UDK: 351.78(4-672EU)(497.11)
Biblid:1451-3188, 19 (2020)
God XIX, br. 71, str. 22–37

Originalan naučni rad
Primljen 10. novembra 2019.
Odobren 29. novembra 2019.

DIREKTIVA SAVETA O UTVRĐIVANJU I OZNAČIVANJU EVROPSKE KRITIČNE INFRASTRUKTURE I PROCENI POTREBE UNAPREĐENJA NJENE ZAŠTITE

*Dalibor KEKIĆ**
*Aleksandar ČUDAN***

Apstrakt: Cilj ovog rada bio je da se ukaže na važnost kritične infrastrukture u okviru Republike Srbije i da kao takva bude prepoznata u evropskim okvirima. Prvi obrisi kritične infrastrukture prepoznaju se još u Zelenoj knjizi o evropskom programu zaštite kritične infrastrukture. Nakon toga doneseno je niz propisa koji se odnose na kritičnu infrastrukturu. Jedan od najbitnijih propisa je i Direktiva Saveta 2008/114/EZ u okviru koje je detaljno opisana procedura identifikacije i imenovanja evropske kritične infrastrukture. U okviru aktuelnog Zakona o kritičnoj infrastrukturi posebno poglavlje posvećeno je evropskoj kritičnoj infrastrukturi. Dakle, neophodno je da se u potpunosti upodobe Zakon, ali i podzakonski akti sa propisima Evropske unije (u daljem tekstu kao: EU). U tom smislu, potrebno je istražiti sve propise koji se odnose na kritičnu infrastrukturu, kako bi svi podzakonski akti u Republici Srbiji bili sistemski i sistematični, tj. da ne bi bilo kolizije. Naročitu pažnju treba obratiti na sajber-bezbednost, odnosnu informacionu mrežu, kao jednu od glavnih temelja bezbednosti kritične infrastrukture.

Ključne reči: kritična infrastruktura, bezbednost, zaštita, informaciona mreža.

1) UVOD

Svaka država, kao suštinski sadržaj, ima sopstvenu značajnu infrastrukturu a čine je sistemi, mreže, objekti i njihovi delovi. Prekid njihovog funkcionisanja, ili prekid isporuke usluga ili robe, može imati goleme posledice po nacionalnu bezbednost, zdravlje i živote ljudi, imovinu, životnu sredinu, ekonomsku koheziju, bezbednost građana i najzad ugrožavanje delovanja države. Objekti kritične

* Vanredni profesor, Kriminalističko-policijski univerzitet, dalibor.kekic@kpu.edu.rs.

** Vanredni profesor, Kriminalističko-policijski univerzitet, Zemun.

infrastrukture prevashodno podrazumevaju one objekte koji su od vitalnog značaja za državu i pretežno se misli na telekomunikacione objekte, objekte za proizvodnju i prenos električne energije, finansijski i bankarski sistem, skladište i transport nafte, gasa i drugih derivata, vodosnabdevanje, saobraćaj, ali i ostale objekte od vitalnog značaja za funkcionisanje države.[1]

Ozbiljno remećenje rada navedenih objekata vodilo bi ozbiljnim i dugoročnim oštećenjima po socijalni i ekonomski život ljudi. Uzimajući u obzir bitnost ovih objekata, njihova zaštita je od esencijalnog i predominantnog značaja za funkcionisanje i predstavlja mnogovrstan sistem bezbednosnih sredstava, ljudi i procedura koje se moraju poštovati da bi bezbednost bila na najvišem mogućem stupnju. Neke od mera, koje se neophodno moraju sprovesti, u pogledu doslednih sprovođenja mera protekcije kritične infrastrukture su: identifikovati kritičnu infrastrukturu, sačiniti mapu, razmeniti informacije sa relevantnim subjektima, osposobiti, a potom obučiti ljude i to menadžere, radnike i specijalne službe i unaprediti sistem zaštite kritične infrastrukture ili oporavak u slučaju nastanka vanredne situacije. Da bi se kritična infrastruktura sačuvala i da bi se obezbedila njena bezbednost neophodno je preduzeti niz aktivnosti.

Ono što je prvi krug obezbeđenja je zaštita okruženja objekta i postiže se kombinacijom sistema protivprovalne zaštite i video nadzora sa inteligentnom video 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.

Da bi smanjila ugroženosti kritične infrastrukture, Evropska komisija pokrenula je Evropski program za zaštitu kritične infrastrukture. Ovo je paket mera usmerenih na poboljšanje zaštite kritične infrastrukture u Evropi, u svim državama EU i u svim značajnim sektorima ekonomske aktivnosti. Inicijativa EU za zaštitu kritične informacijske infrastrukture ima za cilj da unapredi bezbednost i otpornost vitalne infrastrukturne informacione i komunikacione tehnologije (IKT). Podržavajući napore EU u zaštiti kritične infrastrukture, Zajednički istraživački centar (*Joint Research Centra* – JRC) koordinira Evropsku referentnu mrežu za zaštitu kritične infrastrukture (*European Reference Network for Critical Infrastructure Protection* – ERNCIP), pruža tehničku podršku za reviziju Direktive o evropskim kritičnim infrastrukturama i sprovodi različite istraživačke aktivnosti kao što su razvoj metoda i alate za međunarodne vežbe za sajber-bezbednost, procenu ugroženosti

[1] Vladimir Jakovljević, Jasmina Gačić, „Zaštita kritične infrastrukture u kriznim situacijama", Međunarodna naučna konferencija – *Menadžment 2012*, Mladenovac, str. 280-286.

mrežne infrastrukture u slučaju ekstremnih svemirskih vremenskih događaja i procenu otpornosti zgrada i saobraćajnih sistema na eksplozije.

2) SVRHA

Posebno poglavlje iz nadležnosti Civilne uprave za spremnost i strategije za vanredne situacije je Evropski program zaštite kritične infrastrukture. Njen opšti cilj je poboljšati zaštitu kritične infrastrukture u Evropskoj uniji. Ovaj cilj bi trebalo da bude postignut Direktivom Saveta br. 2008/114/EZ i drugim pratećim evropskim projektima (Mreža upozorenja o kritičnoj infrastrukturi – *Critical Infrastructure Warning Information Network,* Evropska referentna mreža za zaštitu kritične infrastructure – *European Reference Network for Critical Infrastructure Protection*) i finansijskim merama.

