DEVELOPMENT OF THE CONCEPT OF CRITICAL INFRASTRUCTURE PROTECTION IN MONTENEGRO - ROADS, EXPERIENCES, ROLE AND RESPONSIBILITY

Mersad Mujevic
Ministry of Internal Affairs of Montenegro, Montenegro, mersadm@t-com.me
Safet Korac
Ministry of Internal Affairs of Montenegro, Montenegro, safet.korac@mup.gov.me

Abstract: In the time behind us, significant progress has been made in various industries in many fields such as economy, innovation, transport, information and communication technologies, health and others. without these as well as some other services, social cohesion, economic prosperity, security of the country are or would be endangered. However, the progress made in these areas brings with it our dependence on the one hand and on the other hand the risks in case of "improper" functioning that can be vital for the well-being of the country. And in that sense, the resilience of our infrastructure must be part of a strong economic and dynamic business sector.
Security and proper functioning of infrastructure is crucial for ensuring the development of society, which puts the issue of improving the level of resilience in the forefront in the field of crisis management.
In the light of this situation, Montenegro has assessed and decided that it must improve the level of resilience of its critical infrastructure in order to identify it in the first place, thus further enabling its maintenance / functioning to prevent crises and absorb potential impacts when it arises, in a word, the ability of the system to prevent the occurrence of a crisis, and in the case when and if it occurs, the ability to absorb the magnitude of the impact and effectively recover and return to the normal situation.
This paper should present the development of the concept of critical infrastructure protection in Montenegro, which would help critical infrastructure operators to improve, among other things, the level of their role and responsibility in critical infrastructure management. This paper provides a list of policies and sub-policies that critical infrastructure operators need to implement in their critical infrastructure to increase its resilience level.
Keywords: critical infrastructure, resilience, protection, critical infrastructure operators

RAZVOJ KONCEPTA ZAŠTITA KRITIČNE INFRASTRUKTURE U CRNOJ GORI – PUTEVI, ISKUSTVA, ULOGA I ODGOVORNOST

Mersad Mujević
Ministarstvo unutrašnjih poslova Crne Gore, mersadm@t-com.me
Safet Korać
Ministarstvo unutrašnjih poslova Crne Gore, safet.korac@mup.gov.me

Abstrakt: U vremenu iza nas u različitim djelatnostima ostvaren je značajan napredak i to na mnogim poljima kao što su ekonomija, inovacije, saobraćaj, informaciono komunikacione tehnologije, zdrastvo i dr. bez ovih kao i nekih drugih usluga, socijalna kohezija, ekonomski prosperitet, bezbjednost zemlje su ili bi bili ugroženi. Međutim ovako ostvareni napredak u pomentim oblastima sa sobom nosi i našu zavisnost od iste s jedne strane a sa druge i rizike u slučaju „nepravilnog“ funkcionisanja koje mogu biti od vitalnog značaja za dobrobit zemlje. Te u tom smislu otpornost naše infrastrukture mora biti dio snažnog privrednog i dinamičnog poslovnog sektora.
Bezbjednost i pravilno funkcionisanje infrastrukture od presudne je važnosti za obezbjeđenje razvoja društva, što pitanje poboljšanja nivoa otpornosti postavlja u prvi plan na polju upravljanja krizama.
U svjetlu ove situacije, Crna Gora je procijenila i donijela odluku da mora poboljšati nivo otpornosti svoje kritične infrastrukture kako bi se ista prije svega identifikovala a na taj način se dodatno omogućilo njeno održavanje/ funkcionisanje kojim bi se spriječilo nastajanje kriza i apsorbovali eventualni uticaji kada se ona pojavi, jednom riječju, sposobnost sistema da se spreči pojava krize, a u slučaju kada i ako se se dogodi, sposobnost da apsorbuje veličinu utjicaja i efikasan oporavak i porvaraćaj normalnoj situaciji.
Ovaj rad upravo treba da predstavi razvoj koncepta zaštite kritične infrastructure u Crnoj Gori koji bi pomogao operaterima kritične infrastrukture da poboljšaju između ostalog nivo svoje uloge i odgovornosti u upravljanju kritičnom infrastrukturom. Ovaj rad pruža popis politika i podpolitika koje operateri kritične infrastrukture trebaju da implementiraju u svoju kritičnu infrastrukturu kako bi povećali nivo njene otpornosti.
Ključne riječi; kritična infrastruktura, otpornost, zaštita, operateri kritične infrastrukture

1. UVOD

Rasprave u međunarodnoj naučnoj i stručnoj zajednici o značenju onoga što sačinjava "kritičnu infrastrukturu" nijesu nove i nepoznate. Prije nego je sintagma "kritična infrastruktura" postala izuzetan predmet interesovanja u brojnim analizama koje su se odnosile na terorizam i unutrašnju bezbjednost, pojam "infrastruktura" osamdesetih godina je bio referentna tačka kreatora javne politike i bezbjednosti. Danas se u brojnim analizama "kritična infrastruktura" najčešće određuje kao skup fizičkih i virtuelnih sistema i sredstava koji su ključni za normalno funkcionisanje države.

