**F. Mehović***

# RAZLOZI NEPRIHVAĆANJA ZAKONA O KRITIČNIM INFRASTRUKTURAMA U BOSNI I HERCEGOVINI

UDK: 351.78(497.6)
PRIMLJENO: 9.12.2024.
PRIHVAĆENO: 18.3.2025.



*SAŽETAK: Bosna i Hercegovina suočava se s ozbiljnim posljedicama neusvajanja zakona o kritičnim infrastrukturama na državnoj razini, što ugrožava sigurnost i stabilnost ključnih sektora. Ovaj zakon je ključan za identifikaciju, zaštitu i otpornost sektora poput energetike, transporta i komunikacija. Nedostatak jedinstvenog zakonodavnog okvira otežava koordinaciju između razina vlasti i povećava rizik od prirodnih i sigurnosnih prijetnji. U radu se analiziraju politički razlozi neprihvaćanja zakona, posljedice za infrastrukturu i mogućnosti prilagođavanja EU standardima. Fokus je stavljen na sigurnosne implikacije, uključujući ranjivost na kibernetičke prijetnje i otežanu međunarodnu suradnju. Rad također razmatra prepreke u donošenju zakona, uključujući političke nesuglasice i ulogu međunarodnih aktera.*

**Ključne riječi:** *kritična infrastruktura, zakonodavni okvir, EU standardi, sigurnost, kibernetičke prijetnje*

## UVOD

Kritična infrastruktura (KI) obuhvaća fizičke i virtualne sustave koji su ključni za funkcionalnost društva, ekonomije i sigurnosti države, uključujući energetske mreže, transport, vodovodnu i kanalizacijsku infrastrukturu, komunikacijske sustave i zdravstvo. Oštećenje ili prekid rada ovih sustava može imati ozbiljne posljedice za sigurnost i kvalitetu života građana (UNU EHS). Europska unija (EU) prepoznaje značaj KI i razvila je politike za zaštitu tih sustava, definirajući ih kroz Direktivu 2008/114/EC[1] i njezinu nasljednicu Direktivu (EU) 2022/2557[2], koje pozivaju države članice na identifikaciju i procjenu KI prema zajedničkim standardima.

Bosna i Hercegovina, kao kandidat za članstvo u EU, dužna je uskladiti svoje zakonodavstvo s europskim direktivama. Međutim, na državnoj razini još uvijek nije prihvaćen zakon o KI, što stvara pravnu nesigurnost i otežava definiranje sektora kritične infrastrukture. Pojam "kritična infrastruktura" odnosi se na sustave i objekte čije oštećenje može izazvati negativne posljedice za sigurnost, ekonomiju i životni okoliš. Kaskadni učinci nastaju kada poremećaj u jednom sektoru izazove lančane reakcije u povezanim sektorima, što može imati ozbiljan utjecaj na šire sustave *(Nguyen et al., 2021., Reis et al., 2022.)*.

Zakon o KI, koji je ključan za usklađivanje s međunarodnim i europskim normama, u BiH nije prihvaćen zbog političke fragmentacije, administrativnih prepreka i blokiranja donošenja ključnih odluka.

*Fikret Mehović, MA, (professorfik@gmail.com), Fakultet političkih nauka u Sarajevu, Sarajevo, Bosna i Hercegovina.

[1]https://eur-lex.europa.eu/legal-content/hr/ALL/?uri=CELEX:32008L0114

[2]https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

## KRITIČNA INFRASTRUKTURA

Kritična infrastruktura je kralježnica modernog društva (UNU EHS)[3]. Kritična infrastruktura predstavlja ključne sustave i objekte koji su od esencijalnog značaja za funkcioniranje društva, ekonomije i sigurnosti. Lewis *(2023.)* napominje da pojam KI nije postojao prije 1990-ih, a zaštita kritične infrastrukture (CIP) nije bila prepoznata dok teroristički napadi 11. rujna 2021. nisu izazvali promjene u shvaćanju njezinog značaja. Pojam se proširio od osam sektora na 18 sektora i ključnih resursa do 2013. godine *(Lewis, 2023.)*. Pojam "kritična infrastruktura" postao je evolutivan i dvosmislen, kako objašnjavaju Cronin i Marion *(2017.)*, prepoznajući važnost infrastrukture u kontekstu opasnosti, uključujući terorizam i prirodne katastrofe.

Prema Svjetskom ekonomskom forumu[4], kritična infrastruktura ima ključnu ulogu u globalnim ekonomijama, a njezina zaštita postaje izazov u digitalnoj eri. Mitrovska *(2019.)* ističe da je učinkovita zaštita KI od esencijalnog značaja za kvalitetu života i ekonomski prosperitet u današnjem turbulentnom svijetu. S obzirom na rastuću povezanost sektora, prepoznaju se kaskadni učinci koji se mogu širiti među povezanim sektorima, uzrokujući ozbiljne posljedice za šire društvo *(Nguyen et al., 2021., Reis et al., 2022.)*.

## IZAZOVI I GLOBALNA PERSPEKTIVA

Zaštita kritične infrastrukture na nacionalnoj razini zahtijeva identifikaciju, prioritetizaciju i implementaciju zaštitnih mjera *(Petrakos & Kotzanikolaou, 2019.)*. U Sjedinjenim Američkim Državama, povećanje ulaganja u kibernetičku sigurnost, kao i osnivanje platformi za zaštitu od ransomware napada, potvrđuju potrebu za stalnim unaprjeđenjem sigurnosnih mjera. Napadi na Colonial Pipeline i elektroenergetsku mrežu u Ukrajini ukazuju na ranjivost ključnih sektora *(CISA, 2021.)*.