Kritična infrastruktura se može shvatiti kao objekat na kome se događa vanredna situacija, i kao takav predstavlja predmet zaštite, ali je i sredstvo koje omogućava smanjivanje opasnosti ili olakšava, odnosno omogućava otklanjanje posledica u situacijama kada je opasnost nastupila.[2] Bilo da su u pitanju napadi ili nesreće, procena rizika može pomoći u određivanju razmere sredstava koja će se rasporediti kako bi se smanjili mogući rizici ili poboljšali planovi zaštite postojećih kritičnih infrastruktura. Međuzavisnost različitih sektora dodatno otežava problem. Ipak, Zimerman je pokazao važnost ove međuzavisnosti u okviru osiguranja mreža (uključujući IKT mreže).[3]

Evropski program zaštite kritične infrastrukture (*European Programme for Critical Infrastructure Protection* – EPCIP) od 12. decembra 2006. godine postavio je opšti okvir za aktivnosti usmerene na poboljšanje zaštite kritične infrastrukture u svim zemljama EU i u svim relevantnim sektorima ekonomske aktivnosti.[4]

Četiri glavna područja fokusa EPCIP-a su:

1. Procedura za identifikaciju i imenovanje evropske kritične infrastrukture i procena potrebe za njihovim unapređenjem zaštite detaljno je obrađeno u Direktivi Saveta 2008/114/EZ;

2. Mere dizajnirane da omoguće implementaciju EPCIP-a, uključujući akcioni plan, Informaciona mreža za upozorenje na kritičnoj infrastrukturi (*Critical Infrastructure Warning Information Network – CIWIN*), upotrebu stručnih grupa

[2] Marija Mićović, „Bezbednosni aspekti funkcionisanja kritične infrastrukture u vanrednim situacijama", doktorska disertacija, Fakultet bezbednosti, 2016, str. 85.

[3] R. Zimmerman, "Decision making and the Vulnerability of Interdependent Critical Infrastructure", *CREATE Report 04-005*, Homeland Security Center, 2004, pp. 1-4.

[4] Madelene Lindström, Stefan Olsson, "The European Programme for Critical Infrastructure Protection", in: *Crisis management in the European Union: Cooperation in the face of emergencies*, Springer, pp. 37-59.

CIP (*Critical Infrastructure Protection)* na nivou EU, CIP procesa razmene informacija i identifikacije i analiza međuzavisnosti;

3. Finansiranje mera i projekata vezanih za CIP koji se fokusiraju na prevenciju, pripremljenost i upravljanje posledicama terorizma i druge rizike povezane sa bezbednošću za period 2007–2013. godine;

4. Razvoj eksterne dimenzije EPCIP.

Ključni stub ovog programa je Direktiva Saveta 2008/114 / EC od 8. decembra 2008. godine o identifikaciji i određivanju evropske kritične infrastrukture i proceni potrebe da se poboljša njihova zaštita. Ono što je ovom Direktivom definisano je kritična infrastruktura:

– „kritična infrastruktura" znači imovinu, sistem ili njihov deo koji se nalazi u državama-članicama i neophodan je za održavanje vitalnih društvenih funkcija, zdravlja, bezbednosti, zaštite, ekonomske i socijalne dobrobiti ljudi, čiji bi poremećaj rada ili čije bi uništenje, kao posledicu neuspelog održavanja tih funkcija, moglo imati znatan uticaj u državi-članici;

– „evropska kritična infrastruktura" ili „EKI" predstavlja kritičnu infrastrukturu koja se nalazi u državama-članicama, a čiji bi poremećaj u radu ili čije bi uništenje imalo znatan učinak na najmanje dve države-članice. Značaj učinka ocenjuje se u pogledu na međusektorska merila. To uključuje učinke čiji su rezultat međusektorska zavisnost od drugih vrsta infrastrukture;

Kritična infrastruktura su oni fizički i virtuelni sistemi ili agregacija sredstava koja pružaju osnovne funkcije i usluge koje podržavaju društvene, ekonomske i ekološke sisteme. Ovi sistemi se smatraju „životnom linijom" ili „kritičnom" infrastrukturom, a usluge koje pružaju smatraju se vitalnim za bezbednost, svakodnevno poslovanje, ekonomiju, zdravu i sveukupnu dobrobit modernih društava. Ovi infrastrukturni oblici se prepoznaju kao osnovna energija koja se koristi u domovima i kancelarijama, poput: pitke vode, različitih transportnih sistema, komunikacionih sistema, kao i policija koja čuva građane, ali i razne hitne službe, poput vatrogasne. Imovina, sistem ili njegov deo koji se nalazi u državama-članicama koji su od ključnog značaja za održavanje vitalnih društvenih funkcija, zdravlja, bezbednosti, ekonomskog ili društvenog blagostanja, a čije bi narušavanje ili uništavanje imalo značajan uticaj na državu-članicu kao rezultat neuspeha u održavanju tih funkcija.

Direktiva Saveta 2008/114/EZ zahteva od država-članica da identifikuju i imenuju evropsku kritičnu infrastrukturu u cilju poboljšanja njene zaštite. Ovo je takođe pokrenulo nekoliko država-članica da identifikuju nacionalnu kritičnu infrastrukturu i sektore, promovišući dodatne mere bezbednosti koje treba da se primene.[5]

[5] Setola, R., Luiijf, E., & Theocharidou, M. "Critical infrastructures, protection and resilience", in R. Setola, V. Rosato, E. Kyriakides, & E. Rome (Eds.), *Managing the Complexity of Critical Infrastructures,* Studies in Systems, Decision and Control*,* Vol. 90, 2016, pp. 1-18.

