pristupilo se kontroli tih subjekata. Utvrđeno je da gotvo svi kategorisani subjekti nemaju odgovarajuće procjene, što je rezultiralo upozorenjem policije da se isto uradi u roku koji je ostavljen. U prosjeku taj rok traje oko šezdeset dana. Aktiviranjem agencija i lica koji ispunjavaju uslove za bavljenje poslovima procjene uvidjele su se značajne manjkavosti kako u samom Zakonu, tako i u Pravilnicim. Prilikom donošenja Zakona, predlagač nije tražio mišljenje od onih koji razumiju problem i koji svakako mogu dati prijedlog rješenja problema koji se zasniva na nauci i struci, posebno na iskustvu. Treba napomenuti da predlagač Zakona i nije u obavezi da traži bilo čije mišljenje, ali imajući u vidu kompleksnost primjene Zakona, kao i njegov značaj, bilo bi korisno da su prije upućivanja Zakona u parlamentarnu procedure tražili mišljenje, prije svega naučnih radnika koji se bave ovom problemtikom. Nakon usvajanja Zakona, zakonodavac nije našao za shodno da kroz organizovanje prezentacije zakona sa istim upozna subjekte koji su kategorisani, kao i one koji treba da vode proces izrade same procjene. Sledeći propust koji se odrazio na primjenu Zakona jeste veliko kašnjenje u donošenju pravilnika kojim se uređuje način implementacije Zakona.

Subjekti koji su htjeli primijeniti zakon isto nisu učinili upravo zbog nepostojanja pravilnika koji bi konkretnije propisali šta sve obveznici zakona treba da urade. Značajne primjedbe odnose se na član 5. Zakona koji je ostao nedorečen u samoj kategorizaciji. Naime, banke su sa svojim organizacionim jedinicama svrstane u I kategoriju, a bankomati u III kategoriju. Za obe kategorije radi se posebno procjena, što je i razumljivo, ali nije jasno definisano šta se radi sa bakomatom koji nije na izdvojenoj lokaciji već je u sklopu banke. Dalje, u članu 8. Zakona, stav 3. kaže se "obveznici zakona III kategorije (bankomati) dužni su u objektima i prostorijama u kojima se posluje gotovim novcem i drugim vrijednostima obezbijediti osnovne mjere bezbjednosti…". Da li se ovo odnosi i na bankomat koji se ne nalazi u prostorijama u kojima se posluje gotovim novcem i drugim vrijednostima? Takođe, u članu 5. kategorizacijom je određeno da II kategoriji pripadaju mikrokreditne

organizacije. Članom 8. stav 2. propisano je da mikrokreditne organizacije moraju imati instaliran protivprovalni sistem i sistem video nadzora u prostoru u kome se posluje gotovim novcem i drugim vrijednostima. Većina mikrokreditnih organizacija ne posluje gotovim novcem iz čega proizilazi da im navedene mjere bezbjednosti nisu ni potrebne. Član 8. stav 2. je u koliziji sa članom 3. Zakona u kome je jasno rečeno da su mikrokreditne organizacije obveznici Zakona, ne navodi se da li posluju gotovim novcem ili ne. Sledeća nejasnoća samoga Zakona koja znatno utiče na rad procjenitelja jeste član 5. stav 5. Zakona u kome se kaže da su obveznici zakona "pravna i fizička lica koja posluju gotovim novcem i ostvaruju dnevni promet gotovog novca u iznosu većem od 5.000 konvertibilnih maraca". Niti zakonom, niti pravilnikom nije navedeno na koji vremenski period se odnosi ovaj novčani iznos. Zakonom je propisano da obveznik može primijeniti i niži stepen mjera bezbjednosti ako se aktom o procjeni ugroženosti utvrdi manji stepen ugroženosti pojedinih objekata i prostorija. Šta će se desiti ako je obveznik već primijenio obavezne mjere bezbjednosti, a procjena utvrdila manji stepen ugroženosti? Da li to znači da obvezniku Zakona uopšte nisu potrebne mjere zaštite?

Pravilnik o procjeni ugroženosti u poslovanju gotovim novcem i drugim vrijednostima usvojen 29.12.2016. godine samo je dodatno produbio ranije nedoumice proistekle iz Zakona i stvorio nove. Propisanih šest kategorija zaštite, kao i data metodologija kvantifikacije sa tabelom proračuna primjenjiva je na obveznike zakona I kategorije, dok je kod većine ostalih kategorija to skoro neizvodivo. Radi lakšeg shvatanja iznosimo primjer:

Bankomat je zakonom kategorisan u III kategoriju primjene obaveznih mjera zaštite. Ukoliko kvantifikacijom dođemo do broja 55 i više, automatski se govori o vrlo visokom riziku, koji između ostalog u članu 17. pravilnika za takav kvantifikator zahtijeva "fizičku zaštitu s najmanje jednim nadzornim mjestom i sistemom veza sa pripadnicima fizičkog obezbjeđenja na objektu koji se obezbeđuje"[10]. Ovakva kvantifikacija negira član 8. zakona u kojem se kaže da bankomat mora imati neprekidan video nadzor i alarm otvorenih vrata trezorskog dijela bankomata.

Pravilnikom je određeno da kvantifikator procjene čini parameter ugrožavanja (deset faktora) i parameter bezbjednosti (deset faktora). Izostanak bilo koga faktora daje neispravan kvantifikator procjene, odnosno stepen ugroženosti, odnosno pogrešne mjere zaštite. Radi lakšeg shvatanja iznosim primjer:

Mikrokreditne organizacije su zakonom kategorisane u drugu kategoriju, bez obzira da li posluju gotovim novcem ili ne. Propisana metodologija je neprimjenjiva na iste, što u konačnom može dovesti do

[10] Pravilnik objavljen u Službenom glasniku Republike Srpske broj 115, 29.12.2016.godine

pogrešne preporuke o primjeni mjera zaštite. Jedan od faktora ugroženosti (U7) traži odgovore na pitanja o broju radnih mjesta na kojima se posluje sa gotovim novcem i način čuvanja tog novca. U ponuđenim odgovorima nema ocjena kojom bi se moglo reći da se u objektu ne posluje gotovim novcem. Prema tome, ovaj faktor se preskače, i automatski se dobija ocjena koja nije potpuno prihvatljiva.

Ovih primjera nelogičnosti u primjeni Zakona i Pravilnika je vise, bitna je suština koja se odnosi na otežanu primjenu Zakona i Pravilnika u praksi. Naročito su u nezavidnom položaju procjenitelji, koji su nerijetko izloženi pritisku da svjesno i namjerno tumače pojedine odredbe Zakona i Pravilnika, a sve u cilju davanja ocjene i preporuke koja će predložiti niži stepen zaštite, odnosno zaštitu koja ne zahtijeva značajnija materijalna ulaganja u ista od strane obveznika Zakona.