Mikac *(2019.)* ističe da je Europska unija usmjerena na zaštitu KI, naročito nakon terorističkih napada, uvevši nove regulative poput NIS2 Direktive koja postavlja visoke sigurnosne standarde za sektore kritične infrastrukture. Diljem svijeta kritična se infrastruktura, osim u državnom, nalazi i u privatnom vlasništvu. Čak 85 % kritičnih infrastruktura u zapadnom svijetu u vlasništvu je ili njima upravlja privatni sektor. Bez obzira na oblik vlasništva, učinkovita zaštita kritične infrastrukture zadaća je i odgovornost kako javnog tako i privatnog sektora i zahtijeva usku suradnju tijela javne vlasti i poslovne zajednice. Također, Mikac, Cesarec i Larkin *(2018.)* ističu značaj javno-privatnog partnerstva u zaštiti KI, gdje privatni sektor pridonosi sigurnosti kritičnih objekata. Kroz javno-privatno partnerstvo privatni sektor može usmjeriti svoje resurse i vještine u pružanje dobara i usluga koje po tradiciji osiguravaju državne službe. Tako se može stvoriti nova kvaliteta odnosa između država i privatnog sektora kroz uravnoteženost podjele zadaća u sustavu *(Mikac, Cesarec, Larkin, 2018.)*

## PRAVNI OKVIRI I BUDUĆNOST

Tako Coffelt i Hendrickson *(2019.)* smatraju da "ljudsko društvo presudno ovisi o nizu infrastrukturnih ulaganja koja su učinjena tokom vijekova. Izgradili smo vodovodne, kanalizacijske i elektroenergetske sisteme, kao i zgrade, ceste, luke, željezničke pruge i druge objekte. U novije vrijeme izgradili smo složene telekomunikacijske sisteme. U tom su procesu ljudi duboko izmijenili prirodne krajolike i ekološke sisteme. Bez naše infrastrukture društvo ne bi funkcioniralo u kakvom je stanju danas". Kako bi se osigurala otpornost infrastrukture, nužno je razviti odgovarajuće zakonske okvire i promovirati suradnju između javnog i privatnog sektora. S obzirom na složenost međunarodnih prijetnji, zemlje poput Njemačke i SAD-a već implementiraju napredne zakone za jačanje digitalne sigurnosti i otpornosti ključnih sektora. Ovi pristupi pokazuju da je pravovremeno donošenje zakona ključ za smanjenje rizika i zaštitu društvenih i ekonomskih sustava. Američka inicijativa u ovom pravcu započela je 1998. godine kroz Predsjedničku Direktivu 63[5] koja je identificirala sektore poput telekomunikacija, energetike, transporta i vodoopskrbe kao esencijalne.

[3]UNU EHS, United Nations University, Institute for Environment and Human Security.

[4]https://www.weforum.org/stories/2022/05/securing-systemically-important-critical-infrastructure/

[5]https://irp.fas.org/offdocs/pdd/pdd-63.htm

## KRITIČNA INFRASTRUKTURA U ENTITETIMA BIH I DISTRIKTU BRČKO BIH

Entitet Republika Srpska (RS) prihvatio je zakon o sigurnosti kritičnih infrastruktura 2019. godine, dok Federacija BiH (FBiH) i Brčko distrikt (BD BiH) još nisu donijeli slične zakone. Zakon RS-a definira kritičnu infrastrukturu kao sustave i objekte čije uništavanje može izazvati ozbiljne poremećaje u funkcijama poput transporta, zdravstva, sigurnosti i ekonomske stabilnosti[6]. Uključuje 12 sektora, među kojima su industrija, energetika, promet i zdravstvo. Zakon također predviđa godišnju analizu sigurnosnih planova i imenovanje sigurnosnog koordinatora za implementaciju zaštite. Iako ovaj zakon ne definira specifičnu europsku kritičnu infrastrukturu na području entiteta RS, član 4. točka 8 navodi međunarodnu infrastrukturu kao onu koja je definirana kao kritična između dvije susjedne zemlje, što je u skladu s definicijom europske kritične infrastrukture.

U entitetu FBiH, prednacrt zakona[7] o zaštiti kritične infrastrukture objavljen je u srpnju 2023. godine, regulirajući identifikaciju i zaštitu kritičnih objekata, procjenu rizika, sigurnosne planove i imenovanje koordinatora. Ovaj prednacrt zakon implementira EU Direktivu 2022/2557 i predviđa ažuriranje sektora prema potrebama. Također, predviđa suradnju s Ministarstvom sigurnosti BiH za identifikaciju europske kritične infrastrukture.

Za Brčko distrikt BiH još uvijek nije prihvaćen zakon o KI, ali je Policija Brčko angažirana na projektu EU[8] za razvoj zakonodavstva o otpornosti kritične infrastrukture. Projekt je podržan od nekoliko europskih zemalja, a uključuje procjenu rizika i metodologiju prema CER Direktivi EU 2022/2557[9]. Iako nisu zabilježeni ozbiljni incidenti koji bi ugrozili kritičnu infrastrukturu, prijavljeni su manji incidenti povezani s građevinskim radovima.

Iako se zakonodavstvo o kritičnoj infrastrukturi u BiH razvija, postoji potreba za harmonizacijom zakona između entiteta i uvođenjem zajedničkog zakonodavnog okvira na državnoj razini. To bi omogućilo bolje koordinirane mjere zaštite i povećanje otpornosti na sigurnosne prijetnje. Prihvaćanje prednacrta zakona o kritičnoj infrastrukturi u Federaciji BiH predstavlja ključni korak prema usklađivanju i unapređenju zaštite kritičnih objekata na cijelom teritoriju BiH. Zakon prihvaćen u RS-u već postavlja osnovu za razvoj zakonodavstva na državnom razini, čime se omogućava donošenje jedinstvenog zakona. Ovaj okvir objedinjuje smjernice za procjenu rizika i zaštitu sektora poput energetike, transporta i komunikacija te poboljšava koordinaciju među nadležnim tijelima. Integracija najboljih praksi iz oba entiteta omogućava izgradnju sveobuhvatnog zakonodavnog okvira koji zadovoljava sigurnosne zahtjeve i omogućava bolju zaštitu na nacionalnoj razini, čime BiH postaje otpornija na sigurnosne prijetnje te pridonosi stabilnosti i sigurnosti zemlje u skladu s međunarodnim standardima.