Proces pregleda trenutnog EPCIP-a, sproveden kao bliska saradnja sa državama-članicama i drugim zainteresovanim stranama, otkrio je da nije bilo dovoljno razmatranja veza između kritične infrastrukture u različitim sektorima, niti u prekograničnoj saradnji. Da bismo pravilno zaštitili našu kritičnu infrastrukturu i kako bismo izgradili svoju otpornost, potreban je bio novi pristup koji bi se uhvatio u koštac sa tim jazom i tim problemima. Da bi se implementirao novi pristup, Komisija je počela sa radom sa četiri kritične infrastrukture evropske dimenzije: Evrokontrol (EU menadžer za upravljanje vazdušnim saobraćajem – *Eurocontrol: EU Air Traffic Management Network Manager*), Galileo, mreža za prenos električne energije i mreža za prenos gasa.

Informaciona mreža za upozorenje na kritičnoj infrastrukturi (*Critical Infrastructure Warning Information Network* – CIWIN) pruža internetski višestepeni sistem za razmenu kritičnih ideja o zaštiti infrastrukture, studije i dobre prakse. Portal CIWIN, koji je pokrenut od sredine januara 2013. godine, takođe služi kao skladište za CIP informacije. Razmena brzih informacija o potencijalnim pretnjama i ranjivostima igra presudnu ulogu. Kao takvo, bilo je očigledno da je potrebna određena mreža: ovaj zadatak je dodeljen Informacionoj mreži za upozorenje na kritičnoj infrastrukturi. Ova mreža ispunjava dve funkcije. To je, pre svega, elektronski forum za razmenu informacija u vezi sa zaštitom kritične infrastrukture. Služi kao instrument za brzo upozoravanje između država-članica radi informisanja Komisije o uobičajenim rizicima i pretnjama. Sve države članice potpisale su memorandum o razumevanju kako bi doprinele operativnom učešću u mreži. Način na koji se te informacije moraju osigurati još se razmatra. Treba napomenuti da se, što se tiče civilne zaštite, pomoć može zatražiti preko Centra za nadgledanje i informisanje civilne zaštite (*Civil Protection Monitoring and Information Centre*): sistem upozorenja Evropske komisije koji omogućava ljudima da koordiniraju međusobnu pomoć i saradnju između država članica u slučaju većih hitnih slučajeva.

Radni dokument Komisije o novom pristupu evropskom programu za zaštitu kritične infrastrukture usvojen je 28. avgusta 2013. godine. Ovaj dokument iznosi revidiran i praktičniji pristup implementaciji Evropskog programa zaštite kritične infrastrukture (EPCIP). Dokumentom se omogućava analiza stanja elemenata programa i predlaže preoblikovani pristup programu zaštite kritične infrastrukture EU, zasnovan na praktičnoj primeni aktivnosti u okviru prevencije i radnih aktivnosti za spremnost i odgovor. Deo novog pristupa je posmatranje međuzavisnosti između kritične infrastrukture, industrije i državnih institucija. Pretnje u okviru jedne kritične infrastrukture mogu imati veoma značajan uticaj na širok spektar aktera u različitim infrastrukturama, ali i šire. Naravno, efekti tih međuzavisnosti nisu ograničeni na pojedine zemlje. Mnoge kritične infrastrukture imaju prekograničnu dimenziju. Pored međuzavisnosti između sektora, postoje i mnoge međuzavisnosti unutar istog sektora, ali obuhvata i brojne evropske zemlje, kao što je npr. međusobno povezane nacionalne visokonaponske elektroenergetske mreže.

3) MERE EU

U novije vreme, Direktiva (EU) 2016/1148 o bezbednosti na mrežama i informacionoj bezbednosti (*Network and Information Security Directive* – NIS Directive) podstakla je povećani nivo bezbednosti u mrežama i informacionim sistemima. Štaviše, finansiranje istraživanja u programu Horizon 2020 bavi se temama kao što su zaštita obaveštajnih podataka, bezbednost saobraćaja i energetskih sistema i kibernetska bezbednost.

Komunikacijom Komisije Savetu i Evropskom parlamentu – Zaštita kritične infrastrukture u borbi protiv terorizma (COM/2004/0702 final) navedeno je šta se to sve uračunava u kritičnu infrastrukturu: energetske instalacije i mreže, komunikacije i informaciona tehnologija, finansije, briga o zdravlju, hrana, pitka voda, transport, proizvodnja, transport i skladištenje opasnih materija i vladine institucije. Ova infrastruktura je u vlasništvu i njom upravljaju i javni i privatni sektor. Međutim, u svom saopštenju 574/2001 od 10. oktobra 2001. godine, Komisija je izjavila: „Jačanje nekih bezbednosnih mera od strane državnih vlasti nakon napada usmerenih na društvo u celini, a ne na industrijske aktere, mora da snosi država". Javni sektor stoga mora igrati ključnu ulogu.

U okviru Evropskog programa zaštite kritične infrastrukture pomenuto je 11 sektora sa 37 povezanih usluga i identifikovano je kao kritična infrastruktura. Predlog direktive na kraju je zadržao 11 sektora i 29 podsektora. Sama direktiva pominje samo dva sektora (energetika i transport) i 8 podsektora. Štaviše, inicijalna odgovornost za zaštitu kritične infrastrukture ostaje nacionalna. Pored ovih sektora, EU je svesna da se Zajednička infrastruktura može geografski nalaziti izvan teritorije EU. Ovo ukazuje na značaj nafte i gasovoda koji snabdevaju EU: susedni objekti EU su od presudne važnosti za snabdevanje njene ekonomije. Uništavanje ili sabotaža te infrastrukture u potencijalno nestabilnim regionima mogla bi imati neviđene posledice za Evropsku uniju.[6]

Mora se priznati da sve države članice ne napreduju istim tempom i na isti način ne sprovode ove direktive. Shodno tome, od najvećeg je značaja da se postigne evropska koordinacija kako bi se ispunili ciljevi navedeni u akcionom planu. Agencija Evropske unije za bezbednost mreže i informacija (*European Union Agency for Network and Information Security – ENISA*) je telo EU osnovano 2004. godine za obavljanje vrlo specifičnih tehničkih i naučnih zadataka u oblasti mrežne i informacione bezbednosti. Ovaj posao se obavlja samo u okviru „domena Zajednice" („prvi stub" i na unutrašnjem tržištu EU): kao „Agencija Evropske zajednice".[7] Misija

[6] Bart Smedts, "Critical infrastructure protection at the European level", *Studia diplomatica*, Egmont Institute, LXIV-1, 2011, pp. 71-78.