PRIMJENA ZAKONA O BEZBJEDNOSTI KRITIČNE INFRASTRUKTURE U REPUBLICI SRPSKOJ

Iskustava u Republici Srpskoj o primjeni Zakona o bezbjednosti kritične infrastrukture nema, jer se Zakon još uvijek ne sprovodi. Izostala je izrada Metodologije koja bi dovela do određenih zaključaka. Bez obzira što su uloženi napori da se dođe do kvalitetnog zakonskog rješenja, koje je definisalo sektore iz kojih se identifikuje kritična infrastruktura (član 3. Zakona), izostala je izrada Metodologije za procjenu rizika koja predstavlja polaznu osnovu za sve druge aktivnosti. Ne ulazeći u razloge kašnjenja izrade metodologije, a samim tim i prvih iskustava, nužno je da se oslonimo na sredine koje već godinama proučavaju i usavršavaju metodologiju procjene rizika i zaštite kritične infrastrukture. Naravno, država koja prednjači u ovim aktivnostima je Republika Srbija. Znajući da se usvojeni zakon u Republici Srpskoj, ne razlikuje znatno od zakona u Republici Srbiji, samim tim i poređenje ima veći značaj.

MOGUĆNOSTI PRIVATNOG SEKTORA BEZBJEDNOSTI U PRIMJENI ZAKONA O BEZBJEDNOSTI KRITIČNE INFRASTUKTURE

Sprovođenje mjera savremene bezbjednosti više nije isključivi ekskluzivitet države, kao vrhovnog autoriteta, već je sve više predmet interesovanja i angažovanja privatne bezbjednosti. Karakteristike savremenih bezbjednosnih izazova, rizika i prijetnji su takve da je sasvim logično da privatna bezbjednost učestvuje u zaštiti vrijednosti kritične infrastrukture, kroz

odnose poznate kao javno-privatno partnerstvo. Država preko kontrolnog aparata zadržava poziciju autoriteta koji u konačnom i odgovara za ukupan kvalitet bezbjednosnog okruženja.

Iskustvo u dosadašnjem radu nam, na žalost, pokazuje da je kontrolni aparat potpuno ili djelimično zakazao u kontroli primjene zakona, što je ostavilo prostora različitim pojedincima da nestručnim radom omalovažavaju i struku i nauku. Posljedica toga je odustajanje klijenata od primjene obaveza koje je zakon kao takve predvidio. Takvo "razvodnjavanje" zakona, koje je direktna posljedica njegove primjene od strane nestručnih i nekvalifikovanih kadrova, kao i izostanka inspekcijskog nadzora nad primjenom zakona od strane ministarstva je dovelo do stanja u kome će zakon i prije same primjene biti vjerovatno proglašen nedorečenim, nepotpunim odnosno odložiće se njegova primjena "do daljnjeg".

Usvojeni Zakon nije jasno definisao mjesto i ulogu privatnog sektora bezbjednosti u samoj primjeni Metodologije za procjenu rizika kritične infrastructure. Uzroci takvom stavu predlagača zakona mogu se naći u nespremnosti javnog sektora da prihvati pomoć i saradnju privatnog sektora bezbjednosti, bez obzira na iskustvo koje privatna bezbjednost ima u sprovođenu mjera fizičke i tehničke zaštite.[11] Pri tome, u Zakonu se eksciplitno kaže da ministarstva mogu tražiti pomoć strukovnih udruženja kod primjene pojedinih odredbi zakona. Na ovom mjestu nije jasno definisano šta su to strukovna udruženja, i šta podrazumijeva njihova pomoć.

Nespremnost javnog sektora da privatni sektor prihvati kao realnost, i kao značajan subjekt u ostvarivanju sistema bezbjednosti je posljedica izostanka saradnje upravo od strane državnih organa. Odnosno, državni organ je još uvijek "zarobljen" u prošlom vremenu i socijalističkom shvatanju organizovanja sistema bezbjednosti koji ne poznaje privatnu bezbjednost.[12] Iluzorno je jedan takav subjekt zanemariti u ostvarivanjuju zaštite kritične infrastrukture. Primjer kvaltetne saradnje u zaštiti kritične infrastrukture treba da nam budu zemlje Evropske unije u kojima je nezamisliva zaštita objekata kritične infrastrukture bez privatne bezbjednosti. Ako je naše zvanično opredjeljenje članstvo u Evropskoj uniji zbog čega onda bježimo od definisanja

[11] Ilustracije radi, ističemo kompaniju Sector Security koja je za dvadeset godina rada izvršila veliki broj fizičkih i tehničkih obezbjeđenja objekata i prostora koji po svojoj namjeni sigurno pripadaju kritičnoj infrastrukturi. Primjera radi navodimo tehničko obezbjeđenje graničnih prelaza BiH, tehničko obezbjeđenje UKC Banja Luka, tehničko obezbjeđenje saobraćajne infrastrukture u opštini Prnjavor, tehničko obezbjeđenje RITE Gacko i RITE Ugljevik, fizičko i tehničko obezbjeđenje najveće željezare u ovom dijelu Evrope Arcellor Mital Zenica i dr. Više vidjeti na: www.sectorsecurity.org

[12] Kompanija Sector Security, u svom radu, na poslovima fizičko-tehničke zaštite angažuje svakodnevno oko 1200 radnika i značajan broj naoružanih radnika, što je stavlja na treće mjesto subjekata bezbjednosti, odmah iza oružanih snaga i policije.

mjesta i uloge privatne bezbjednosti u zaštiti kritične infrastrukture? Moguća su dva odgovora: animozitet prema privatnoj bezbjednosti, ili nepoznavanje savremenih tokova obezbjeđenja kritične infrastrukture.

Na temelju iskustva, potpuno odgovorno se može reći, da ovaj trenutak u Republici Srpskoj, mjere zaštite može sprovesti privatni sektor bezbjednosti, odnosno kompanija Sector Security, koja je, kao što je napomenuto svoj rad dokazala radom za preko pet hiljada zadovoljnih klijenata. Kako bi se izbjegla bilo kakva pristrasnost ili stvaranje monopola nad primjenom mjera, svaka aktivnost mora biti javna, transparentna, zasnovana na jasnim i provjerljivim čeinjenica. Naročito kod kritične infrastrukture za čiju bezbjednsot je odgovorna država. Na taj način će se izbjeći zloupotrebe Zakona na tržištu ponude i potražnje, koje su prisutne u primjeni Zakona o procjeni ugroženosti u poslovanju gotovim novcem i drugim vrijednostima.

Da će privatna bezbjednost biti glavni akter u primjeni mjera zaštite kritične infrastrukture vidimo u nekoliko nepobitnih činjenica:

- angažovanje privatne bezbjednosti u zaštiti objekata kritične infrastrukture u Evropskoj Uniji;
- ministarstvo unutrašnjih poslova ne raspolaže dovoljnim kapacitetima da zaštiti sve objekte, iz razloga što je njegovo brojno stanje ograničeno Dejtonskim mirovnim sporazumom;
- odgovorno lice kritične infrastrukture neće se odlučiti za organizovanje vlastite službe fizičko tehničke zaštite jer mu je takav vid angažovanja radnika preskup, ekonomski neopravdan;
- sektor privatne bezbjednosti ima iskustvo i resurse da odgovori izazovu zaštite kritične infrastrukture;

Privatni sektor bezbjednosti u Republici Srpskoj je pokazao, kroz niz svojih aktivnosti, da može biti, i da jeste, kvalitetan partner Vladinom sektoru u zaštiti objekata visokog stepena rizika. To se pokazalo kroz fizičko i tehničko obezbjeđenje finansijskih ustanova, koje su stub razvoja svakog društva, pa tako i našega. Iskustvo kompanije Sector Security, koja je lider u obezbjeđenju finansijskih ustanova, je pokazalo da je moguće ovladati poslovima zaštite objekata finansijskih ustanova koje jesu objekti kritične infrastrukture. Stečeno iskustvo ovoj kompaniji daje legitimno pravo da se nametne kao lider u obezbjeđenju objekata kritične infrastrukture koji su definisani Zakonom o bezbjednosti kritične infrastrukture. Da bi privatni sektor spreman dočekao primjenu Zakona mora mnogo više uložiti u odabir i obuku kadrova koji će biti nosioci odgovora na izazove zaštite objekata kritične infrastrukture. Privatne kompanije u ovoj javno-privatnoj saradnji mogu se ministarstvima nametnuti u sljedećem:

- učestvovanje u procesu identifikacije nekih rizika;
- učestvovanje u procesu identifikacije nekih mjera odgovara na rizike;

- učestvovanje u neposrednom odgovoru na neke rizike fizičko - tehničkim aktivnostima.