## CERT

### Nastajanje CERT-a

Morris worm[10] incident bio je jedan od najpoznatijih i najznačajnijih cyber napada u povijesti interneta, koji se dogodio u studenom 1988. godine. Ovaj napad, poznat i kao Morris worm ili Internet worm, bio je prvi veliki napad na internet koji je izazvao globalnu pozornost i imao dugoročne posljedice na način na koji su razvijane sigurnosne mjere za računalstvo i mreže. Poslije Morris warm incidenta Agencija za napredne istraživačke projekte (DARPA) odlučila je formirati tim za odgovor koji bi pružio trenutni, brz odgovor na veće napade na računalne resurse. Re-

[6]Službeni glasnik Republike Srpske (2019), Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj, https://ruczrs.org/wp-content/uploads/2022/11/ZAKON-O-BEZBJEDNOSTI-KRITICNIH-INFRASTRUKTURA-U-REPUBLICI-SRPSKOJ-Sluzbeni-Glasnik-RS-broj-58.19.pdf

[7]FMUP Sarajevo. (2023). Prednacrt Zakona o zaštiti kritične infrastrukture u Federaciji BiH. http://www.fmup.gov.ba/files/Prednacrt%20Zakona%20o%20zastiti%20kriticne%20infrastrukture%20u%20FBiH.doc

[8]Policija Distrikta Brčko BiH.

[9]https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

[10]Morris worm je lansirao Robert Tappan Morris, student na Sveučilištu Cornell, 2. studenog 1988. godine. U početku je Morris razvijao crv kao eksperiment u svrhu testiranja veličine internetske mreže i njezinih veza, ali je ubrzo izmaknuo kontroli. Worm je, naime, iskoristio nekoliko sigurnosnih rupa u operativnim sustavima Unix na računalima povezanima na ARPANET (preteča današnjeg interneta). Morris worm postao je važan slučaj u povijesti računalne sigurnosti jer je pokazao opasnosti i potencijalne učinke cyber napada te doveo do razvoja jačih sigurnosnih protokola i alata za zaštitu računalnih mreža.

zultat je bio formiranje Računalnog tima za hitne slučajeve (CERT); *(Lucas i Moeller, 2003.).*

CERT (Computer Emergency Response Team) predstavlja organizaciju ili tim stručnjaka koji se bavi identifikacijom, analizom i odgovorom na računalne sigurnosne incidente, kao što su cyber-napadi, provale u sustave, virusi, malware i druge prijetnje koje mogu ugroziti sigurnost informacijskih tehnologija i infrastrukture. CERT-ovi su ključni u prevenciji, detekciji i brzom odgovoru na računalne prijetnje te pružaju podršku organizacijama u zaštiti njihovih informacijskih sustava i podataka. Tako Willems tvrdi da su CERTovi potrebni, korisni i obavljaju dobar posao. Prate kibernetičke prijetnje u svakodnevnom životu i pokušavaju brzo odgovoriti na kršenja sigurnosti računala i mreža *(Willems, 2019.).*

U kontekstu sigurnosti kritične infrastrukture, CERT nije samo preventivni element već i reakcijski mehanizam koji se aktivira u slučaju napada na računalnu infrastrukturu koja podržava ključne usluge poput energetske mreže, komunikacijskih sustava, financijskog sektora, transporta i drugih sektora od strateške važnosti za funkcioniranje države ili organizacije. Dakle, iako CERT ima ključnu ulogu u zaštiti i sigurnosti tih sustava, on je samo jedan dio šireg okvira zaštite kritične infrastrukture, koja uključuje fizičku, informatičku i ljudsku sigurnost, kao i koordinaciju između različitih institucija i tijela na nacionalnoj i međunarodnoj razini. Osim CERT-a, koji se bavi zaštitom od cyber prijetnji, sigurnost kritične infrastrukture uključuje nekoliko drugih ključnih elemenata, kako bi se osigurala sveobuhvatna zaštita i minimizirali rizici. Ti elementi obuhvaćaju fizičku, operativnu, ljudsku i pravnu dimenziju sigurnosti:

- Fizička sigurnost: zaštita ključnih objekata (npr. energetske stanice, bolnice, komunikacijski centri) putem kamera, barijera, nadzora i kontrole pristupa;
- Operativna sigurnost: održavanje nesmetanog rada sustava kroz efikasne protokole za prevenciju, detekciju i reagiranje na incidente, uključujući planove oporavka;
- Ljudski faktor: poduka zaposlenika za prepoznavanje sigurnosnih prijetnji i primjenu odgovarajućih sigurnosnih procedura, uz razumijevanje etičkih i zakonskih aspekata;
- Pravna sigurnost: implementacija zakona, regulativa i politika na nacionalnoj i međunarodnoj razini, uključujući mjere protiv cyber napada i kaznene sankcije;
- Koordinacija i suradnja između različitih institucija i agencija na nacionalnoj i međunarodnoj razini zbog globalne prirode sigurnosnih prijetnji.