[7] Aikaterini Poustourli, David Ward, Angelos Zachariadis, et al., "An Overview of European Union and United States Critical Infrastructure Protection Policies", 12th International conference on *Standardization, Protypes and Quality: A Means of Balkan Countries' collaboration*, Kocaeli University İzmit, Kocaeli, Turkey, 2015.

ENISA je od suštinske važnosti za postizanje efektivnog i efikasnog nivoa sigurnosti mreže i informacija u okviru EU. Zajedno sa institucijama EU i državama-članicama, ENISA nastoji razviti kulturu mrežne i informatičke sigurnosti za dobrobit građana, potrošača, preduzeća i organizacija javnog sektora u Evropskoj uniji. ENISA pomaže Evropskoj komisiji, državama-članicama i poslovnoj zajednici da se pozabave, odgovore i posebno u sprečavanju problema u vezi sa mrežom i informacijom. Agencija, takođe, pomaže Evropskoj komisiji u tehničkom pripremnom radu za ažuriranje i razvoj zakonodavstva Zajednice u oblasti bezbednosti mreža i informacija. ENISA je osnovana Uredbom (EZ) br. 460/2004, gde se njen trenutni regulatorni okvir sastoji od Uredbe (EU) br. 526/2013. Predlog nove Uredbe o ENISA, kojom se stavlja van snage Uredba (EU) 526/2013 i o sertifikovanju o sajber bezbednosti informacione i komunikacione tehnologije („Zakon o kibernetskoj bezbednosti"), obećavaju prodavnicu Agencije i poboljšavaju njene mogućnosti i kapacitete u cilju postizanja sajber bezbednosti, otpornosti i bolje podrške državama-članicama. U decembru 2018. Evropska komisija, Evropski parlament i Savet Evropske unije postigli su politički dogovor o Zakonu o kibernetskoj bezbednosti.[8] U martu 2019. Evropski parlament usvojio je Zakon o kibernetskoj bezbednosti (*Cyber Security Act*). Ova nova EU uredba daje ENISA stalni mandat i jača njegovu ulogu. Zakon, takođe, uspostavlja EU okvir za sertificiranje kibernetske sigurnosti, pojačavajući sajber sigurnost digitalnih proizvoda i usluga u Evropi.

Ukratko, Zakon o kibernetskoj bezbednosti:

- jača ENISA tako što je agenciji dodelio stalni mandat, ojačavajući njene finansijske i ljudske resurse, i uopšte ojačavajući svoju ulogu u podršci EU da postigne zajednički i visok nivo sajber bezbednosti;
- uspostavlja prvi okvir sertifikovanja kibernetske bezbednosti u celoj EU da bi se osigurao zajednički pristup sertifikovanju kibernetske bezbednosti na unutrašnjem evropskom tržištu, i na kraju poboljšala kibernetska bezbednost u širokom spektru digitalnih proizvoda i usluga.

4) SADRŽAJ DOKUMENATA

Zelena knjiga o evropskom programu zaštite kritične infrastukture (*Green Paper on a European programme for critical infrastructure protection* – COM(2005) 576 final) od 17.11.2005. godine definiše pojam evropske kritične infrastrukture i njom se podrazumeva obuhvat onih fizičkih resursa, usluga, objekata informacione tehnologije, mreža i imovine infrastrukture koji bi, ako bi bili poremećeni ili

[8] Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", *Computer Law & Security Review: The International Journal of Technology Law and Practice*, https://doi.org/10.1016/j.clsr.2019.06.007, pristupljeno 11/11/2019.

uništeni, imali ozbiljan uticaj na zdravlje, bezbednost, ekonomsku ili socijalnu dobrobit:

(a) dve ili više država članica – to bi uključivalo određenu bilateralnu kritičnu infrastrukturu (gde je relevantno);

(b) uključuju tri ili više država članica – to bi isključilo sve bilateralne kritične infrastrukture.

Dokumentom je potvrđeno prepoznavanje tri grupe infrastrukturnih dobara:

- Javna, privatna i vladina infrastrukturna dobra i međusobno zavisne sajber i fizičke mreže;
- Postupci i gde su relevantni pojedinci koji vrše kontrolu nad kritičnim funkcijama infrastrukture;
- Objekti koji imaju kulturni ili politički značaj, kao i „meke mete" koje uključuju masovne događaje (tj. sportske, zabavne i kulturne sadržine).

Zelenom knjigom su ponuđena moguća rešenja za uspostavljanje programa i ustrojavanje Informacione mreže za uzbunjivanje vezano uz kritičnu infrastrukturu. U odgovorima pristiglima na Zelenu knjigu naglašavala se dodatna vrednost okvira Zajednice s obzirom na zaštitu kritične infrastrukture.

Komunikacija Komisije o evropskom programu zaštite kritične infrastrukture (Communication From the Commission on a European Programme for Critical Infrastructure Protection – COM (2006) 786 final) od 12.12.2006. godine o Akcionom planu EPCIP organizuje aktivnosti povezane sa zaštitu kritične infrastrukture u okviru tri radna toka:

- Tok rada 1 koji će se baviti strateškim aspektima EPCIP-a i razvojem mera koje se horizontalno primenjuju na sve aktivnosti u zaštiti kritične infrastrukture;
- Tok rada 2 koji se bavi evropskim kritičnim infrastrukturama i implementiran je na sektorskom nivou;
- Tok rada 3 koji će pružiti podršku državama-članicama u njihovim aktivnostima koje se tiču nacionalne kritične infrastrukture.

Dijalog sa zainteresovanima je ključan za poboljšanje zaštite kritične infrastrukture u EU. Tamo gde je potrebna posebna ekspertiza Komisija može osnovati ekspertske grupe CIP-a na nivou EU, kako bi se bavila jasno definisanim pitanjima i olakšala dijalog između javnog i privatnog sektora o zaštiti kritične infrastrukture.