Kroz zakon se jasno provlači i njegova osnovna teza da se teži ka stvaranju bezbjednosnog ambijenta u kome će maksimalno biti zaštićena materijalna dobra, životi ljudi i životna sredina. Odnosno žele se izbjeći:

- posljedice po život i tijelo, smrt, ranjavanje ili povrijeđivanje;
- trajni gubitak ili oštećenje materijalno - tehničkih sredstava;
- zagađenje životne sredine;
- narušavanje ugleda poslovnog subjekta;
- gubitak dozvole za rad;
- gubitak radnih mjesta i drugo.

Rad na spriječavanju pobrojanog za privatni sektor bezbjednosti nije ništa novo, jer ovo su svakodnevni poslovi ovoga sektora.

ZAKLJUČAK

Usvojeni Zakoni su svojim sadržajem pokazali da je privatno - javno partnerstvo neminovnost koja se kao takva mora prihvatiti. Države koje su tako i nastupile u mnogome su poboljšale kvalitet života svojih građana. Tromost u primjeni Zakona, kao i inspekcijskog nadzora nad primjenom Zakona jasno pokazuje da se mi kao društvo još uvijek nalazimo u nekom prošlom vremenu u kome se "neko stara o našoj bezbjednosti". Ovo samo pokazuje da smo mi nespremni da prihvatimo sve prednosti koje privatni sektor bezbjednosti daje prilikom preuzimanja poslova koji su bili u nadležnosti državnih organa.

Ukoliko počnemo, što prije, sa aktivnom primjenom usvojenih Zakona utoliko ćemo biti spremniji da izvršimo kvalitetne analize, da usavršimo Zakone i osnažimo saradnju javno - privatnog sektora u oblasti bezbjednosti i zaštite objekata kritične infrastrukture. Da bi to postigli neophodno je da se oslobodimo ranije prihvaćene državne nedodirljivosti, nepriznavanja privatne imovine i vrijednosti privatnog sektora bezbjednosti.

LITERATURA

1. Zorić Z, (2019). "Cooperation between the private and public security in order to realise security system", V International scientific and professional conference security and crises management - theory and practice – safety for the future. SeCMan2019. Beograd
2. Grbić N. Kosić, D. Pavlović, G. Zorić Ž. (2021). *Zaštita kritične infrastrukture – evropski standardi i domaće zakonodavstvo. Zbornik radova: Prevencija katastrofa, zaštita i spasavanje u vanrednim*

situacijama: Regionalna asocijacija za bezbjednost i krizni menadžment, S4 GloSee Globalna bezbjednost doo, Bezbjednosi istraživački centar. Beograd.
3. Kosić, D. Pavlović G. (2021). *Obaveza zaštite kritične energetske infrastrukture prema evropskim direktivama.* Zbornik radova: Istočna ili južna interkonekcija - politika ili ekonomija: Centar za lobiranje Banja Luka. *Banja Luka.*
4. *Zakon o mjerama bezbjednosti u poslovanju gotovim novcem i drugim vrijednostima,* Službeni glasnik Republike Srpske, broj 33, 30.04.2015.godine
5. *Pravilnik o uslovima i načinu sprovođenja tehničkog i fizičkog obezbjeđenja,* Službeni glasnik Republike Srpske, broj 85, 11.09.2012.godine
6. *Pravilnik o transportu i prenosu gotovog novca i drugih vrijednosti,* Službeni glasnik Republike Srpske, broj 6, 03.02.2016.godine
7. *Pravilnik o standardu i kvalitetu sredstava za primjenu osnovnih mjera bezbjednosti,* Službeni glasnik Republike Srpske, broj 12, 18.02.2016.godine
8. *Pravilnik o procjeni ugroženosti u poslovanju gotovim novcem i drugim vrijednostima,* Službeni glasnik Republike Srpske, broj 115, 29.12.2016.
9. *BAS ISO 31000:2016,* Institut za standardizaciju Bosne i Hercegovine. Više na: http://www.bas.gov.ba/standard/

NETWORKING OF THE LAW ON SECURITY MEASURES IN CASH AND OTHER VALUE OPERATIONS WITH THE LAW ON CRITICAL INFRASTRUCTURE SECURITY IN THE REPUBLIC OF SRPSKA

Dr Željko Zorić[13]
Mr Dragana Kosić[14]

Abstract: Driven by the need to raise security to a higher level, especially in the sector in which cash and other valuables are traded, the National Assembly of the Republic of Srpska adopted the Law on Security Measures in Cash and Other Valuables in 2015. The basis for the adoption of the Law on Security Measures in Cash and Other Values was found in the international standard ISO 31000 which defines the principles and general

[13] Sector Security, Director of the Physical Security Sector, e-mail: zeljko.zoric@sectorsecurity.org
[14] Sector Security, General Manager, e-mail: dragana.kosic@sectorsecurity.org

guidelines for risk management, thus creating a legal framework that will enable effective application of basic security measures in cash and other values, and contribute to reducing risks and protecting employees from committing crimes and misdemeanors that violate the security of persons and property. Frequent crises, accompanied by inevitable damage, as well as the need to harmonize security flows with international practice, influenced the adoption of the Law on Critical Infrastructure Security in 2019, which should lead to a level of security that will affect crisis prevention. The paper will analyze the practical application of the Law on Security Measures in Business with Cash and Other Values. The role and importance of the private security sector in the application of the mentioned laws will be presented, i.e. the importance of private-public partnership in the realization of the security system.

Keywords: vulnerability assessment, protection measures, physical and technical security, critical infrastructure

Прегледни рад

ПОСЉЕДИЦЕ УГРОЖАВАЊА КРИТИЧНЕ ИНФРАСТРУКТУРЕ ПО НАЦИОНАЛНУ БЕЗБЈЕДНОСТ: ФАКТОР ЗА ИЗГРАДЊУ ПРАВНИХ И ИНСТИТУЦИОНАЛНИХ КАПАЦИТЕТА