Svi navedeni elementi, zajedno s CERT-om, čine osnovu zaštite kritične infrastrukture od širokog spektra prijetnji, uključujući fizičke napade, cyber prijetnje, prirodne katastrofe i druge opasnosti koje mogu ugroziti funkcionalnost i sigurnost tih ključnih sustava.

## CERT U BOSNI I HERCEGOVINI

Bosna i Hercegovina je jedina zemlja u regiji Zapadnog Balkana koja nije prihvatila zakon o kritičnim infrastrukturama na državnoj razini. Druge zemlje Zapadnog Balkana imaju zakone o KI na državnoj razini dok Albanija i Sjeverna Makedonija nemaju specifične zakone koji se izričito odnose na zaštitu kritične infrastrukture. Međutim, obje zemlje poduzele su korake prema usklađivanju svojih zakonodavstava s europskim standardima u ovom području.

U Albaniji, zakonodavni okvir za zaštitu kritične infrastrukture temelji se na Općem zakonu o zaštiti podataka i informacijskih sustava, koji je usklađen s europskim propisima. Ovaj zakon propisuje obveze za subjekte koji upravljaju kritičnom infrastrukturom u pogledu sigurnosti podataka i informacija. Također, Albanija je prihvatila zakonodavne mjere za zaštitu sektora poput energetike, transporta i komunikacija, integrirajući ih u širi okvir nacionalne sigurnosti. Sjeverna Makedonija, s druge strane, implementirala je zakonodavne mjere koje se odnose na sigurnost mreža i informacijskih sustava, usklađujući ih s Direktivom EU o sigurnosti mreža i informacijskih sustava (NIS Direktiva). Ove mjere obuhvaćaju obveze za pružatelje usluga digitalne infrastrukture i ključne usluge u pogledu upravljanja sigurnosnim rizicima i incidentima. Iako ne postoji specifičan zakon o kritičnoj infrastrukturi, ove mjere predstavljaju značajan korak prema usklađivanju s europskim standardima u zaštiti kritične infra-

strukture. Važno je napomenuti da, iako Albanija i Sjeverna Makedonija nemaju specifične zakone o kritičnoj infrastrukturi, poduzete mjere i usklađivanja s europskim propisima pokazuju njihovu predanost jačanju sigurnosti kritičnih objekata i usluga u skladu s europskim standardima što nije slučaj u Bosni i Hercegovini na državnoj razini.

Bosna i Hercegovina je zemlja koja je Dejtonskim mirovnim sporazumom[11] koji je službeno potpisan u Parizu 14. prosinca 1995. godine, podijeljena na dva entiteta, Federacija Bosne i Hercegovine (FBiH) i Republika Srpska (RS) i Brčko distrikt Bosne i Hercegovine (BDBiH). Godinu ranije, 18. ožujka 1994. u Washingtonu, potpisan je Washingtonski sporazum[12] kojim je FBiH podijeljena na deset kantona. CERT[13] je ključni element u zaštiti kritične infrastrukture, naročito u kontekstu cyber sigurnosti.

Na osnovi člana 17. Zakona o Vijeću ministara Bosne i Hercegovine te zaključka sa 64. sjednice Vijeća ministara održane 14. srpnja 2016. godine[14], donesena je odluka o formiranju tima za odgovor na računalne incidente. Ova odluka, koja je potvrđena na 93. sjednici Vijeća ministara 8. ožujka 2017. godine, uspostavlja Tim za odgovor na računalne incidente (CERT) za institucije Bosne i Hercegovine, koji funkcionira unutar Ministarstva sigurnosti BiH. Odluka detaljno regulira rad CERT-a, njegove aktivnosti, organizaciju i nadležnosti. Također, Ministarstvo sigurnosti BiH bilo je obvezno da u roku od tri meseca predloži izmjene postojećeg Pravilnika za formiranje unutrašnje organizacijske jedinice koja bi bila odgovorna za rad CERT-a. Odluka se, međutim, ne primjenjuje na situacije u kojima drugi zakoni propisuju upotrebu papirnih dokumenata i podataka za koje je sigurnost regulirana Zakonom o zaštiti tajnih podataka. CERT obavlja različite aktivnosti, kao što su koordinacija preventivnih mjera za zaštitu od sigurnosnih prijetnji, prikupljanje informacija o rizicima, praćenje računalnih incidenata, reakcija na prijavljene incidente, edukacija o sigurnosti informacijskih sustava, priprema sigurnosnih mjera i izdavanje preporuka za zaštitu sustava te suradnja sa sličnim timovima unutar i izvan zemlje. Međutim, uspostavljeni CERT za institucije BiH nije u potpunosti usklađen s Direktivom (EU) 2016/1148 Europskog parlamenta i Vijeća, koja nalaže formiranje nacionalnog CERT-a. U Bosni i Hercegovini trenutno postoje tri različita CERT-a: jedan za državne institucije te dva entitetska. Distrikt Brčko BiH još nema svoj vlastiti CERT, ali se očekuje da će uskoro započeti rad na njegovoj uspostavi. Prema istraživanjima, ključni izazovi za CERT-ove uključuju izgradnju povjerenja, upravljanje resursima i suradnju s partnerima. Preporuke uključuju jačanje tehničke ekspertize i pravnih okvira, što je presudno za njihovo efikasno djelovanje. Resursna efikasnost i prilagodljivost su posebno važni za suočavanje s rastućim prijetnjama, uključujući ransomware i napade na kritičnu infrastrukturu (GCSCC)[15].