Direktiva Saveta 2008/114/EZ od 8. decembra 2008. o utvrđivanju i označivanju evropske kritične infrastrukture i proceni potrebe poboljšanja njene zaštite. Ova Direktiva predstavlja prvu meru u postupnom pristupu s ciljem utvrđivanja i označivanja Evropske kritične infrastrukture i proceni potrebe njene zaštite. Direktiva je usredsređena na sektore energije i saobraćaja. Njen opseg

primene se odnosi i na druge sektore, pored ostalog, sektor informaciono-komunikacione tehnologije.[9]

Radni dokument članova Komisije o novom pristupu Evropskom programu zaštite kritične infrastrukture, kroz povećanje bezbednosti evropskih kritičnih infrastruktura od 28.8.2013. godine (SWD (2013) 318 final), sadrži revidiranu i praktičniju primenu evropskog programa zaštite kritične infrastrukture.[10] U tom kontekstu, ovim dokumentom dat je prikaz u kojoj je meri taj uticaj uzet u obzir u trenutnom planiranju zaštite kritične infrastrukture i kako se razmatranje međuzavisnosti može poboljšati. Utvrđeno je manje od 20 evropskih kritičnih infrastruktura i izrađeno je vrlo malo novih planova bezbednosti operatora. Neke jasne kritične infrastrukture evropske dimenzije, kao što su glavne mreže za prenos energije, nisu obuhvaćeni ovim planovima. Predložena Uredba kojom se uspostavlja instrument za stabilnost – instrument spoljne saradnje – omogućava pomoć u zaštiti kritične infrastrukture u trećim zemljama, u oblastima međunarodnog transporta (vazduhoplovstva i pomorstva), energetskih operacija i distributivne infrastrukture i elektronskih informacija i komunikacione mreže (sajber-bezbednost).[11]

Direktiva (EU) 2016/114 Evropskog parlamenta i Saveta, od 6. jula 2016, o merama za visoki zajednički nivo bezbednosti mrežnih i informacionih sistema širom Unije, utvrđuje da postojeće sposobnosti nisu dovoljne za osiguranje visokog stepena bezbednosti mrežnih i informacionih sistema unutar Unije. Države-članice imaju vrlo različite nivoe pripravnosti, što je dovelo do postojanja raznolikih pristupa širom Unije. Da bi se postigao i održao visok nivo bezbednosti mrežnih i informacionih sistema, svaka država-članica trebala bi da ima nacionalnu strategiju za bezbednost mrežnih i informacionih sistema u kojoj će biti definisani strateški ciljevi i konkretna politička aktivnost koju treba preduzeti.[12]

Direktiva se fokusira na tri prioriteta: (a) spremnost država-članica – zahtevajući od njih da se na odgovarajući način opreme, npr. putem računarskog tima za odgovor na nezgode i nadležnog nacionalnog organa; (b) saradnjom svih država članica – osnivanjem grupe za saradnju u cilju podrške i olakšavanja

[9] "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", *OJ L* 345, 23.12.2008, pp. 75-82.

[10] European commission, "Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure", https://ec.europa.eu/transparency/regdoc/rep/10102/2013/EN/10102-2013-318-EN-F1-1.PDF, pristupljeno: 20.10.2019. godine.

[11] COM(2011) 845 final.

[12] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", *OJ L 194, 19.7.2016,* pp. 1-30.

strateške saradnje i razmene informacija među državama-članicama; (c) kultura sigurnosti između sektora koji su od vitalnog značaja za našu ekonomiju i društvo i koji se u velikoj meri oslanjaju na IKT, poput energije, transporta, vode, bankarstva, infrastrukture finansijskog tržišta, zdravstvene zaštite i digitalne infrastrukture.[13]

Direktiva 2008/114/ES je osnova za naredne korake u definisanju kriterijuma za kritičnu infrastrukturu. U aneksu III ove Direktive navedene su procedure, koje svaka zemlja-članica treba da primeni, kroz nekoliko konsekventnih koraka:

- korak 1: svaka zemlja-članica treba da primeni sektorske kriterijume radi kreiranja inicijalne selekcije kritične infrastrukture u okviru sektora;
- korak 2: svaka zemlja-članica treba da primeni definiciju kritične infrastrukture, na potencijalne evropske kritične infrastrukture identifikovane nakon koraka 1. Značaj učinka određuje se upotrebom nacionalnih metoda za utvrđivanje kritične infrastrukture ili upućivanjem na unakrsne, međusektorske kriterijume, na odgovarajućem nacionalnom nivou. Za infrastrukture koje se koriste za pružanje osnovnih servisa treba uzeti u obzir dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa;
- korak 3: svaka zemlja-članica treba da implementira prekogranični element za definisanje evropske kritične infrastrukture na potencijalne evropske kritične infrastrukture koje su prošle prva dva koraka ove procedure. Za potencijalnu evropsku kritičnu infrastrukturu koja zadovoljava definiciju primenjuje se sledeći korak procedure. Za infrastrukture koje se koriste za pružanje osnovnih servisa, treba uzeti u obzir dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa;
- korak 4: svaka zemlja-članica treba da primeni unakrsne, međusektorske kriterijume za preostale evropske kritične infrastrukture. Unakrsni, međusektorski kriterijum treba da uzme u obzir: ozbiljnost napada, i za infrastrukture koje se koriste za pružanje osnovnih servisa dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa. Ukoliko potencijalna evropska kritična infrastruktura ne ispunjava unakrsne, međusektorske kriterijume smatraće se da nije evropska kritična infrastruktura.[14]

Zaštita komunikacija Evropskom parlamentu i Savetu – Zajednički okvir za suzbijanje hibridnih pretnji – odgovor Evropske unije navodi da je važno zaštititi kritičnu infrastrukturu, jer bi nekonvencionalan napad na bilo koju „meku metu" koji bi izvršili učinioci hibridnih pretnji mogao dovesti do ozbiljnih privrednih ili

[13] Roberto Setola, Eric Luiijf, Marianthi Theocharidou, "Critical Infrastructures, Protection and Resilience", *Studies in Systems, Decision and Control*, Volume 90, 2016, pp. 1-18.