Kritična infrastruktura obuhvata pojedine institucije javnog i privatnog sektora, kanale distribucije i "mreže" osoba i informacija koje garantuju nesmetan i kontinuiran protok ljudi, roba, usluga, što je ključno za stabilnost ekonomskog, socijalnog i bezbjednosnog sistema zemlje. Krizne situacije u najvećem broju slučajeva prouzrokuju oštećenja na infrastrukturnim sistemima, čime remete ustaljene načine i metode snadbijevanja stanovništva, privrede i drugih korisnika koji su direktno zavisni od njihovog funkcionisanja.

S druge strane, zastoj u svakodnevnom funkcionisanju infrastrukturnih kapaciteta može prouzrokovati stanje krizne situacije. Zbog toga je u svijetu prioritet u zaštiti definisan na način da se, uz ljudske živote, koji su po rangu zaštite ostali na prvom mjestu, definiše potreba zaštite i kritičnih infrastrukturnih sistema.

Crnogorski pravni sistem je još 2016 godine ovom pitanju posvetio određenu, pa možemo reći malu pažnju ovom pitanju, naime, tadašnje Ministarstvo za informaciono društvo i telekomunikacije je izradilo Zakon o izmjenama i dopunama Zakona o informacionoj bezbjednosti[1] kojim je definisana kritična informatička infrastruktura. Vlada Crne Gore je na prijedlog tadašnjeg Ministarstva za informaciono društvo i telekomunikacije usvojila Metodologiju izbora kritične informatičke infrastrukture. Na osnovu Metodologije, Ministarstvo javne uprave koje je naslijedilo određene nadležnosti nekadašnjeg Ministarstva za informaciono društvo i telekomunikacije, je u saradnji sa drugim nadležnim institucijama definisalo listu kritične informatičke infrastrukure u Crnoj Gori, a u toku je i izrada Uredbe o mjerama za zaštitu.

Početna lista kritične informatičke infrastrukture u Crnoj Gori je usvojena. Nakon usvajanja Uredbe o mjerama za zaštitu KI, istu je neophodno i implementirati u saradnji sa vlasnicima KI.

Na tragu pomenutih propisa krajem 2019 godine crnogorski Parlament usvaja Zakon o određivanju i zaštiti kritične infrastrukture kojim se uređuje buduća identifikacija, određivanje i zaštita kritične infrastrukture Crne Gore, kao i nadležnosti, odgovornosti, i druga pitanja od zanačaja za kritičnu infrastrukturu, zakonom je predviđena i evropska kritična infrastruktura, tj. kritična infrastruktura EU, čije odredbe će se primjenjivati po ulasku Crne Gore u EU.

Crnogorska kritična infrastruktura (u daljem tekstu KI) je specifična, prevashodno iz razloga što obuhvata više resora, te je prilikom određivanja iste, bilo potrebno da se vodi računa o tome da se obuhvati svaka oblast društva na koju se ona odnosi. Navedene oblasti nazvane su sektorima kritične infrastrukture. Za upravljanje kritičnom infrastrukturom zaduženi su operatori kritične infrastrukture, a to mogu biti državni organi, organi državne uprave, organi lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, privredna društva i druga pravna lica koji upravljaju sistemima, mrežama, objektima ili njhovim djelovima koji su određeni kao kritična infrastruktura.

2. INICIJATIVE ZA ZAŠTITU KRITIČNE INFRASTRUKTURE - ISKUSTVA CG

Analizirajući globalne bezbjedonosne rizike i prijetnje ovo područje postaje sve zahtjevnije i sveobuhvatnije te zahtijeva uključenost svih mogućih aktera na ovom području. Crna Gora svjesna činjenice da efikasan sistem zaštite KIa stvara preduslove za normalno i nesmetano funkcionisanje šireg društvenog sistema, ulaže značajne napore, kako u pogledu normativnog definisanja tog sektora, tako i na planu iznalaženju optimalnih mehanizama zaštite nacionalne KI. Ovi napore nijesu isključivo reagovanje na savremene trendove u ovoj oblasti, već potreba, usklađivanja nacionalnog zakonodavstva i prakse sa pravnim tekovinama EU u procesu pridruživanja CG EU. Sve to predstavlja i diskontituitet sa ranijim stanjem u kome je nacionalna KI posmatrana isključivo iz ugla oružanih snaga i potreba sistema odbrane države. U aktuelnim okolnostima, posebno se osjetljivim smatra spektar vitalnih sektora koje obuhvata KI i čiji djelimičan ili potpun prekid rada može narušiti normalno funkcionisanje određenog sistema i ugroziti nacionalnu bezbjednost. S druge strane, od KI Crne Gore očekuje se da pruža osnovne usluge koje podržavaju razvoj crnogorskog društva i odražavaju način na koji život u njemu funkcioniše [1]. S tim u vezi, kao jedan od prvih zadataka se nametnulo pitanje definisanje sektora infrastrukture koji su od vitalnog značaja i kao takvi predstavljaju KI.

Bezbjednost sistema KI i njihovih funkcija nije značajna samo za državne institucije, budući da se bezbjednosne dileme u pogledu zaštite KI mogu pojaviti u i privatnom sektoru koji se pojavljuje kao partner u izvršavanju misija i zadataka u toj oblasti.