## VAŽNOST CERT-a

Važnost CERT-a na državnoj razini jest u njegovoj sposobnosti da koordinira i integrira odgovore na cyber prijetnje i incidente diljem države. Državni CERT može efikasnije upravljati velikim brojem cyber sigurnosnih rizika jer ima širu odgovornost, pokrivajući sve sektore i institucije te može osigurati koherentnu i jedinstvenu politiku zaštite u cijeloj zemlji. Također, on može koordinirati međunarodnu suradnju s drugim državama i organizacijama, čime se omogućava bolje upravljanje globalnim prijetnjama, kao i bolja koordinacija u kriznim situacijama. Državni CERT može također pružiti usluge poduke, podizanje svijesti o sigurnosti i preporuke za oba entiteta i BDBiH u zemlji, što poboljšava opću razinu cyber sigurnosti na nacionalnoj razini. S druge strane, postojanje CERT-a na entitetskoj razini, iako može biti korisno za specifične potrebe na regionalnoj razini, nosi sa sobom određene slabosti. Prvo, entitetski CERT-ovi mogu raditi u izolaciji, što može dovesti do fragmentacije sigur-

[11]Dejtonski mirovni sporazum je važan politički i vojni dogovor koji je postignut 1995. godine u Bosni i Hercegovini, a koji je označio kraj rata u toj zemlji. Sporazum je nazvan prema mestu na kojem je potpisan, Dayton, u američkoj saveznoj državi Ohio. Točnije, Daytonski mirovni sporazum (poznat i kao Opći okvirni sporazum za mir ili OFS), postignut je 21. studenog 1995. godine, nakon intenzivnih pregovora i mirovnih pregovarača pod pokroviteljstvom SAD-a.

[12]Washingtonski sporazum je od ključne važnosti jer je postavio temelje za dalji mirovni proces u Bosni i Hercegovini, koji će kulminirati Daytonskim mirovnim sporazumom 1995. godine. Sporazum je bio korak prema stvaranju političke osnove za izgradnju mira između Bošnjaka i Hrvata.

[13]Computer Emergency Response Team

[14]http://www.sluzbenilist.ba/page/akt/g4E0HNrVpsc

[15]https://gcscc.ox.ac.uk/home-page

nosnih napora i otežanog odgovora na prijetnje koje prelaze entitetske granice. Bez koordinacije s državnom razinom, različiti CERT-ovi mogu razviti različite standarde zaštite i politike, što može dovesti do nesklada u zaštiti cijele zemlje. Također, entitetski CERT-ovi mogu imati ograničene resurse i kapacitete, što im otežava borbu protiv sofisticiranih cyber prijetnji koje se ne zaustavljaju na entitetskim granicama. Na kraju, entitetski CERT-ovi mogu ometati izgradnju jedinstvene nacionalne strategije za cyber sigurnost. Bez centraliziranog tijela, BiH može biti podložna većim rizicima, jer bi odgovori na incidentne situacije mogli biti usporeni ili nesinkronizirani. Ovo može rezultirati značajnim sigurnosnim slabostima, jer cyber prijetnje često nisu ograničene političkim ili administrativnim granicama. Zato je za Bosnu i Hercegovinu od ključne važnosti da uspostavi jedinstveni nacionalni CERT, koji bi mogao integrirati resurse, znanje i iskustvo oba entiteta i Brčko distrikta BiH, čime bi se poboljšala ukupna otpornost zemlje na cyber prijetnje.

## SREDNJOROČNI PROGRAMI RADA VIJEĆA MINISTARA BIH

U srednjoročnom planu rada Vijeća ministara Bosne i Hercegovine za razdoblje 2024.-2026[16]. godine, Ministarstvo komunikacija i transporta BiH navodi se donošenje Zakona o kritičnim infrastrukturama do kraja 2025. godine. Ovaj zakon se prepoznaje kao ključni korak u jačanju nacionalne sigurnosti, upravljanju rizicima i osiguravanju otpornosti kritične infrastrukture. Srednjoročni plan rada VM BiH za razdoblje 2024.-2026. razmatra ključne sektore infrastrukture u Bosni i Hercegovini, posebno digitalnu i transportnu infrastrukturu te ističe važnost kontinuiranih ulaganja i unapređenja kako bi se poboljšala kvaliteta života i podržao razvoj različitih društvenih sektora. Digitalna infrastruktura je označena kao temelj za suvremeno poslovanje, omogućavajući globalno tržište i optimizaciju usluga, uključujući "just in time delivery" model[17]. Kontinuirana ulaganja u ovu infrastrukturu smatrana su ključnim imperativom kako bi se povećala dostupnost i kvaliteta usluga za građane BiH, a time indirektno poboljšala i druga društvena područja poput zdravstva, školstva i urbanog planiranja.

U sektoru transporta, cilj je unaprijediti kvalitetu usluga u skladu s razinama razvijenim u okolnim zemljama. To podrazumijeva poboljšanje upravljanja transportnom infrastrukturom, uspostavljanje održivog financijskog sustava te osiguranje sigurnosti na cestama kroz bolje zakonodavstvo, održavanu infrastrukturu i vozila, kao i obrazovne inicijative za podizanje svijesti.

Srednjoročni ciljevi povezani s ovim sektorima obuhvaćaju dva ključna područja. Prvo, unaprjeđenje sektora komunikacija, informacijskog društva i poštanskih usluga uz usklađivanje regulatornog okvira s EU standardima, pod nadležnošću Ministarstva transporta i komunikacija BiH, Agencije za poštanski saobraćaj i Regulatorne agencije za komunikacije. Drugi cilj odnosi se na stvaranje uvjeta za uspostavu suvremenijih, sigurnijih i efikasnijih sustava transporta i komunikacija, što uključuje nadležne institucije poput Ministarstva komunikacija i transporta BiH te Direkcije za civilno zrakoplovstvo BiH. U suštini, ciljevi su usmjereni na poboljšanje digitalne i transportne infrastrukture kako bi se postigao veći ekonomski i društveni napredak u Bosni i Hercegovini.