[14] Mirko Škero, Vladimir Ateljević, „Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa Direktivom Saveta Evrope 2008/114/ES", *Vojno delo*, 3/2015, 2015, str. 192-207.

društvenih problema.[15] Kako bi se zaštitila kritična infrastruktura, Evropskim programom zaštite kritične infrastrukture omogućava se međusektorski sistemski pristup utemeljen na svestranom razmatranju rizika, uzimajući u obzir međuzavisnosti na temelju izvođenja mera u okviru područja delovanja koja se odnose na sprečavanje, pripravnost i odgovor. Mera koja se predlaže ovim dokumentom je da će Komisija, u saradnji sa državama-članicama i zainteresovanim stranama, utvrditi zajedničke alate, uključujući pokazatelje, s ciljem poboljšanja zaštite i otpornosti kritične infrastrukture na hibridne pretnje u relevantnim sektorima. Takođe, Komisija će u saradnji sa državama-članicama podupirati nastojanja za diverzifikacijom izvora energije i unaprediti standarde bezbednosti kako bi se pojačala otpornost nuklearne infrastrukture.

Zaštita komunikacija Evropskom parlamentu i Savetu – Otpornost, odvraćanje i odbrana: jačanje sajber bezbednosti EU predočava da Agencija Evropske unije za mrežu i informacionu bezbednost (ENISA) ima ključnu ulogu u jačanju sajber otpornosti i odgovora EU-a na sajber napade, ali ograničava je postojeći mandat. Komisija stoga predstavlja ambiciozan predlog reforme koji uključuje trajni mandat agencije. Bezbednost sredstava informaciono-komunikacione tehnologije je od važnosti za evropsku kritičnu infrastrukturu, jer je ona osnov i temelj svih ostalih oblika kritične infrastrukture. Razvoj jedinstvenog tržišta EU-a zavisi i od uključivanja sajber bezbednosti u trgovinsku politiku i politiku ulaganja. Zbog sajber bezbednosnih zahteva, više trećih zemalja već je uvelo prepreke trgovini robom i uslugama iz EU-a u važnim sektorima. Okvirom EU-a, sajber-bezbednosna sertifikacija dodatno je ojačala međunarodni položaj.[16]

Zajednička komunikacija Evropskom parlamentu, Evropskom savetu i Savetu – Jačanje otpornosti i povećanje sposobnosti za odgovor na hibridne pretnje odnosi se na aktivnosti državnih i nedržavnih aktera, koje i dalje predstavljaju ozbiljnu i akutnu pretnju za EU i njegove države-članice. Sve su češći pokušaji destabilizacije zemalja narušavanjem poverenja javnosti u državne institucije te dovođenjem u pitanje temeljnih vrednosti društava.

Hibridne su kampanje višedimenzionalne te se u njima istovremeno primenjuju prisilne i subverzivne mere uz upotrebu konvencionalnih i nekonvencionalnih alata i taktika (diplomatskih, vojnih, privrednih i tehnoloških) za destabilizaciju

[15] Joint communication to the European parliament and the council, Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52016JC0018, pristupljeno: 20.10. 2019. godine.

[16] Joint communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017JC0450, pristupljeno: 20.10.2019. godine.

protivnika. U Zajedničkom okviru za suzbijanje hibridnih pretnji – odgovor Evropske unije iz aprila 2016. godine podstaknut je pristup na svim nivoima uprave, te su navedena 22 područja delovanja u nastojanju da se suzbiju hibridne pretnje i ojača otpornost EU, država-članica i međunarodnih partnera.

Kad je reč o sajber bezbednosti, 9. maj 2018. godine bio je važna prekretnica jer su dotad sve države članice EU morale preneti prvi pravno obavezujući skup pravila o sajber bezbednosti na nivou EU: Direktivu o bezbednosti mrežnih i informacionih sistema. To je važan deo šireg pristupa utvrđenog u Zajedničkoj komunikaciji iz septembra 2017. – „Otpornost, odvraćanje i odbrana: jačanje sajber bezbednosti u Evropi", u kojoj se navode dalekosežne konkretne mere za vanredno poboljšanje sajber bezbednosnih struktura i sposobnosti u EU.[17] Komisija i Visoki predstavnik doneli su i predložili niz inicijativa za odgovaranje na izazove koje donose hibridne pretnje. Komisija ujedno ubrzava provedbu Akcionog plana iz 2017. godine za poboljšanje spremnosti s obzirom na rizike za hemijsku, biološku, radiološku i nuklearnu bezbednost. Svrha ove Zajedničke komunikacije je izvestiti Evropski savet o radu, te utvrditi područja u kojima bi trebalo pojačati delovanja kako bi se dodatno produbio i ojačao ključni doprinos EU suočavanju s tim pretnjama.[18]

5) DALJI SMEROVI RAZVOJA

Strateška agenda za 2019–2024. godinu, koju je u junu usvojio Savet Evrope zahteva sveobuhvatan pristup zaštiti Evrope od zlonamernih sajber aktivnosti i hibridnih pretnji. Evropska komisija procenila je Direktivu iz 2008. o zaštiti kritične infrastrukture. Procena pokazuje razvoj pretnji sa kojima se Evropa suočava. Evaluacija takođe naglašava da pristup EU u zaštiti kritične infrastrukture mora biti fleksibilan i zasnovan na riziku kako bi se odrazile pretnje i ranjivosti s kojima će se kritične infrastrukture verovatno suočavati u narednim decenijama. Procena je sugerisala da postoje dodatni sektori za koje države članice smatraju da su vredne dodatnih zaštitnih akcija na evropskom nivou. Na osnovu nalaza evaluacije postoje razlozi za ispitivanje opsega okvira kritične infrastrukture EU s ciljem da se obuhvate i dodatni sektori.