Милица Сикимић[1], ма

Апстракт: У лансираном програму Европске уније за заштиту критичне инфраструктуре представљени су захтјеви и дате смјернице за заштиту европских критичних инфраструктура, те достизање и очување безбједности на нивоу заједнице. Према тим смјерницама примарна и коначна одговорност за безбједност критичне инфраструктуре адресира се на државе чланице, њихову националну легислативу и власнике/оператере критичних инфраструктура. Приликом спровођења заштите на националном нивоу државе треба да заузму приступ којим се у обзир узимају сви извори угрожавања и све опасности, те да активно подстичу укључивање приватног сектора у циљу успостављања јединственог система заштите. Критична инфраструктура је разврстана по секторима и сагледава се кроз националне вриједности попут привреде и енергетике, економске стабилности и социјалног просперитета, националних информационих ресурса, здраве животне средине и сл. У вези са наведеним вриједностима државе имају различите националне интересе на основу којих постављају циљеве и задатке националне безбједносне политике те успостављају национални систем безбједности. Стога је циљ овог рада истражити посљедице дисфункционалности критичне инфраструктуре које наступају на територији и у административном апарату једне државе. Посљедице су један од фактора који се разматрају приликом доношења одлука о издвајању средстава и капацитета за успостављање националног система за заштиту критичне инфраструктуре. У доступној литератури о концепту критичне инфраструктуре и њене заштите најчешће се истиче повезаност, међузависност и преливајући ефекат угрожене критичне инфраструктуре - наднационални значај јединствене заштите. Међутим, постоји одређена празнина о посљедицама прекида у раду критичних инфраструктурних постројења, система и мрежа које имају првенствен и незаобилазан ефекат на стање националне безбједности. У раду ће бити представљени резултати истраживања о

[1] Асистент на Факултету безбједносних наука Универзитета у Бањој Луци и докторанд на Обуда универзитету у Будимпешти. E-mail: milica.sikimic@fbn.unibl.org

посљедицама угрожавања критичне инфраструктуре које се односе на људске и економске губитке једне земље, дисфункционалност система владиног и невладиног сектора, као и прекиде у раду комплетног административног апарата.

Кључне ријечи: критична инфраструктура, обавезе државе, безбједност, угрожавање, директна штета, индиректна штета.

УВОД

Безбједносна политика Европске уније усмјерена је на једнаке стандарде заштите вриједности и интереса заједнице у свим земљама чланицама и земљама кандидатима за чланство. Конкретна дешавања на плану развоја европског програма за заштиту критичне инфраструктуре уочавају се 2004. године.[2] Централно мјесто у развоју безбједносног оквира заузима *Директива Савјета Европе 2008/114/ЕК о утврђивању и означавању европске критичне инфраструктуре и процјени потребе побољшања њене заштит*е (Директива 2008/114/ЕК) из 2008. године која садржи смјернице за одређивање *европске критичне инфраструктуре* и операционализацију постављеног стратешког европског оквира.[3] Упркос томе што Директива 2008/114/ЕК даје смјернице за заштиту европске критичне инфраструктуре и тежи унитарности, примарна и коначна одговорност за безбједност инфраструктуре адресира се на државе чланице појединачно, њихову националну легислативу и власнике/оператере критичних инфраструктура.[4]

Достизање европских стандарда у области критичне инфраструктуре је једно од отворених питања са којима се суочавају субјекти националних система безбједности приликом идентификовања

[2] EVALUATION of COUNCIL DIRECTIVE 2008/114 ON THE IDENTIFICATION AND DESIGNATION. European Commission, Brussels, 2019; Critical Infrastructure Protection in the fight against terrorism . Commission of the European Communities, European Council, Brussels, 2004.Green Paper on a European Programme for Critical Infrastructure Protection. Commission of the European Communities, Brussels, 2005; REVIEW OF THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION. European Commission, Brussels, 2012.

[3] COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union L 345/75, Brussels, 2008.

[4] Poustourli, A.: A Concise Survey of Security Standards and Certification Services. 13th INTERNATIONAL CONFERENCE "STANDARDIZATION, PROTYPES AND QUALITY: A MEANS OF BALKAN COUNTRIES COLLABORATION," Brasov, Romania, 2016, pp 230-246.

националне критичне инфраструктуре и успостављања система њене заштите.[5] Тек након рјешења овог питања долази до одређења европских критичних инфраструктура и то из реда националне критичне инфраструктуре.[6] Иако Босна и Херцеговина још увијек није чланица Европске уније, у Републици Српској је препозната потреба за суочавањем са изазовима на европском путу. У току је рад на имплементацији законског оквира и достизању европских безбједносних стандарда у заштити критичне инфраструктуре и националне безбједности Републике Српске. За националну контакт тачку за заштиту критичне инфраструктуре одређено је Министарство унутрашњих послова Републике Српске, а легислатива даље налаже анализу ризика, израду безбједносних планова и именовање безбједносних координатора за сваки сектор критичне инфраструткуре. Међутим, законодавство Републике Српске не познаје европску критичну инфраструктуру што је централна одредница европског програма за заштиту критичне инфраструктуре. [7]

Држава прокламује националне вриједности од виталног значаја и гарантује их својим правним поретком. Неке од националних и државних вриједности су здрава животна средина, енергетска стабилност, економски и социјални просперитет, информациони ресурси, права и безбједност грађана и друштвених група итд. Области из којих се одређује критична инфраструктура су прилично широко постављене и у њима су садржане националне вриједности попут националних информационих ресурса, националне привреде и енергетике, финансија и банкарства, здравства, саобраћаја и транспорта, васпитања и образовања, културних и природних добара.[8] Када је угрожена критична инфраструктура шире се негативни утицаји на унутрашњу и спољну безбједност, здравље и животе људи, имовину и животну средину и најзад, угрожена је национална безбједност. Посљедице угрожавања критичне инфраструктуре могу бити људски и/или економски губици, као и прекид у раду комплетног административног апарата. Зато државни органи законодавне и извршне

[5] Lazari, A., & Simoncini, M.: Critical Infrastructure Protection beyond Compliance. An Analysis of National Variations in the Implementation of Directive 114/08/EC. Global Jurist 3 (16), 2016, pp 267–289; Keković, Z., Ninković, V.: *Zaštita kritične infrastrukture – sistemski pristup*. Centar za analizu i upravljanje krizama, Beograd, 2020.

[6] Трбојевић, М.: Заштита критичних инфраструктура - искуства транзиционих земаља. Политичка ревија, 2018, стр. 99-118.

[7] Сикимич, М.: Современные вызовы безопасности национальной критической инфраструктуры в Республике Сербской. Материалы VII Международной научно-практической конференции *Актуальные проблемы безопасности жизнедеятельности*, Москва, фебраль, 2021.

[8] 1Комарчевић, М.: Увод у критичну инфраструктуру. Академска мисао, Београд, 2018.; Сикимић, исто.

власти именују субјекте одговорне за заштиту критичне инфраструктуре који чине један од подсистема у националном систему безбједности.[9]

Национална безбједност је и даље централни концепт, а држава основни провајдер безбједности. Суверена власт, територија и становништво су конститутивни елементи сваке државе. Национални идентитети и бреме међунационалних сукоба из прошлости упућују на то да ће тежња за националном државом (подударање географског простирања државе и нације) још дуго бити тренд и реалност Европе, упркос све снажнијем процесу глобализације.[10] Одсуство националних институционалних механизама и правне регулативе може имати деструктивне ефекте по безбједност читаве планете, али функционисање критичне инфраструктуре првенствено има утицај на националну безбједност. Циљ овог рада је предочавање могућих посљедица прекида у раду критичне инфраструктуре које наступају на територији и у административном апарату једне државе, односно имају негативне ефекте првенствено по националну безбједност. Структура рада заснована је на законској регулативи Републике Српске.[11] Тачније, посљедице прекида у раду критичне инфраструктуре елаборирane су као потенцијална директна и/или индиректна штета.