Srednjoročni program rada Vijeća ministara Bosne i Hercegovine za razdoblje 2025. – 2027[18]. godine prepoznaje infrastrukturu kao ključnu komponentu za ostvarenje održivog i pametnog ekonomskog razvoja. Program ističe potrebu za kontinuiranim ulaganjima u modernizaciju i proširenje infrastrukture kako bi se podržao gospodarski rast, povećala konkurentnost i poboljšala kvaliteta života građana.

Ključni aspekti infrastrukture prema Srednjoročnom programu rada:

- Digitalna infrastruktura;
- Transportna infrastruktura;
- Energetska infrastruktura;
- Infrastruktura kvalitete.

[16] http://www.dep.gov.ba/naslovna/default.aspx?id=2859&langTag=bs-BA

[17] Just-In-Time (JIT) isporuka je strategija upravljanja lancem opskrbe u kojoj se roba, materijali i proizvodi isporučuju točno kada su potrebni u procesu proizvodnje ili za trenutnu upotrebu. Cilj je povećati efikasnost i smanjiti troškove skladištenja minimiziranjem razina zaliha.

[18] https://www.vijeceministara.gov.ba/akti/program_rada/default.aspx?id=44396&langTag=bs-BA

Ovi prioriteti odražavaju opredjeljenje Vijeća ministara BiH za stvaranje poticajnog okruženja za razvoj poduzetništva, inovacija i održivog gospodarskog rasta kroz ulaganja u ključne infrastrukturne sektore.

Isti prioritet naveden je i u srednjoročnom planu rada Vijeća ministara BiH, potvrđujući važnost ovog cilja kao integralnog dijela državnih razvojnih i sigurnosnih politika. U Programu reformi Bosne i Hercegovine za 2023. godinu[19], koji je izradila Komisija za saradnju s NATO-om BiH, navodi se izrada Nacrta zakona o kritičnim infrastrukturama koja će biti usklađena s europskom legislativom. Rok za završetak ovog zadatka također je postavljen za kraj 2025. godine. Ova aktivnost ima strateški značaj jer harmonizacija s EU zakonodavstvom pridonosi međunarodnom usklađivanju i jača kapacitete BiH u zaštiti kritične infrastrukture.

## IZAZOVI U PROVEDBI SREDNJOROČNIH PLANOVA VM BIH

Postoji nekoliko izazova u prihvaćanju i implementaciji ciljeva srednjoročnih planova Vijeća ministara Bosne i Hercegovine (VM BiH), posebno u područjima sigurnosti, pravosudnog sustava i infrastrukture. Politička fragmentacija u zemlji predstavlja jedan od glavnih problema jer BiH ima podijeljeni politički sustav na entitetske i kantonalne razine, što otežava usklađivanje politika i zakonodavnih okvira među različitim razinama vlasti. Ovaj politički jaz često dovodi do sporosti u donošenju odluka i implementaciji planova.

Pravosudni sustav, iako je postigao određene napretke, još ima značajnih problema s efikasnošću, transparentnošću i usklađenošću s međunarodnim standardima. Zakonodavne promjene i implementacija strateških planova suočavaju se s preprekama u obliku političkih utjecaja i nesigurnosti u pravnoj praksi. Implementacija sigurnosnih standarda, posebno onih koji se odnose na NATO i industrijsku sigurnost, zahtijeva velika ulaganja u infrastrukturu i edukaciju. Iako postoji napor za unapređenje, izazovi u integraciji novih tehnologija i održavanju ažurnih procedura prema međunarodnim standardima i dalje postoje. Pored toga, BiH je još uvijek uvelike ovisna o međunarodnoj pomoći za implementaciju reformi, a nedostatak domaće političke volje ili kapaciteta može usporiti ili omesti realizaciju ključnih ciljeva. Financijska ograničenja i potreba za ravnomjernom raspodjelom resursa među različitim razinama vlasti dodatno otežavaju implementaciju srednjoročnih planova, naročito u području infrastrukture i sigurnosti. Korupcija i administrativna neefikasnost također su značajni faktori koji negativno utječu na realizaciju strateških ciljeva. Slabi administrativni kapaciteti i dugotrajni birokratski procesi često usporavaju donošenje odluka i provedbu ključnih inicijativa. Iako postoji jasan strateški okvir za unapređenje sigurnosnih, pravosudnih i infrastrukturnih sustava u BiH, brojni faktori, kao što su politička nestabilnost, financijska ograničenja, korupcija i administrativna neefikasnost, predstavljaju ozbiljne prepreke za potpunu realizaciju tih ciljeva.

## POZITIVNI EFEKTI PRIHVAĆANJA ZAKONA O KI

Prihvaćanje zakona o kritičnim infrastrukturama u Hrvatskoj i Srbiji donijelo je značajne pozitivne efekte u nekoliko ključnih područja. Zakon o kritičnim infrastrukturnim objektima u Hrvatskoj[20] pridonosi povećanoj sigurnosti ključnih objekata i sustava, poput energetskih, prometnih i vodnih resursa. Uvođenjem analize rizika omogućava se prepoznavanje prijetnji i ranjivosti, što pomaže u pripremi na krizne situacije. Obveza izrade sigurnosnih planova i imenovanja koordinatora poboljšava koordinaciju i učinkovitost u kriznim reakcijama. Zakon također osigurava usklađenost s europskim standardima i omogućava bolju suradnju među zemljama EU-a. Potiče pripremljenost na prekide u infrastrukturi, praćenje sigurnosti i jačanje međunarodne suradnje, dok povećava odgovornost vlasnika infrastruktura. Zakon o kritičnoj infrastrukturi Republike Srbije[21] predstavlja pravni okvir za identifikaciju, zaštitu i upravljanje kritičnom infrastrukturom. Osim toga, regulira