Postoje zabrinutosti da bi imenovanje finansijskih usluga kao kritične infrastrukture moglo navesti države-članice da sve više proglašavaju finansijsku regulativu pitanjem nacionalne bezbednosti, čime bi narušavale ciljeve unutrašnjeg tržišta. Iako je zabrinutost za ovaj oblik, s obzirom na kritičnu ulogu finansijskog sektora i promene u evropskom bezbednosnom okruženju, čini se da je potrebno

[17] JOIN(2017) 450 final.

[18] Joint communication to the European parliament, the European Council and the Council, Increasing resilience and bolstering capabilities to address hybrid threats, JOIN/2018/16 final.

da se pronađu načini za rešavanje kritičnih bezbednosnih pitanja u politici finansijskih usluga EU, istovremeno čuvajući integritet internog tržišta finansija. Rešavanje otpornosti finansijskog sektora deo je izazova otpornosti na nivou celog društva. Savremeno društvo karakteriše mreža složenih međuzavisnosti, a u samom srcu toga je finansijski sektor. Finansijske usluge zavise o kontinuitetu drugih delova kritične infrastrukture poput telekomunikacija i energije. Takve međusobne veze idu u oba smera, a velike poremećaje u bilo kojem od ovih sektora imaće ozbiljne posledice u ostalim.

Sigurnost regionalno relevantne kritične infrastrukture je i dalje opasno fragmentirana, a teroristički napadi, kriminalne aktivnosti ili čak destabilizacije koje sponzoriše država mogu predstavljati, naročito u sajber prostoru, ozbiljne pretnje integritetu zajedničkog civilnog društva ako iskoriste nedostatke predstavljene u obaveštajnim, odbrambenim i upravljačkim sistemima pojedinačnih nacionalnih institucija koje su i dalje odgovorne za zaštitu svih objekata. Prihvatajući teoriju da domen karakteriše neprekidna aktivnost, koja se odvija uglavnom pod pragom formalne definicije ratnog čina, i da je potrebna strategija stalnog prisustva za kontrolu i uticaj na događaje, jasno je da bilo kakvo odlaganje u razumevanju događaja, komunikacija ili koordinacija mogu biti fatalni. Iz tog razloga je potreban poboljšani evropski pristup. Trebalo bi da se zasniva na pogodnijem tumačenju principa supsidijarnosti i, shodno tome, konstituisanja regionalnih bezbednosnih čvorišta kritične infrastrukture, tamo gde je to neophodno.

Po mišljenju Larisa Gajzera, EU bi trebalo da pokrene pilot projekat, na primer, u regionu poput Centralne Evrope koju obeležavaju brojne zemlje povezane zajedničkom kritičnom infrastrukturom, a koji bi omogućio razvoj novih sposobnosti radi boljeg jamčenja stabilnosti na zajedničkom tržištu i unapređenje bezbednosti države-članice. Stabilnost i otpornost postižu se oblikovanjem novog sistema upravljanja sajber bezbednošću koji se zasniva na regionalnim sajber ekosistemima koji deluju autonomno u cilju efikasnog predviđanja potencijalnih poremećaja.[19]

6) ZNAČAJ ZA REPUBLIKU SRBIJU

Akcionim planom za pregovaračko poglavlje 24 – „Pravda, sloboda i bezbednost", tačkom 7 „Borba protiv terorizma" predviđa se lanac aktivnosti, među kojima je usaglašavanje sa Direktivom 2008/114/EC. U toku je izrada predloga zakonodavnog okvira za identifikaciju, određivanje i zaštitu kritične infrastrukture u Republici Srbiji. S tim u vezi, donet je Zakon o kritičnoj infrastrukturi[20] iz kojeg proističe potreba

[19] Laris Gaiser, "European Critical Infrastructure Protection: The Need For a Regional Approach and a Cyber Constant Contact Strategy", *National Security and The Future*, 1-2 (19), 2018, pp. 45-63.

[20] Zakon o kritičnoj infrastrukturi, *Službeni glasnik Republike Srbije* 87/18.

donošenja podzakonskih akata u roku od šest meseci od stupanja na snagu. Zakon o kritičnoj infrastrukturi upućuje na donošenje tih podzakonskih akata, a samim zakonom je uređeno pitanje nacionalne i evropske kritične infrastrukture.

Evropsku kritičnu infrastrukturu na teritoriji Republike Srbije, na predlog Ministarstva unutrašnjih poslova, određuje Vlada na zahtev i u saglasnosti sa zainteresovanim državama članicama Evropske unije i obaveštava zainteresovane države članice o određivanju evropske kritične infrastrukture na teritoriji Republike Srbije. Ministarstvo unutrašnjih poslova, u vezi sa kritičnom infrastrukturom, organizovalo je Projektnu grupu koja je zadužena da u što kraćem roku donese sistem podzakonskih akata.

7) ZAKLJUČAK

Danas su kritične infrastrukture regionalno povezane. Bezbednost i stabilnost zemalja svakodnevno se više oslanjaju na međunarodnu saradnju i to bi trebalo biti još pouzdanije u okviru EU. Nedavno je EU dala opštu definiciju kritične infrastrukture i predložila Evropski program zaštite kritične infrastrukture. Teži se pružanju međusektorskog pristupa za sve rizike, a podržava ga redovna razmena informacija između država EU u okviru sastanaka kontaktnih tačaka CIP-a. EPCIP je osnovni za našu zajedničku sigurnost na tržištu, ali analizirajući najsavremeniju tehnologiju ovaj dokument će pokušati da pokaže da EPCIP nema u potpunosti efikasnu zaštitu kritične infrastrukture i tako će predložiti EU model saradnje zasnovan na regionalnim pristupima. Jedinstvena koordinacija nekoliko regionalnih okvira kritične infrastrukture mogla bi predstavljati efikasno i efektivno rešenje, sprovedeno na principu supsidijarnosti EU, izbegavajući prekomernu birokratiju.