1 "Službeni list Crne Gore", br. 40/16

U crnogorskom zakonodavdstvu KI se odnosi na elemente fizičkih i logičkih sistema koji su ključni za funkcionisanje državne administracije i ekonomije. U sastav KI ulaze oblasti energetike, saobraćaja, snabdijevanja vodom, zdravstva, finansija, elektronskih komunikacija i informaciono-komunikacionih tehnologija, zaštite životne sredine i funkcionisanja državnih organa.

Jasno nam je da pomenuti sistemi postaju sve više isprepletani i u tom smislu identifikujemo dva trenda. Prvi se odnosi na brzinu razvoja tehnologije, koji nije jednako izražen u cijelom svijetu pa ni u našoj zemlji. Jer neka društva-oblasti evidentno zaostaju, neka se bore da zadrže korak sa razvojem tehnologije, dok se kod drugih mogu vidjeti revolucionarni iskoraci [2].

2.1. Strateška i normativna dimenzija Zakona

Direktiva Savjeta 2008/114/EZ [2] od 08. decembra 2014 godine predstavlja okosnicu mnogih procesa na nivou EU, njom se propisuju postupak utvrđivanja potencijalne evropske KI; primjena međusektorskih mjerila (kao što su moguće žrtve, ekonomske posljedice i uticaj na javnost) i sektorskih mjerila specifičnih za pojedine vrste KI; saradnja država u utvrđivanju i označavanju evropske KI; materija bezbjedonosnih planova operatera; važnost operatera za vezu zaduženog za bezbjednost KI; izvještavanje država svake dvije godine prema Evropskoj komisiji o vrstama rizika, prijetnjama i slabostima u zaštiti evropske KI.

Komisija je do sada pokrenula dvije značajne revizije pomenute Direktive Savjeta 2008/114/EZ.

Nakon prve revizije (u kojoj su utvrđeni izazovi implementacije, saradnje i izvještavanja Komisije), Komisija je 2013. godine u Radnom dokumentu službi o novom pristupu Evropskom programu zaštite KI preporučila:

- *Efikasnije obezbjeđenje evropske KI, i naglasila potrebu razvoja zajedničkih alata i pristupa jačanju otpornosti i zaštiti KI na nivou EU, naglašavajući međusobnu zavisnost i važnost dodatne saradnje između vlasnika/upravljača KI, industrije i država.*

Druga revizija je sprovedena tokom 2018. i 2019. godine (utvrđena je djelimična efikasnost glavnih aktera u postizanju zadanih ciljeva), a razultati su objedinjeni u Radnom dokumentu službi o novom pristupu Evropskom programu zaštite KI:

- *Efikasnije obezbjeđenje evropske KI, gdje su pružene vrlo korisne preporuke za dalju saradnju i zaštitu evropske KI.*

Oba dokumenta pružaju neophodne informacije o promjenama koje se događaju unutar EU konteksta te ih je bilo potrebno sagledati i uvažiti u izradi Zakona o KI naše zemlje. Što je svakako bio zadatak za ispunjenje crnogorske strane.

Pored analize ponemutih revizija, bilo je potrebno da se sa naše strane analizira naglašenost svih EU strategija i procjena, u dijelu jačanja otpornosti i zaštite KI, koje pored razvojne komponente daju i smjernice vezane uz nove rizike prema KI i načine bavljenja njima. Neizostavna komponenta bila je i saradnja sa akademskim i privatnim sektorom u osmišljavanju, razvoju, dizajnu, implementaciji i sprovođenju mjera jačanja otpornosti i zaštite KI.

Slika 1. Savremeni rizici

Na nivou CG, nakon donošenja Zakona o određivanju i zaštiti KI 2019. godine, bitno ćemo osnažiti strateško-bezbjedonosne dimenzije i arhitekturu gdje se području KIa pridaje značajna pažnja. U Strategiji nacionalne

[2] Vijeće Europske unije (2008), Direktiva Vijeća 2008/114/EC o identifikaciji i određivanju europskih kritičnih infrastruktura (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF)

bezbjednosti CG iz 2018. godine[3] Crna Gora se odredila prema tri strateška nacionalna interesa koje realizuje putem četrnaest strateških interesa/ciljeva. Jedan od strateških ciljeva je dostizanje najvišeg stepena bezbjednosti i zaštite stanovništva kao i KI. Dio vezan uz KI izrazito je kvalitetno postavljen i pruža čitav niz političkih smjernica (neke od njih će biti pokušati izdvojiti u daljem radu), koje je bilo potrebno razraditi i uvrstiti u naš Zakon o KI. Jednako važno je da je Strategijom određeno uspostavljanje sistema državne bezbjednosti koji treba da obezbijedi usklađenu pripremu i sprovođenje propisa kojima će se određivati bezbjedonosne mjere i postupci važni za nacionalnu bezbjednost, posebno zaštitu KI.

Sistem državne bezbjednosti uspostavljen je Zakonom o odbrani[4] koji, pored zaštite KI kao svrhe donošenja, izdvaja i potrebu ojačavanja funkcije upravljanja u vanrednim i kriznim stanjima koja su rizik za nacionalnu bezbjednost, uključujući i krizna stanja upravljana na nivou Organizacije Sjevernoatlantskog saveza, kao i omogućavanja primjerenog doprinosa u zaštiti i jačanju nacionalne bezbjednosti na svim nivoima države i društva.

Sve su ovo elementi koje je bilo potrebno imati u vidu kod izrade Zakona o određivanju i zaštiti KI.