ДИРЕКТНА ШТЕТА КАО ПОСЉЕДИЦА ПРЕКИДА У РАДУ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Законом о безбједности критичних инфраструктура Републике Српске прописано је да се анализом ризика свих критичних инфраструктура, као директна штета, процјењује сљедеће:

- људски губици;
- економски губици и
- утицај на јавност.[12]

[9] Сикимић, М.: *Критична инфраструктура као одредница националне безбедности – мастер рад*. Криминалиситчко-полицијски универзитет, Београд, 2021.

[10] Мијалковић, С.: *Национална безбедност*. Криминалистичко-полицијска академија, Београд, 2015.

[11] Закон о безбједности критичних инфраструктура Републике Српске, Службени Гласник број 58/19.

[12] Исто, члан 9.

Људски губици

Могући број смртно страдалих или повријеђених лица сматра се директном штетом у разматрању могућих сценарија пријетњи, односно прекида у раду поједине критичне инфраструктуре.[13] Примјери који илуструју везу између критичне инфраструктуре и посљедица по живот и тијело човјека могу се пронаћи у различитим секторима.

Концепт националне безбједности детерминише опстанак државе и друштва који је услов за достизање, развој и уживање осталих вриједности. Три димензије опстанка су: опстанак државе, национални опстанак и физичко самоодржање. Под опстанком државе подразумијева се, најкраће речено, опстанак суверене политичке заједнице која се својим идентитетом разликује од истоврсних творевина у међународном систему. Национални опстанак значи опстанак националне свијести и националног идентитета људских колектива.[14] У контексту људских губитака најзначајнија је трећа димензија опстанка државе и друштва - физичко самоодржање које се односи на физичко преживљавање људи. Постојаност становништва, односно стална настањеност људи на једној територији је услов постојања државе.[15]

Неопходно је да се националне мјере за заштиту критичне инфраструктуре усмјеравају према ризицима и пријетњама у оним критичним секторима гдје се посљедице огледају у броју смртно страдалих лица. Црне статистике земаља у окружењу показују да је највећи број живота изгубљен у саобраћају. Проблеми и застоји у раду путне инфраструкутре узрокују саобраћајне незгоде које за посљедицу имају тјелесне повреде или смрт лица. Даље, објекти који нису изграђени у складу са грађевинским стандардима лако се урушавају приликом земљотреса што проузрокује велике материјалне и људске губитке. [16]

Економски губици

У извјештају Свјетског економског форума „Глобални ризици 2020. године“ квар на критичној инфраструктури смјештен је у област економских ризика са потенцијално највећим ефектима на глобалну

[13] Исто.
[14] Мијалковић, 2015, исто.
[15] Исто.
[16] Опширније у: Mijalković, S., & Cvetković, V.: Vulnerability of Critical Infrastructure by Natural Disasters. *National Critical Infrastructure Protection - Regional Perspective Ljubljana - Belgrade*: Institut for Corporative Security Studies, 2013, pp 91-102.

ситуацију.[17] Ефекти ове врсте процјењују се према важности економског губитка или смањења квалитета производа или услуга.

Стање националне безбједности одређује квалитет живота који се између осталог односи на услове живота и степен економског развоја. Животни услови обухватају личну и колективну потрошњу, односно појединачно трошење материјалних добара којим се обезбјеђује материјална егзистенција људи и заједничко коришћење услуга које пружају бројне институције.[18] Квалитет живота укључује низ економских и многих других фактора који људима доносе задовољство у материјалном и у духовном смислу. Материјалне ствари су људима важне када их имају, док им је новац далеко важнији када га немају. Новац пресудно утиче на животе људи у сваком погледу, ствара им финансијске бриге и када га имају и када га немају. „Можда се и читав живот може преживјети без квалитета, али тешко да може без новца.“[19]

Критична инфраструктура из сектора банкарства и финансија обухвата производњу националне валуте, системе пласирања новца, системе осигурања, банкарско пословање, електронско банкарство и друге услуге. Носећи стуб националног финансијског система представљају банке које имају важну улогу у економији сваке државе. Угроженост берзе, инвестиција, система плаћања и клијената банке може довести до нестабилности банкарског система и нестабилне националне валуте.[20] Нестабилна национална валута угрожава финансијску моћ, тј. једну од више видова моћи које заједно чине моћ државе. Националну безбједност умногоме детерминишу потенцијал и моћ државе. Богате државе су војно, технолошки и културно моћне и утицајне у међународним односима.[21]

Утицај на јавност

У корпусу критичних инфраструктурних сектора своје мјесто пронашао је и сектор за информационо-комуникациону инфраструктуру, односно електронске комуникације, пренос података, информациони системи, пружање аудио, и аудио и видео медијских услуга.[22] Директна

[17] *Global Risks Report,* World Economic Forum, Davos, 2020.

[18] Мијалковић, исто.

[19] Luburić, R., & Fabris, N: Money and the Quality of Life. *Journal of Central Banking Theory and Practice*, 2017, pp 17-34.

[20] Žiravac Mladenović, M.: Razlozi i interesi za regulaciju banaka. *Međunarodna konferenciji o društvenom i tehnološkom razvoju STED 2013*. Univerzitet za poslovni inženjering i menadžment, Banjaluka, 2013.

[21] Мијалковић, 2015, исто.

[22] Закон о безбједности критичних инфраструктура Републике Српске, Службени Гласник број 58/19.

штета по критичну инфраструктуру у контексту јавности процјењује се према утицају на повјерење јавности, физичке патње и нарушавање свакодневног живота, укључујући и губитак основних, те јавних услуга.[23]

Овдје елаборирамо негативни утицај по националну безбједност са акцентом на садржаје медијских извјештавања, док ће у другом дијелу рада бити више ријечи о посљедицама прекида у раду самих мрежа и система комуникације и информисања.

Савремени организациони и технолошки облици информисања, националне и мултинационалне телевизијске мреже и радио станице, као и новинске агенције врше информисање јавности о важним догађајима из свих области људске дјелатности и интересовања. То су обично информације о најважнијим политичким питањима, о функционисању институција система, међународне заједнице и међународних организација, али и из области културе, спорта, привреде, научног и технолошког развоја итд. У одређеном броју извјештавања ради се о вјеродостојним чињеницама које су обрађене на стучан и професионалан начин, поготово уколико су плод тзв. истраживачког новинарства.[24] Садржаји који се пласирају путем медија утичу на људе у смислу начина на који размишљају, перцепције важних друштвених проблема и начина на који додјељују одговорност за политичке проблеме.[25]

Формирање ставова о националним вриједностима и интересима под великим је утицајем медија, нарочито уколико се има у виду то да се о одлукама носилаца државне власти грађани у највећој мјери информишу преко медија. Медији се стога често називају и *четвртом граном власти* или *седмом свјетском силом*.

Усљед свега наведеног јасно је да треба обезбиједити несметано функционисање информационог сектора, обезбиједити проток информација, односно онемогућити пласирање непровјерних и нетачних информација које негативно утичу на националну безбједност. Као примјер таквих инфорација можемо навести нетачна информисања о корупцији у органима управе, нетачне наводе о криминалним активности државника или нефункционисању државног апарата. Поред тога, у контексту очувања нације, националног идентитета, националног поноса и достојанства јако је битно водити рачуна о медијским садржајима за младе. Ради се о указивању на језик, религију, културу и начин живота као примарне друштвене вриједности које могу бити угрожене, а у уској су

[23] Исто.