[19]https://ekonsultacije.gov.ba/legislativeactivities/details/122492-

[20]https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html

[21]https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2018/87/8

nadležnosti različitih organizacija, odgovornosti operatera, kao i postupke identifikacije, zaštite i nadzora. Definira sektore od značaja, uključujući energetiku, promet, zdravstvo te zaštitu životne okoline. Zakon postavlja načela zaštite, uključujući integrirani pristup i odgovornost operatera. Pored toga, uvođenje ovakvog zakona omogućava bolju suradnju s međunarodnim institucijama, uključujući EU i NATO, jer osigurava da se nacionalni okvir za zaštitu infrastrukture uskladi s najboljim praksama i standardima. Time se također jača povjerenje stranih investitora i podržava ekonomska stabilnost zemlje.

Unatoč jasno prepoznatim koristima, postoje specifični problemi zbog kojih Zakon o kritičnim infrastrukturama još nije prihvaćen na razini BiH. Ključni izazov predstavlja složenost političkog sustava BiH, gdje različie razine vlasti često ne uspijevaju postići dogovor o zakonodavnim prioritetima. Nedostatak konsenzusa među entitetima dodatno usporava napredak, jer se kritična infrastruktura često tretira kao pitanje unutar entitetske nadležnosti, što stvara pravnu i administrativnu nejasnoću na državnoj razini. Još jedan problem je nedostatak jasne institucionalne koordinacije i kapaciteta. Trenutno ne postoji centralizirano tijelo koje bi bilo odgovorno za planiranje, implementaciju i nadzor zaštite kritične infrastrukture na državnoj razini. Također, često su prisutni financijski i ljudski resursi koji nisu dovoljni za razvoj i provedbu ovakvog zakona, što dodatno usporava procese. Izazov predstavlja i svijest o važnosti ovog zakona, kako među donosiocima odluka, tako i među javnošću.

Prihvaćanjem zakona o kritičnim infrastrukturama na državnoj razini, Bosna i Hercegovina, ostvarila bi brojne koristi ali bi se suočila i s izazovima, prvenstveno zbog složenog političkog i ustavnog uređenja zemlje. Na državnoj razini, donošenje ovog zakona omogućilo bi centraliziranu koordinaciju zaštite i upravljanja kritičnim infrastrukturama, što je od ključnog značaja za nacionalnu sigurnost, otpornost na rizike i bolje upravljanje krizama. Usklađivanje sa standardima Europske unije i međunarodnim praksama poboljšalo bi odnose BiH s međunarodnim partnerima, jačalo njezinu poziciju u procesu euroatlantskih integracija i omogućilo pristup dodatnim resursima i tehničkoj pomoći. Također, zakon bi osigurao bolju zaštitu ključnih sektora, poput energetike, transporta, komunikacija i zdravstva, što bi pridonijelo ekonomskoj stabilnosti i sigurnosti građana.

Još jedan izazov je nedostatak povjerenja među političkim akterima. Na razini BiH, često se izbjegavaju rješenja koja bi mogla narušiti ravnotežu između entiteta. Strah od centralizacije moći i percepcija da bi država mogla nametnuti svoja pravila entitetima dodatno kompliciraju situaciju. Uz to, nedovoljna svijest o važnosti zaštite kritične infrastrukture kao zajedničkog interesa svih razina vlasti pridonosi političkoj blokadi.

S druge strane, prihvaćanje zakona na državnoj razini otvorilo bi vrata za efikasniju raspodjelu resursa, standardizaciju procedura i poboljšanje ukupne sigurnosne arhitekture. Međutim, bez pažljivog pristupa i uvažavanja ustavnih nadležnosti entiteta, proces donošenja zakona može se suočiti s ozbiljnim političkim preprekama. Ključ za nadilaženje ovih problema jest u razvijanju modela suradnje koji bi poštovao entitetske nadležnosti, a istovremeno omogućio djelotvoran i usklađen okvir za zaštitu kritičnih infrastruktura. Taj model mogao bi uključivati jasnu podjelu odgovornosti između državne i entitetske razine i Brčko distrikta BiH, pri čemu bi država osiguravala koordinaciju i usklađivanje s međunarodnim standardima, dok bi implementacija zakona ostala u području entiteta.

Konačno, neprihvaćanjezakona o kritičnim infrastrukturama na državnoj razini šteti ukupnoj sigurnosti i međunarodnom ugledu Bosne i Hercegovine. Nedostatak adekvatnog zakonskog okvira povećava ranjivost na sigurnosne prijetnje, smanjuje otpornost na prirodne i ljudski izazvane katastrofe i ograničava kapacitet za međunarodnu suradnju. Bez državnog zakona BiH bi mogla biti percipirana kao nesiguran partner na međunarodnoj sceni, što bi moglo ugroziti vanjsku suradnju, pristup međunarodnim fondovima i stranom kapitalu. Da bi se savladale prepreke, potrebno je uspostaviti dijalog koji će istaknuti zajedničke interese svih razina vlasti i omogućiti kompromisno rješenje koje uvažava složeni politički kontekst zemlje.