Svaki pravni okvir ima svoje ciljeve i svrhe i uspostavlja svoje mehanizme za njihovo postizanje. Njihova se perspektiva takođe značajno razlikuje: sajber-bezbednost, za razliku od zaštite podataka, pojedincima u suštini ne daje nikakva prava. Bez obzira na izbor pravnog instrumenta, EU nudi dobro osmišljen i uravnotežen odgovor koji uzima u obzir problem (kibernetske bezbednosti) i planove za budućnost. On uspostavlja nova, stalna, nadležna tela na nivou države-članice i uvodi sistem međuevropske saradnje. Postoje zabrinutosti oko toga da li je skup identifikovanih evropskih kritičnih infrastruktura kompletan, pošto se čini da imovina panevropskih usluga nije temeljno procenjena kao potencijalna Evropska kritična infrastruktura, dok je otvoreno prepoznato da su glavne mreže za prenos energije (gas, struja) prekogranično dimenzionisane. Trenutni postupak imenovanja Evropske kritične infrastrukture ne odgovara na ovaj izazov, jer mere zaštite ne mogu biti proizvod jedne države-članice ili operatera.

Sa druge strane, pregled je ostavio utisak da su uopšte povećana svest o Evropskoj kritičnoj infrastrukturi i nivo saradnje u EU u energetskom i transportnom sektoru, kroz različite aktivnosti i forume, organizovane u skladu sa

Direktivom. Međutim, zasluga za poboljšanu svest i saradnju nije u potpunosti zaslužna za Direktivu i EPCIP, jer su i ostale sektorske inicijative, na primer u oblasti bezbednosti vazduhoplovstva, igrale važnu ulogu.[21]

Vremenom je bezbednost postala relevantna i naglašena zbog tehnoloških trendova. Ovo je učinilo da se sektor kritične infrastrukture učini lako podložnim napadima. Nakon što su postali tako čvrsto povezani i međuzavisni, incidenti pokazuju da kompromis, poremećaj i neuspeh međunarodnih uprava nije ograničen samo na uzroke i vektore vezane za prirodne katastrofe. Akcije koje ljudi pokreću zloupotrebom tehnologije ili malverzacijama imaju sve veći uticaj.

Snažno partnerstvo između javnog i privatnog sektora je važno, i obe grupe zainteresovanih strana treba energično da ga realizuju da bi se postigla veća sigurnost i otpornost na CI-ima. Takva saradnja može osnažiti javni sektor da blagovremeno i efikasno nadgleda i objedinjava informacije o bezbednosnim pretnjama, ugroženostima, incidentima i uticajima CI-a kako se pojave. Javni sektor, takođe, može da pruži informacije o riziku operatorima privatnog sektora kako bi im pomogao da obezbede informisano i dobro organizovano upravljanje sigurnošću.

7) LITERATURA

Döbbeling, Ernst-Peter, "Programs and Trends in Critical Infrastructure Protection in the EU", *National Critical Infrastructure Protection Regional Perspective Conference*, Faculty of Security Studies, 2013, pp. 106-118.

Gaiser, Laris, "European Critical Infrastructure Protection: The Need For a Regional Approach and a Cyber Constant Contact Strategy", *National Security and The Future*, 1-2 (19), 2018, pp. 45-63.

Jakovljević, Vladimir, Gačić, Jasmina, „Zaštita kritične infrastrukture u kriznim situacijama", Međunarodna naučna konferencija, *Menadžment 2012*, Mladenovac, str. 280-286.

Lindström, Madelene, Olsson, Stefan, "The European Programme for Critical Infrastructure Protection", in: *Crisis management in the European Union: Cooperation in the face of emergencies*, Springer, pp. 37-59.

Markopoulou, Dimitra, Papakonstantinou, Vagelis and Paul de Hert, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", *Computer Law & Security Review: The International Journal of Technology Law and Practice*.

[21] Ernst-Peter Döbbeling, "Programs and Trends in Critical Infrastructure Protection in the EU", *National Critical Infrastructure Protection Regional Perspective*, Faculty of Security Studies, 2013, pp. 106-118.

Mićović, Marija, „Bezbednosni aspekti funkcionisanja kritične infrastrukture u vanrednim situacijama“, doktorska disertacija, Fakultet bezbednosti, 2016.

Poustourli, Aikaterini, Ward, David, Zachariadis, Angelos et al., “An Overview of European Union and United States Critical Infrastructure Protection Policies”, 12th International conference on *Standardization, protypes and quality: a means of balkan countries' collaboration*, Kocaeli University İzmit, Kocaeli, Turkey, 2015.

Setola, R., Luiijf, E., & Theocharidou, M., “Critical infrastructures, protection and resilience”, in R. Setola, V. Rosato, E. Kyriakides, & E. Rome (Eds.), *Managing the Complexity of Critical Infrastructures,* Studies in Systems, Decision and Control*,* Vol. 90, 2016, pp. 1-18.

Smedts, Bart, “Critical infrastructure protection at the European level”, *Studia diplomatica*, LXIV-1, 2011, pp. 71-78.

Škero, Mirko, Ateljević, Vladimir, „Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa Direktivom Saveta Evrope 2008/114/ES“, *Vojno delo*, 3/2015, str. 192-207.

Zimmerman, R., “Decision making and the Vulnerability of Interdependent Critical Infrastructure”, *CREATE Report 04-005*, Homeland Security Center, pp. 1-4, 2004.

COUNCIL DIRECTIVE ON THE ESTABLISHMENT AND MARKING OF EUROPEAN CRITICAL INFRASTRUCTURE AND ASSESSMENT OF THE NEED TO IMPROVE ITS PROTECTION

Summary: The paper aimed to highlight the importance of critical infrastructure for the Republic of Serbia and recognize it as such within the European framework. The first outlines of critical infrastructure are recognized in the Green Paper on a European Critical Infrastructure Protection Program. Subsequently, a series of regulations were passed concerning critical infrastructure. Within the framework of the current Critical Infrastructure Law, a special chapter is devoted to European Critical Infrastructure. Therefore, it is necessary to fully approximate the law, as well as the legal acts with the EU regulations. In this regard, it is necessary to investigate all regulations related to critical infrastructure, so that all by-laws in the Republic of Serbia are systematic, i.e., to avoid a collision. Particular attention should be paid to cyber security, the related information network, as one of the main pillars of critical infrastructure security.

Keywords: critical infrastructure, security, protection, information network.