[24] Мијалковић, С., & Милошевић, М: *Обавјештајно-безбедносна делатност и службе*. Висока школа унутрашњих послова, Бањалука, 2011.

[25] Sokolović, H: *Uticaj medija na formiranje političkih stavova i vrijednosti*. Filozofski fakultet Univerziteta u Sarajevu, Sarajevo, 2018.

корелацији са безбједношћу државе и нације. Референтни објекат социјеталне безбједности је колективни идентитет који се поред родног, сексуалног и вјерског идентитета у првом реду односи на национални индентитет. У нераскидивој вези су оданост и осјећај припадности појединца држави и њезиним конститутивним групама.[26]

Јењавање осјећања припадности држави или нацији и губитак повјерења у националне институције најчешће се подстиче и постиже пласирањем пажљиво одабраних медијских садржаја. Уколико критична инфраструктура у овој области није адекватно заштићена и уколико дође до прекида у контроли квалитета пласираних информација може доћи и до нарушавања безбједности у већем обиму, насилних преврата, угрожености националног јединства и политичке стабилности и најзад, доводи се у питање опстанак државе и друштва.

ИНДИРЕКТНА ШТЕТА КАО ПОСЉЕДИЦА ПРЕКИДА У РАДУ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Анализом ризика свих критичних инфраструктура, као индиректна штета, процјењује се:

- дугорочан утицај на интегритет појединаца и заједнице;
- дугорочна економска штета и
- дугорочан утицај на квалитет животне средине.[27]

Дугорочан утицај на остваривање људских права и слобода

Људска права и слободе су обавезан супстрат устава и правног поретка демократских друштава и представљају националне и државне вриједности.[28] Ниво развијености неког друштва одређујемо, између осталог и према томе колики је степен заштите слобода и права грађана.[29]

Основно људско право је право на живот, а поред тога нека од људских права на којима се једноставно и јасно може илустровати повезаност са заштитом критичне инфраструктуре су: право на здравствену заштиту, право на социјалну заштиту, тајност писама и других средстава општења, заштита података о личности, слобода медија,

[26] Ћеранић, П.: *Безбједносна политика - прилике у Босни и Херцеговини*. Факултет безбједносних наука, Бањалука, 2020.
[27] Закон о безбједности критичних инфраструктура Републике Српске, Службени Гласник број 58/19, члан 9.
[28] Мијалковић, 2015, исто.
[29] Ђорђевић, исто.

право на правну помоћ. Уколико је угрожена здравствена критична инфрастурктура (нпр., производња, транспорт и надзор над лијековима, неадекватан систем вакцинације и имунизације), долази до застоја у пружању здравствене заштите грађанима и угрожено је здравље становништва. Безбједност здравља се одражава на природни прираштај, стопу фертилитета, очекивану дужину живота[30] и посљедично угрожено је основно људско право – право на живот. Напади на информационе и комуникационе инфраструктуре воде до угрожавања права на тајност писама и других средстава општења. Сајбер напади могу довести и до јавног објављивања заштићених података о личности.

Уколико прекиди у раду критичне инфраструктуре потрају или се понављају долази до дугорочног утицаја на интегритет појединца и заједнице.

Дугорочан утицај на квалитет животне средине

Посљедице угрожавања критичне инфраструктуре процјењују се према важности и транспарентности података о системима и опасностима које могу битно утицати на квалитет животне средине.[31] Квалитативна анализа стања животног окружења обухвата процјену квалитета ваздуха, воде, земљишта и стање биодиверзитета.[32] У погледу подјеле на секторе ријеч је у првом реду о критичним секторима за водопривреду, храну и пиће, комуналне дјелатности, културна и природна добра.

Најзначајнији извор загађења ваздуха је индустријска активност, а након тога моторна возила и гријање. У заштити животне средине врло је важно да се утврде сви извори загађења и да се направи катастар загађивача. Након тога се контролом утврђује прекорачење емисије загађујућих материја[33] и предузимају неопходне мјере.

Један од највећих проблема савремене цивилизације постаје проблем квалитета воде за пиће.[34] Посљедице „неисправне“ воде за пиће често се не могу ограничити само на дио популације који конзумира ту воду. Заразне болести које се јављају након кориштења загађене воде

[30] Исто.

[31] Poljanšek, K., Marin Ferer, M., De Groeve, T., & Clark, I.: Science for disaster risk management 2017: knowing better and losing less. *Publications Office of the European Union*, Luxembourg, 2017.

[32] Ђорђевић, исто

[33] Исто.

[34] Милашиновић, М.: Међународна сарадња и смањење ризика од елементарних непогода. *Безбедност* 3, 2019, стр. 200-219.

често попримају епидемијске размјере и на тај начин посљедице обухватају чак и становнике који користе исправну воду.[35]

Услов за здравље људи је и квалитетно обрадиво земљиште које даје квалитетнију и јефтинију храну уз мање трошење енергије и вјештачких ђубрива и омогућава прехрану становништва. Проценти обрадивог земљишта се смањују како усљед ерозија изазваних активностима људи, тако и оним које су настале као посљедица природних процеса. Додатно, земљиште које стално плави може да буде посљедица незаинтересованости или неспособности државних структура да адекватно заштите стратешке интересе грађана.[36]

Очување разноврсности биљног и животињског свијета представља наслеђе потомству. У том контексту однос према природи као животном станишту и наслеђу за будућност показује колико су институције у функцији интереса грађана и колико је заправо одређена заједница зрела по питању очувања биодиверзитета и природних добара.[37]

Здрава животна средина није омеђена државним границама и посљедице њеног угрожавања могу да поприме континенталне и глобалне размјере. Повезана је са националном, међународном и глобалном политиком и безбједношћу, што је чини битним изазовом међународних односа. Поред тога „здрава животна средина је значајна за живот и здравље човјека, исхрану, ментални и физички развој, привредну дјелатност, креативност и самоафирмацију, стварање културних вриједности итд.“[38]

Дисфункционалност информационих система владиног и невладиног сектора

Информациона безбједност је интегрална компонента националне безбједности и представља пресјек свих сектора безбједности у којима информационе технологије заузимају важно мјесто. Подразумијева стање заштићености животно важних вриједности и интереса индивидуе, друштва и државе од спољашњих и унутрашњих ризика.[39] Главне компоненте информационе безбједности су заштита личних података, државне и службене тајне, заштита података од случајних или намјерних природних или вјештачких утицаја, гаранција уставних права и слобода

[35] Ђорђевић, А: *Картографско моделовање инфраструктирних система у просторном планирању - докторска дисертација*. Географски факултет, Београд, 2013.
[36] Исто.
[37] Исто.
[38] Мијалковић, 2015, исто.
[39] Исто.

човјека и грађанина у погледу активности у информационој сфери и заштита потреба грађана од негативних (намјерних и случајних) информационо-психолошких и информационо-техничких утицаја. „Национални интереси државе у информационој сфери састоје се у поштовању уставних права и слобода грађана у области добијања информација и њиховог коришћења, у развоју савремених телекомуникационих технологија, у заштити државних информационих ресурса од неовлашћеног приступа.“[40]

Комплексан скуп система који укључују велики број технологија и сервиса чине телекомуникациону инфраструктуру. Ту спадају жичне, бежичне, кабловске и технологије за емитовање, језгрене мреже базиране на интернет протоколу као и интерни информациони системи.[41] Поред интернета као универзалне мреже („мреже свих мрежа“) постоје затворене интерне мреже – интранети, и затворене спољне мреже – екстранети. У оба случаја комуникација се одвија коришћењем интернет протокола. Интранет је интерни систем који користе различита одјељења исте организације повезана у рачунарске мреже, док екстранет служи за повезивање компанија и пословних партнера или удаљених дијелова исте корпорације.[42] Један од органа управе који користе интранет су министарства надлежна за унутрашње послове.