Nacionalna strategija sajber bezbjednosti za period 2018-2020 snažno naglašava važnost KI u opšte, kao i kritične komunikacijske i informacine infrastrukture specifično, sa ciljem: „povećanja otpornosti/smanjenja ranjivosti komunikacionih i informacionih sistema; umanjivanja posljedica negativnih događaja (prirodne i tehničko-tehnološke nesreće) i mogućih napada (namjernih i nenamjernih); omogućavanja brzog i efikasnog oporavka te nastavka rada“.

Kritičnu komunikacionu i informacionu infrastrukturu predstavljaju oni komunikacioni i informacioni sistemi koji upravljaju KI ili su bitni za njeno funkcionisanje, a pristup njihovoj zaštiti holistički je postavljen sa svrhom integracije postojećih i razvoja novih procedura unutar sistema upravljanja u sajbet odnosno kibernetičkim krizama EU i NATO-a, kao i dovršetak nacionalnog sistema upravljanja kibernetičkim odnosno sajber krizama. Iz ovog je dijela, bilo potrebno izdvojiti elemente kako bi novi Zakona o određivanju i zaštiti KI sa sobom obuhvatio smjernice i rješenja koje EU i NATO Savez razvijaju u predmetnom području.

Mnogi javni izvještaji u Crnoj Gori navode da su članice NATO-a i EU često pod napadima malicioznih kibernetičkih kampanja koje imaju za cilj probijanje u zaštićene informacione i komunikacione sisteme, pa je tako i Crna Gora bila meta niza kibernetičkih napada posljednjih godina, naročito u oči učlanjenja u NATO i da one postaju sve češće, složenije i destruktivnije. NATO saveznici snose primarnu odgovornost za svoju nacionalnu sajber obranu, na što su se tokom Varšavskog samita 2016. obavezali čelnici država članica, označavajući jačanje sajber odbrane kao prioritet. Kao vrste napada na Alijansin sistem ispitivanje NATO mreža kako bi se iskoristile potencijalne ranjivosti odbrane ili izvukle informacije, pokušaje savladavanja NATO zaštite i ometanja internetskih stranica Alijanse.

U Crnoj Gori do sada je najčešće registrovani slučajevi u kojima su računari zaraženi "WannaCry" ransomwarom. To je jedan od najopasnijih ransomwara koji se pojavio 2017.godine, a koji se se proširio ogromnom brzinom i tokom prva dva dana zarazio preko 170.000 uređaja širom svijeta. Tokom 2018. godine registrovan je veliki broj napada povezanih sa više hakerskih grupa, kao i značajan porast napada na informacione sisteme državnih organa i pravnih lica.

Cilj takvih napada je različit, od narušavanja funkcionisanja u državi ili privatnom sektoru onesposobljavanjem web sajtova, aplikacija i interneta, pa do otuđivanja podataka.

Da je taj prostor sve ugroženiji, govori statistika prijavljenih incidentnih situacija na internetu u Crnoj Gori, koja je tokom ove decenije u porastu: samo jedan slučaj je prijavljen 2011, da bi taj broj lani narastao na oko 500. To su podaci Tima za odgovor na računarske incidente (CIRT), objavljeni u Izvještaju o incidentnim situcijama na internetu u Crnoj Gori za 2017 i 2018 godinu (Ministarstvo javne uprave) [3].

Citirano smo izdvojili kako bi pokazali potrebu robusnijeg i sveobuhvatnog pristupa ovom području i kako bi Zakon o određivanju i zaštiti KI trebao odražavati svjesnost o novim rizicima i potrebnoj saradnji svih segmenata našeg društva.

Do izrade implementacionih akata pomenuti zakoni i Strategije u mnogme rješevanju postavljene ciljeve Zakona o određivanju i zaštiti KI. Pored pomenutih zakona izdvojićemo ovom prilikom i zakon o zaštiti i spašavanju CG koji obuhvata skup mjera i radnji koje se preduzimaju u cilju otkrivanja i sprječavanja opasnosti od prirodnih nepogoda, požara, tehničko-tehnoloških nesreća, hemijskih, bioloških, nuklearnih i radioloških kontaminacija, posljedica ratnog razaranja i terorizma, epidemija, epizootija, epifitotija i drugih nesreća, kao i spašavanja građana i materijalnih dobara ugroženih njihovim djelovanjem.

Kako smo već i napomenuli svjesni činjenica da efikasan sistem zaštite KI stvara preduslove za normalno i nesmetano funkcionisanje društva i države uopšte, svaka država ulaže značajne napore u cilju izrade adekvatnih

[3] (“Službeni list CG” br. 85/2018),
[4] (“Službeni list CG” br. 046/19),

mehanizama zaštite. Ono što zaista predstavlja otežavajuću okolnost prilikom izrade adekvatnih mehanizama zaštite jeste širok spekrat vitalnih sektora koji obuhvata KI, već smo naveli oblasti energetike, saobraćaja, snabdijevanja vodom, zdravstva, finansija, elektronskih komunikacija i informaciono-komunikacionih tehnologija, zaštite životne sredine idr. Djelimičan ili potpun prekid rada ovih infrastruktura može da naruši normalno funkcionisanje jednog sistema i ugroziti državu bezbejdnost.