Дигитализација података у јавним службама има висок степен безбједносних ризика. Најслабија тачка концепта електронске управе је угрожавање критичне информационе и телекомуникационе инфраструктуре, односно безбједносни ризици од потенцијалних сајбер напада, злоупотреба и манипулација базама података. Као примјер наводимо могућност да усљед неадекватне заштите аутоматизованог сервиса за грађане злонамјерни појединци могу добити извод из матичне књиге другог лица, туђу возачку дозволу, пасош, узимати кредите на туђе име или чак могу некога прогласити мртвим.[43]

Јасно је да методе, начини и средства криминалних активности постају све софистицираније и коришћењем информационих технологија

[40] Герзић, Ч: Информациона безбедност као елемент националне безбедности. *15. Међународна конференција Ризик и безбедносни инжењеринг*, 2020.стр. 257-266).

[41] Gospić, N., Murić, G., & Bogojević, D: Definisanje kritične telekomunikacione infrastrukture u Srbiji. *Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju - PosTel 2012*, Beograd, 2012, str. 367-375.

[42] Ђорђевић, I: *Bezbednosna arhitektura u uslovima globalizacije*. Fakultet bezbednosti i Službeni Glasnik. Beograd, 2007.

[43] Исто.

повећава се број криминалних радњи у кредитно-финансијској сфери и при обради персоналних података.[44]

Производи, знање, услуге или сервиси који омогућавају функционисање организације чине информационе ресурсе који морају да се заштите на националном нивоу. Информације, пословни процеси и активности, хардвер, софтвер, мрежа, кадрови и организациона структура су фактори од којих зависи развој осталих националних вриједности и заштита националних интереса.[45]

У оквиру информационе безбједности развија се неколико специјалистичких области попут безбједности мрежа и информационе инфраструктуре, заштита софтвера и база података, ревизија информационог система, планирање континуитета пословања, рачунарска форензика и детекција електронских записа. „Обезбјеђење информационе заштите један је од кључних задатака формирања информационог друштва.“[46]

Информационо друштво захтијева стандардизоване мрежне услуге, процедуре и опрему, односне инфраструктурне услове који ће омогућити брз и сигуран пренос података. Информациони системи треба да буду у функцији подстицања дијалога и размјене информација од представника власти до грађана и обрнуто. Интернет као универзални сервис је један од приоритетних циљева развоја како националних држава тако и Европске уније и потребно је да се сваком појединцу омогући приступ интернету на индивидуалном нивоу. Стимулација употребе интернета обухвата конкретне акције попут увођења услуга електронске управе и електронског здравства. Уколико се уобичајна комуникација са државном управом одвија у електронској форми смањује се вријеме потребно за издавање дозвола, царињење робе и друге административне потребе грађана које могу да се обаве путем виртуелог шалтера.[47]

ЗАКЉУЧАК

Европска унија од свих земља чланица и земаља кандидата за чланство захтјева идентификовање и заштиту европских критичних инфраструктура. Са друге стране, у превенцији и ублажавању посљедица угрожавања суочавамо се са великим међудржавним разликама у финансирању и институционалним капацитетима система заштите и

[44] Герзић, исто.
[45] Мијалковић, 2015, исто.
[46] Герзић, исто.
[47] Đorđević, исто.

спасавања. До 2018. године 18 држава чланица је спровело активности и усвојило безбједносне приједлоге Европске Комисије по питању именовања европске критичне инфраструктуре. У осталим европским државама интензивно се ради на испуњавању обавеза и усаглашавању регулативе у области критичне инфраструктуре са тековинама и стандардима Европске уније.

Основна мисија критичне инфраструктуре је ефикасно функционисање државе и државних органа. Вода, храна, енергија, хемијска индустрија, саобраћајне мреже, информационе и комуникационе технологије су неке од инфраструктура које у модерно доба представљају основне услове за функционисање појединаца и друштва у цјелини. Смртно страдала или повријеђена лица, економски губици, смањење квалитета производа или услуга, утицај на јавност и дугорочан утицај на квалитет животне средине су неке од посљедица угрожавања критичне инфраструктуре по националну безбједност. Иако није лако раздовојити националне од глобалних извора угрожавања чињеница је да постоје локалне специфичности које утичу на безбједност људи са неког простора. Локалне прилике се могу посматрати у контексту климатских и осталих карактеристика географског положаја, али и у контексту уређености система и његове способности да се носи са безбједносним изазовима, ризицима и пријетњама на конкретном подручју.

Након схватања улоге и значаја критичне инфраструктуре и потенцијалних извора угрожавања доношене су одлуке и предузимају се акције на константној и ефикасној заштити критичне инфраструктуре. Ријеч је о комплексном систему безбједносних процедура и активности које имају за циљ да обезбиједе функционалност, непрекидно дјеловање и испоруку робе и услуга критичне инфраструктуре, као и да спријече угрожавање критичне инфраструктуре. Носиоци ових активности су национални системи безбједности чији субјекти имају задатак да остваре функцију националне безбједности. То чине радом на достизању, развоју и унапређењу националних вриједности и интереса, као и контролом безбједносних изазова, ризика и пријетњи.

Посљедице угрожавања критичне информационе и телекомуникационе инфраструктуре могу привремено довести до колапса здравственог и образовног система земље, као и до прекида у раду комплетног административног апарата. Знатан дио информационих ресурса се налази у приватном власништву и управо због тога дисфункционалност информационих система невладиног сектора неминовно води у дисфункционалност информационих система владиног сектора. Истина је да поједине земље немају у толикој мјери развијен систем електронског пословања, али глобално суочавање са пандемијом

COVID 2019 приморало је читаву планету да се довијава и комплетан живот организује посредством информационих технологија. Преко ноћи постајемо свједоци и актери живота „на мрежи“.

Посебно важан је утицај на јавност који производи заштићена или незаштићена критична инфраструктура, јер се о стању у држави грађани информишу преко медија. Уколико пласирање медијских садржаја није адекватно заштићено може доћи до јењавања осјећаја припадности држави или нацији. Уколико дође до губитка повјерења у националне институције националне безбједност може бити нарушена у већем обиму, долази до насилних преврата, угрожено је национално јединство и политичка стабилност – упитан опстанак државе и друштва. Предочавање врсте, садржаја и обима штетних ефеката незаштићене критичне инфраструктуре је фактор у имплементацији безбједнонсих мјера и формирања националних система за заштиту критичне инфраструктуре.

ЛИТЕРАТУРА

1. COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union* L 345/75, Brussels, 2008.
2. Critical Infrastructure Protection in the fight against terrorism. Commission of the European Communities, European Council, Brussels, 2004.
3. Đorđević, I: *Bezbednosna arhitektura u uslovima globalizacije*. Fakultet bezbednosti i Službeni Glasnik. Beograd, 2007.
4. EVALUATION of COUNCIL DIRECTIVE 2008/114 ON THE IDENTIFICATION AND DESIGNATION. European Commission, Brussels, 2019.
5. *Global Risks Report*, World Economic Forum, Davos, 2020.
6. Gospić, N., Murić, G., & Bogojević, D: Definisanje kritične telekomunikacione infrastrukture u Srbiji. *Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju - PosTel 2012*, Beograd, 2012, str. 367-375.
7. Green Paper on a European Programme for Critical Infrastructure Protection. Commission of the European Communities, Brussels, 2005.
8. Keković, Z., Ninković, V.: *Zaštita kritične infrastrukture – sistemski pristup*. Centar za analizu i upravljanje krizama, Beograd, 2020.

9. Lazari, A., & Simoncini, M.: Critical Infrastructure Protection beyond Compliance. An Analysis of National Variations in the Implementation of Directive 114/08/EC. *Global Jurist* 3 (16), 2016, pp 267–289.

10. Luburić, R., & Fabris, N: Money and the Quality of Life. *Journal of Central Banking Theory and Practice*, 2017, pp 17-34.

11. Mijalković, S., & Cvetković, V.: Vulnerability of Critical Infrastructure by Natural Disasters. *National Critical Infrastructure Protection - Regional Perspective Ljubljana - Belgrade*: Institut for Corporative Security Studies, 2013, pp 91-102.

12. Poljanšek, K., Marin Ferer, M., De Groeve, T., & Clark, I.: Science for disaster risk management 2017: knowing better and losing less. *Publications Office of the European Union*, Luxembourg, 2017.

13. Poustourli, A.: A Concise Survey of Security Standards and Certification Services. *13th INTERNATIONAL CONFERENCE "STANDARDIZATION, PROTYPES AND QUALITY: A MEANS OF BALKAN COUNTRIES COLLABORATION,"* Brasov, Romania, 2016, pp 230-246.

14. REVIEW OF THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION. European Commission, Brussels, 2012.

15. Sokolović, H: *Uticaj medija na formiranje političkih stavova i vrijednosti*. Filozofski fakultet Univerziteta u Sarajevu, Sarajevo, 2018.

16. Žiravac Mladenović, M.: Razlozi i interesi za regulaciju banaka. *Međunarodna konferenciji o društvenom i tehnološkom razvoju STED 2013*. Univerzitet za poslovni inženjering i menadžment, Banjaluka, 2013.

17. Герзић, Ч: Информациона безбедност као елемент националне безбедности. *15. Међународна конференција Ризик и безбедносни инжењеринг*, 2020.стр. 257-266).

18. Ђорђевић, А: *Картографско моделовање инфраструктирних система у просторном планирању - докторска дисертација*. Географски факултет, Београд, 2013.

19. Закон о безбједности критичних инфраструктура Републике Српске, Службени Гласник број 58/19.

20. Комарчевић, М.: *Увод у критичну инфраструктуру*. Академска мисао, Београд, 2018.

21. Мијалковић, С., & Милошевић, М: *Обавјештајно-безбедносна делатност и службе*. Висока школа унутрашњих послова, Бањалука, 2011.

22. Мијалковић, С.: *Национална безбедност.* Криминалистичко-полицијска академија, Београд, 2015.

23. Милашиновић, М.: Међународна сарадња и смањење ризика од елементарних непогода. *Безбедност* 3, 2019, стр. 200-219.

24. Сикимић, М.: *Критична инфраструктура као одредница националне безбедности – мастер рад.* Криминалиситчко-полицијски универзитет, Београд, 2021.

25. Сикимич, М.: Современные вызовы безопасности национальной критической инфраструктуры в Республике Сербской. Материалы VII Международной научно-практической конференции *Актуальные проблемы безопасности жизнедеятельности*, Москва, фебраль, 2021.

26. Трбојевић, М.: Заштита критичних инфраструктура - искуства транзиционих земаља. *Политичка ревија*, 2018, стр. 99-118.

27. Ћеранић, П.: *Безбједносна политика - прилике у Босни и Херцеговини*. Факултет безбједносних наука, Бањалука, 2020.

CONSEQUENCES OF THREATENING CRITICAL INFRASTRUCTURE ON NATIONAL SECURITY: A FACTOR FOR BUILDING LEGAL AND INSTITUTIONAL CAPACITIES

Milica Sikimić [48], MA

Abstract: In the launched program of the European Union for the protection of critical infrastructure, the requirements and guidelines for the protection of European critical infrastructures, and the achievement and preservation of security at the community level were presented. According to these guidelines, primary and final responsibility for critical infrastructure safety is addressed to Member States, their national legislation and critical infrastructure owners/operators. When implementing protection at the national level, states should take an approach that takes into account all sources of threat and all dangers, and actively encourage the involvement of the private sector in order to establish a unified system of protection. Critical infrastructure is classified by sectors and is viewed through national values such as economy and energy, economic stability and social prosperity, national information resources, healthy environment and the like. In relation to the stated values, the states have different national interests on the basis of which they set the goals and tasks of the national security policy and establish the national security system. Therefore, the aim of this paper is to investigate the consequences of critical infrastructure dysfunction that occur on the territory and in the administrative apparatus of a country. Consequences are one of the factors

[48] Assistant at the Faculty of Security Sciences, University of Banja Luka and PhD student at Obuda University in Budapest, e-mail: milica.sikimic@fbn.unibl.org

considered when making decisions on the allocation of funds and capacity to establish a national system for critical infrastructure protection. The available literature on the concept of critical infrastructure and its protection most often emphasizes the interconnectedness, interdependence and overflowing effect of endangered critical infrastructure - the supranational importance of unique protection. However, there is a certain gap about the consequences of disruptions in the operation of critical infrastructure facilities, systems and networks that have a primary and unavoidable effect on the state of national security. The paper will present the results of research on the consequences of endangering critical infrastructure related to human and economic losses of a country, the dysfunction of the governmental and non-governmental sector, as well as interruptions in the work of the entire administrative apparatus.

Key words: critical infrastructure, state obligations, security, endangerment, direct damage, indirect damage.

CIP - Каталогизација у публикацији
Народна и универзитетска библиотека
Републике Српске, Бања Лука

351.78(082)

НАУЧНО-стручна конференција са
међународним учешћем „Заштита
критичне инфраструктуре – обавезе
држава и могућности приватног сектора
безбједности“ (2 ; 2021)
Zaštita kritične infrastrukture – obaveze
država i mogućnosti privatnog sektora
bezbjednosti : zbornik radova / [glavni i
odgovorni urednici Nikolina Grbić Pavlović,
Željko Zorić] ; [prevod Gordana Višekruna]. -
Banja Luka : Istraživački centar : Sector
Security, 2021 (Banja Luka : Glas Srpske). -
VIII, 111 стр. : табеле, граф. прикази ; 25 cm

Према предговору, радови су
представљени на 2. Научно-стручној
конференцији са међународним учешћем
на тему: „Заштита критичне
инфраструктуре – обавезе држава и
могућности приватног сектора
безбједности“, која је одржана 21. маја
2021.године. - На спор. насл. стр.: Critical
infrastructure protection - state obligations
and private security sector opportunities :
collection of papers. - Радови на срп. и енгл.
језику. - Лат. и ћир. - Тираж 100. -
Напомене и библиографске референце уз
текст. - Библиографија уз сваки рад. -
Abstracts.

ISBN 978-99976-914-3-9 (Istraživački centar)

COBISS.RS-ID 135077377