Dakle, kada je u pitanju zaštita KI, zajednički cilj kojem teže sve uređene države pa i našu Crnu Goru, jeste izgradnja adekvatnih mehanizama koji će spriječiti stavranje uslova koji se mogu da dovedu do otkazivanja određene infrastinfrastrukture nesreće ili napada na bilo koji element sistema.

Kako skoro svaka zemlja ima različite modele zaštite KI, Crna Gora je pažljivo analizirala dostupne modele i izvukla najbolja iskustva.

3. IMPLEMENTACIJA PROCESA

Implementacija pricesa u našoj zemlji se odvija kroz tri faze i to:

- Identifikacija potencijalne KI,
- Određivanje KI (sektorska i međusektorska mjerila),
- Zaštita KI.

a. Identifikacija potencijalne KI

Nakon usvajanja Zakona o određivanju i zaštiti KI, Crna Gora je relativno brzo pokrenula inicijativu za izradu implementacione regulative kako bi isti dodatno uskladika sa EU zakonodavdstvom. U tom smislu MUPa CG je početkom 2020 formiralo međuresorsku radnu grupu za izradu **Uredbe o sektorskim kriterijumima za određivanje KI.** Ovom uredbom treba da se propišu sektorski kriterijumi za određivanje KI u oblasti energetike, saobraćaja, snabdijevanja vodom, zdravstva, finansija, elektronskih komunikacija i informaciono-komunikacionih tehnologija, zaštite životne sredine i funkcionisanja državnih organa. Radnu grupu su činili predstavnici: ministarstva untrašnjih poslova, ministarstva odbrane, ministarstva saobraćaja i pomorstva, ministarstva ekonomije, ministarstva održivog razvoja i turizma, CBCG, ministarstva javne uprave, ministarstva zdravlja, akademske zajednice.

Međuresorska radna grupa u procesu utvrđivanja sektorskih kriterijuma za određivanje KI u određenim već pomenutim oblatima uradila je nekoliko nacrta. Svaki nacrt je u osnovi sadražavao sljedeće sektorski elemente koji su u završnoj fazi predaje Vladi CG na usvajanje a ticali su se prije svega pitanje definisanja kriterijuma, te se konsenzusom utvrdilo da se KI smatra infrastruktura koja u slučaju prekida rada:

- utiče na ozbiljan poremećaj u radu ili u rada koji može prouzrokovati prekid u snabdijevanju električnom energijom u trajanju od najmanje tri dana na području sa više od 30.000 stanovnika;
- dovodi do ozbiljnog poremećaja u radu ili prekidu rada u snabdijevanju naftnim derivatima u trajanju od najmanje sedam dana na području sa više od 30.000 stanovnika,
- oštećenje infrastrukture koje prouzrokuje nepružanje vode za piće najmanje 7 dana na teritoriji na kojoj živi i radi više od 15.000 stanovnika,
- oštećenje infrastrukture, koje prozrokuje onemogućavanje pružanja hitne medicinske pomoći i medicinske zaštite najmanje 48 časovana teritoriji na kojoj živi najmanje 15.000 stanovnika,
- oštećenje infrastruture koja prouzrokuje nemogućnost funkcionisanja sistema informaciono-kumunikacionih tehnologija koji podržava ključne funkcije u Crnoj Gori, a koji se odnose na osiguranje rada jednog od ključnih sektora infrastrukture, sistem nacionalne bezbjednosti, energetski sistem, zdravstveni sistem i finansije koji dovode do pada podrške u trajanju dužem od šest časova,
- nemogućnost funkcionisanja državnih organa nadležnih zateritoriju u kojoj živi više od 50. 000 ljudi, u trajanju od najmanje 24 časa.
- nemogućnost vršenja bankarskih i finansijskih operacija CBCG duže od 24 časa.

3.1. *Određivanje KI (sektorska i međusektorska mjerila),*

Sektorski kriterijumi u oblasti **energetike** su:

- infrastruktura ili objekat za proizvodnju ili prenos električne energije čiji ozbiljni poremećaj u radu ili prekid rada može prouzrokovati raspad elektroenergetskog sistema Crne Gore do te mjere da je za njegovo ponovno uspostavljanje na cijeloj teritoriji Crne Gore potrebno najmanje sedam dana;
- infrastruktura ili objekat za proizvodnju ili prenos električne energije čiji ozbiljni poremećaj u radu ili prekid rada može prouzrokovati prekid u snabdijevanju električnom energijom u trajanju od najmanje tri dana na području sa više od 30.000 stanovnika;
- objekat za skladištenje naftnih derivata čiji ozbiljni poremećaj u radu ili prekid rada može prouzrokovati prekid u snabdijevanju naftnim derivatima u trajanju od najmanje sedam dana na području sa više od 30.000 stanovnika.

Infrastrukturu u oblasti energetike koja se može odrediti kao kritična čine:

- hidroelektrane instalisane snage veće od 200 MW;
- termoelektrane instalisane snage veće od 200 MW;
- elementi prenosnog sistema električne energije (postrojenja 110 kV, transformatori 110/x kV i vodovi 110 kV, kao i postrojenja, transformatori i vodovi višeg naponskog nivoa);
- objekti za skladištenje naftnih derivata za široku potrošnju zapremine veće od 10.000 m^3;
-objekti za skladištenje mlaznog goriva za vazduhoplove zapremine veće od 4.000 m^3.

Sektorski kriterijumi u oblasti **saobraćaja** su:
- oštećenje infrastrukture iz stava 2 tač. 1 i 2ovog člana, koje prouzrokuje obustavljanje rada drumskog i željezničkog saobraćaja na ključnim pravcima u trajanju dužem od sedam dana, odnosno prouzrokuje materijalnu štetu u iznosu od million eura dnevno,ili više,
- oštećenje infrastrukture iz stava 2 tačka 3 koje onemogućava obavljanje lučkih aktivnosti u trajanju dužem od sedam dana,sa gubitkom većim od milion eura dnevno, ili više,
- oštećenje infrastrukture iz stava 2 tačka 4 ovog člana, koje prouzrokuje nemogućnost obavljanja vazdušnog saobraćaja u vazdušnom prostoru Crne Gore u trajanju od 12 časova ili duže.

Infrastrukturu koja se može odrediti kao kritična čine:
1. U drumskom saobraćaju:
- autoputevi;
- magistralni putevi čija dnevna frekvencija prelazi 20.000 vozila;
- regionalni putevi čija dnevna frekvencija prelazi 10.000 vozila;
- tuneli i mostovi na regionalnim i magistralnim putevima.

2. U željezničkom saobraćaju:
- željeznička mreža koja se pruža pravcem koji povezuje opštine čiji broj stanovnika prelazi 20. 000.

3. U pomorskom saobraćaju:
- luke čija dužina operativne obale iznosi najmanje 500 metara;
- trgovačke luke od nacionalnog značaja, koje su otvorene za međunarodni saobraćaj i koje imaju terminale za pretovar i skladištenje tereta**;**

4. U vazdušnom saobraćaju:
- aerodromi čija poletno slijetna staza ima najmanju dužinu od 2400m i širinu od 40 metara.

Sektorski kriterijumi u oblasti **snabdijevanja vodom** su:
- oštećenje infrastrukture iz stava 2 ovog člana koje prouzrokuje nepružanje vode za piće najmanje 7 dana na teritoriji na kojoj živi i radi više od 15.000 stanovnika.

Infrastrukturu koja se može odrediti kao kritična čine:
- javni vodovodi koji omogućavaju vodosnabdijevanje naseljau kojem je nastanjeno najmanje 2000 stanovnika;
- regionalni vodovodi koji omogućavaju vodosnabdijevanje dvije ili više jedinica lokalnih samouprava, odnosno naselja na njihovom području;
- objekti u kojima se vrši proizvodnja ili distribucija vodekoje imaju proizvodni kapacitet od 15. 000 l vode na čas;
- akumulacije vode za industrijske potrebe;
- skladišta vode.

Sektorski kriterijumi u oblasti **zdravstva** su:
- oštećenje infrastrukture iz stava 2 ovog člana, koje prozrokuje onemogućavanje pružanja hitne medicinske pomoći i medicinske zaštite najmanje 48 časovana teritoriji na kojoj živi najmanje 15.000 stanovnika,
- oštećenje infrastrukture iz stava 2 ovog člana, koje prouzrokuje onemogućavanje pružanja hitne medicinske pomoći i medicinske zaštite najmanje 72 časa na teritoriji čije je geografsko područje manje pristupačno na kojem živi najmanje 5.000 stanovnika.

Infrastrukturu koja se može odrediti kao kritična čine:
- zdravstvene ustanove u kojima se pruža tercijarni nivo zdravstvene zaštite;
- zdravstvene ustanove u kojima se pruža sekundarni nivo zdravstvene zaštite;
- zdravstvene ustanove u kojima se pruža primarni nivo zdravstvene zaštite;
- zdravstvene ustanove u kojima se pruža hitna medicinska pomoć;
- zdravstvene ustanove u kojima se pruža vanbolnička zdravstvena zaštita;
- zdravstvena ustanove koje obavljaju djelatnost transfuzije krvi;

Sektorski kriterijumi u oblasti **finansija** su:
- onemogućavanje snabdijevanja gotovinom najmanje tri dana za dvije ili više teritorija na kojoj živi najmanje 50.000 stanovnika,
- neizvršavanje državnog budžeta za maksimalni period od 14 dana,
- neizvršavanje platnih transakcija učesnika kroz platni sistem u trajanju od najmanje 24 časa;

- neizvršavanje prinudne naplate u trajanju od najmanje 24 časa;
- nemogućnost upravljanja međunarodnim rezervama u trajanju od najmanje 24 časa;
- nemogućnost servisiranja klijenata CBCG u trajanju od najmanje 24 časa;
- nemogućnost obavljanja platnog prometa i korespondentskih odnosa sa inostranstvom u trajanju od najmanje 24 časa;
- nemogućnost snabdijevanja novčanicama i kovanim novcem u trajanju od najmanje 24 časa;
- nemogućnost vršenja bankarskih i finansijskih operacija CBCG duže od 24 časa;
- nemogućnost obezbjeđivanja novčanica i kovanog novca duže od 48 časova;
- nemogućnost vršenja posredne kontrole finansijskihinstitucija duže od 72 časa;
- nemogućnost zaštite novčanica i kovanog novca od falsifikovanjaduže od 72 časa.

Sektorski kriterijumi u oblasti elektronskih komunikacija i **informaciono-komunikacionih** tehnologija su:
- oštećenje infrastrukture iz stava 2 ovog člana koje prouzrokuje nemogućnost funkcionisanja sistema informaciono-kumunikacionih tehnologija koji podržava ključne funkcije u Crnoj Gori, a koji se odnose na osiguranje rada jednog od ključnih sektora infrastrukture, sistem nacionalne bezbjednosti, energetski sistem, zdravstveni sistem i finansije koji dovode do pada podrške u trajanju dužem od šest časova.

Infrastrukturu koja se može odrediti kao kritična čine:
- infrastruktura čija ozbiljna neispravnost ili prekid rada može rezultirati neaktivnošću elektronskih komunikacionih mreža i usluga u trajanju od najmanje četiri časa, a koje podržavaju rad najmanje jednog sektora kritične infrastrukture ili nacionalnog sigurnosnog sistema;
- infrastruktura čija ozbiljna neispravnost ili prekid rada može rezultirati nefunkcionisanjem elektronskih usluga javnog sektora u trajanju od najmanje šest časova;
- infrastruktura čija ozbiljna neispravnost ili prekid rada može rezultirati nefunkcionisanjem elektronskih komunikacionih mreža i usluga u trajanju od najmanje 24 časa, na teritoriji na kojoj je nastanjeno više od 15. 000 stanovnika.

Sektorski kriterijumi u oblasti **zaštite životne** sredine su:
- onemogućavanje tretmana komunalnih i industrijskih otpadnih voda za više od mjesec dana na području sa više od 15.000 stanovnika i povezanom ekonomskom infrastrukturom,
- oštećenje na postrojenju za prečišćavanje otpadnih gasova koje nije moguće otkloniti za 24 časa što zaustavlja rad postrojenja za prečišćavanje otpadnih gasova;
- oštećenje infrastrukture koje onemogućava njen rad kojim se osigurava prikupljanje i obrada otpada više od nedjelju dana na području sa više od 15.000 stanovnika i povezanom ekonomskom infrastrukturom,
- kontaminacija površine veće od 10ha opasnim materijama uzimajući u obzir uticaj na zdravlje ljudi i životnu sredinu;
- kontaminacija voda opasnim materijama, uzimajući u obzir uticaj na zdravlje ljudi i životnu sredinu;

Infrastrukturu koja se može odrediti kao kritična čine:
- objekti za skladištenje hemijskih materija i supstanci.

Sektorski kritrerijumi u oblasti funkcionisanja **državnih organa** su:
- nemogućnost funkcionisanja državnih organa nadležnih zateritoriju u kojoj živi više od 50. 000 ljudi, u trajanju od najmanje 24 časa.

Kriterijumi se odnose na Skupštinu Crne Gore, Vladu Crne Gore, sudove, tužilaštvo, organe državne uprave nadležnih za unutrašnje poslove, finansije, zaštitu i spašavanja, odbranu, ekomoniju, saobraćaj i pomorstvo, …organ uprave nadležan za policijske poslove, ANB,…

3.2. *Zaštita kritične infrastrukture*

Potrebno je istaći da ne postoji jedinstveni, unaprijed utvrđeni institucionalni model, koji ukazuje kako država treba da štiti svoju KI. Od vlada država se očekuje da izaberu okvir koji najbolje odgovara njihovim karakteristikama u pogledu prijetnji, veličine i strukture njihovih ekonomija, kao i njihove kulture javnih politika i ustaljenih institucionalnih praksi. Sa aspekta upravljanja KI posebno treba uzeti u obzir osnovnu ustavnu strukturu države [4].

U savremenoj praksi, arhitektura KI obično varira između dva osnovna modela. Jedan od modela upravljanja KI zasniva se na principima samoregulacije, podsticaja i dobrovoljnog poštovanja. To je takozvani „dobrovoljni pristup“ kao proizvod politike koja je fokusirana na neobavezujućim smjernicama. Prema ovom modelu, sve zainteresovane strane (bez obzira da li su iz javnog ili privatnog sektora) podstiču sa da doprinose definisanju i primjeni politike zaštite KI putem preporuka, dogovaranja i stvaranja zajedničke percepcije za ostvarivanje zajedničkog cilja. Obavezujuća snaga zakonodavnih i regulatornih odnosa koristi se samo kao dopunsko sredstvo, osim u određenim sektorima (kao što je nuklearni sektor) gjde imaju glavnu ulogu.

Drugi model je takozvani „mandatni pristup“, zasnovan na ideji da će se saradnja na polju zaštite KI najbolje postići uspostavljanjem obavezujućih pravnih okvira praćenih sankcijama za operatore KI koji ne udovoljavaju traženim

standardima u okviru zadatih rokova. U stvarnosti, države ne slijede navedene pristupe u njihovim „čistim“ oblicima, već usvajaju elemente i jednog i drugog modela. Njihovi se sistemi mogu definisati samo kao pretežno „dobrovoljni“ ili „mandatni“. Primjeri prvih su SAD, Velika Britanija, Kanada i Švajcarska, a drugih Francuska, Španija, Belgija i Estonija [5]. Za države poseban izazov predstavlja izbor najboljeg modela koji odgovara nacionalnim potrebama. To je posebno značajno prilikom uspostavljanja modela, jer se mogu usvojiti strukture i procesi koje se u praksi pokažu kao neodgovarajućim ili neadekvatnim. Iz tog razloga, države često uspostavljaju mehanizme kojima se osigurava da se politike i strategije u ovoj oblasti povremeno podvrgavaju reviziji. SAD je primjer države koja je počela sa čistim konceptom dobrovoljnog učešća operatora KI u tom procesu. Međutim, vremenom je uočena potreba za jačanjem pravnog okvira za zaštitu KI.

I pored teškoća u generalizaciji, možemo uočiti jedan trend arhitekture KI država. Uobičajeno je da se u centru zaštite nacionalne KI nalazi vladina agencija koja ima ulogu koordinatora u definisanju i sprovođenju nacionalnog strateškog pristupa zaštiti KI. Pored toga, države obično dodjeljuju odgovornost za određeni sektor pojedinim ministarstvima na osnovu utvrđene stručnosti i kompetencije (npr. bezbjednost hrane ministarstvima poljoprivrede, zdravstvo ministarstvima zdravlja i slično). S obzirom da je većina KI na nacionalnom nivou u privatnom sektoru, definiše se obim i modaliteti interakcije između uključenih vladinih agencija i operatora KI.

Na osnovu svega navedenog, a u cilju kvalitetnog zakona i podzakonskih akata CG je upoređivala Zakone i pomeute modele iz ove oblasti sa zemljama u okruženju kao i zemljama poput SAD i Velika Britanija. Pri izboru navednih država i modela rukovodili smo se određenim opštim karakteristikama Crne Gore. Prema površini teritorije i broju stanovnika Crna Gora spada u grupu malih evropskih država, sa izlaskom na more. Njena bliska prošlost vezana je za bivšu SFRJ, dok je u aktuelnom trenutku Crna Gora članica NATO saveza i nalazi se na putu da postane punopravna članica EU.

4. ZAKLJUČAK

Bez izuzetka efikasan sistem zaštite KI stvara preduslove za normalno i nesmetano funkcionisanje šireg društvenog sistema. U skladu sa tim, u Crnoj Gori se ulažu veliki napori u cilju utvrđivanja i implementacije adekvatnih mehanizama zaštite KI. Otežavajući činioci na tom planu su prije svega vezani za širok spektar vitalnih sektora koje kritična infrastruktura obuhvata, poput saobraćaja, energetike, informacionih i komunikacionih sistema, zdravstvenih službi, sistema za snabdijevanje vodom i hranom i dr. S druge strane, politika zaštite KI predstavlja jedan veoma složen sklop različitih strategija, metodologija i planova usmjerenih ka prevenciji rizika i prijetnji kao i sprečavanju većih posledica koje mogu nastati usled kriznih situacija. Kompleksnost te problematike zahtijeva jedan krajnje multidisciplinarni pristup i primjenu namjenski izrađenih alata u zaštiti KI.

Dakle, država u okviru prihvaćenih koncepta bezbijednosti mora alocirati resurse za zaštitu KI, sistem bezbjednosti mora biti prilagođen da služi zajednici. Novonastala situacija u svijetu, ali i lokalno, zahtjeva praćenje i analiziranje mnogo više rizika i prijetnji u odnosu na mnogo više objekata koji su identifikovani kao dio KI. Nova dinamika, zahtjeva novi odgovor sistema bezbjednosti, uspostavljanje novih institucija unutar sistema bezbjednosti koje će interdisciplinarnim pristupom biti u mogućnosti da što bolje analizirju trendove prijetnji po različitim kriterijima.

Implementiranje novih tehnologija mora biti sistemska djelatnost državnih institucija, ali onih koje su adaptibilne, sa proakivnim menadžmentom ljudskim resursima. Nikako se ne može očekivati da tradicionalni elementi sistema bezbjednosti budu glavni bedem obrane od novih prijetnji. Mora se dozvoliti širi zahvat u analizi problema, uključivanje obrazovnih institucija, privatnog sektora i mnogih drugih koji su direktno ili posredno involvirani u rad KI. KI su splet fizičkih i logičkih mreža i obje dimenzije su u velikoj mjeri u ekspanziji i sama ta činjenica primorava one koji se bave zaštitnom KI da sve više vremena provode u sticanju dodatnih vještina kako bi uspjeli pratiti napredak tehnologije koja se sve više i sve brže implementira u sisteme KI.

KORIŠĆENA LITERATURA

Alcaraz , C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and Challenges for the 21st century, Internationa lJournalof CriticalInfrastructure Protection, Volume 8, 54:

Alispahić, B., Kovačević, G., Korajlić, N. (n.d.). Značaj kritične infrastrukture u sustavu nacionalne sigurnosti;Fakultet Kriminalističkih nauka Sarajevo,

Marjanović, M. (2019). Teorijski i normativni okvir zaštite kritične infrastrukture u Crnoj Gori, Doktorska disertacija, Beograd.

Setola, R., Luiijf , E., & Theocharidou, M. (2019). Critical Infrastructures, Protection and Resilience, In: Setola R., Rosato V., Kyriakides E., Rome, E. (eds): Managing the Complexity of Critical Infrastructures, Springer Nature Switzerland AG, Basel, pp. 7-12.

www.mju.gov.me;