**EU zakonodavni okvir**

Kako bi BiH uskladila svoj zakonodavni okvir sa zakonodavstvom Europske unije u području zaštite kritične infrastrukture, ključne promjene trebale bi se odnositi na nekoliko važnih aspekata. Prvo, BiH bi trebala prihvatiti standardizirane definicije i klasifikacije kritične infrastrukture koje su usklađene s onima koje se primjenjuju u EU. To bi omogućilo da se zaštita kritične infrastrukture u BiH uskladi s postojećim zakonodavstvom EU, čime bi se povećala međusobna prepoznatljivost i interoperabilnost sustava zaštite. Osim toga, BiH bi morala razviti obavezujući okvir za procjenu rizika i prijetnji koji se odnose na kritičnu infrastrukturu, a koji bi bio u skladu s EU Direktivom o sigurnosti mreža i informacijskih sustava (NIS Direktiva) i CER Direktiva o otpornosti kritične infrastrukture, što bi obuhvatilo obaveze u vezi sa sigurnošću, nadzorom i izvještavanjem o incidentima. Ovaj okvir uključivao bi obavezne procjene ranjivosti kritičnih objekata i infrastrukture te precizne mjere za ublažavanje tih prijetnji. Također, BiH bi trebala uskladiti pristup zaštiti sektora poput energije, transporta, zdravstva i komunikacija, osiguravajući da se svi ovi sektori tretiraju kao jednako važni za nacionalnu sigurnost i stabilnost. Također se očekuje osnivanje funkcionalnih institucija i tijela za upravljanje zaštitom kritične infrastrukture, koja bi bila odgovorna za provođenje zakona, praćenje sigurnosnih rizika i osiguranje interoperabilnosti sa sličnim tijelima u EU. Poseban fokus stavljen je na jačanje cyber sigurnosti, što zahtijeva razvoj strategija, akcijskih planova i tehničkih kapaciteta u skladu s politikama EU u tom području. BiH bi trebala razviti mehanizme za unutrašnju koordinaciju između različitih razina vlasti i međunarodnu suradnju, posebno s institucijama EU i susjednim zemljama, kako bi se omogućila brza razmjena informacija i zajednički odgovor na prijetnje.

Još jedan ključni korak bio bi osnivanje koordiniranih nacionalnih i sektorskih tijela za upravljanje krizama i zaštitu kritične infrastrukture, koja bi bila odgovorna za implementaciju preventivnih mjera, ali i za brzo reagiranje u slučaju incidenta. Ova tijela trebala bi biti usklađena sa sustavima i protokolima za koordinaciju i razmjenu informacija na razini EU-a, čime bi se omogućila brza reakcija i međunarodna suradnja u kriznim situacijama.

U konačnici, BiH bi trebala razviti specifične mehanizme za podršku i zaštitu privatnih kompanija koje upravljaju kritičnom infrastrukturom, jer su oni često ključni akteri u održavanju sigurnosti. Ističe se i važnost edukacije i podizanja svijesti o zaštiti kritične infrastrukture, uključujući poduku osoblja u institucijama i privatnim kompanijama koje upravljaju ključnim sektorima. Zakoni i regulative trebaju biti jasno formulirani kako bi se osigurala pravna sigurnost i povjerenje privatnog sektora, međunarodnih partnera i građana. Europska legislativa stavlja posebno težište na obveze privatnog sektora da implementira odgovarajuće mjere zaštite, a BiH bi trebala uvesti slične zakonske obaveze kako bi se osigurala optimalna razina sigurnosti i zaštite infrastrukture. Sve ove promjene zahtijevaju opsežnu reformu postojećeg zakonodavnog okvira, kao i institucionalnu prilagodbu u smislu usklađivanja sa zakonima i politikama EU-a, što će omogućiti BiH da bude ravnopravni partner u zajedničkom europskom sigurnosnom okruženju.

Usklađivanje zakonodavnog okvira Bosne i Hercegovine sa zakonodavstvom Europske unije u području zaštite kritične infrastrukture predstavlja ključan korak prema jačanju nacionalne sigurnosti i stabilnosti. Implementacija standardiziranih definicija, razvoj obvezujućih okvira za procjenu rizika te usklađivanje sektorskih pristupa zaštiti infrastrukturnih sektora omogućit će BiH da unaprijedi svoju zaštitu kritičnih objekata i poveća interoperabilnost s EU. Osnivanje funkcionalnih institucija, jačanje cyber sigurnosti te razvoj mehanizama za koordinaciju i krizno upravljanje bit će ključni za brzu reakciju na prijetnje i efektivnu suradnju s međunarodnim partnerima. Također, podrška privatnim kompanijama u upravljanju kritičnom infrastrukturom i edukacija svih relevantnih aktera dodatno će ojačati sustav sigurnosti. Ovaj proces zahtijeva opsežnu reformu zakonodavstva i institucija, čime bi BiH postala ravnopravan partner u europskom sigurnosnom okruženju.

**Sigurnosni izazovi**

Politika države predstavlja njezin skup stavova o društvenim djelatnostima *(Beridan, 2009.)*. Sigurnost kao ključni zadatak države zahtijeva prihvaćanje sigurnosne politike *(Abazović, 2002.)*, a

u BiH je sigurnosna politika prihvaćena u veljači 2006. godine, podijeljena u sedam dijelova *(Lisica i Bajramović, 2021.)*. Prihvaćanje zakona o kritičnoj infrastrukturi smanjuje sigurnosne rizike i osigurava dugoročnu stabilnost. Sigurnosni izazovi u BiH proizlaze iz političkih, etničkih i vanjskih utjecaja, uključujući prijetnje od Rusije i drugih globalnih aktera. Rusija podržava proruske političke aktere, što destabilizira zemlju *(Vikadinović, 1999., Tatalović, 2006.)*. Globalizacija stvara nove prijetnje, poput transnacionalnog kriminala, cyber napada i dezinformacija, koje BiH moraju adresirati *(Mabee, 2009.)*. Zemlje poput BiH suočavaju se s prijetnjama koje dolaze iz organiziranog kriminala, migracija i cyber sigurnosti, dok širenje dezinformacija destabilizira unutrašnju situaciju *(Cikotić et al., 2018.)*.

Pojam "opstojnost države" često se koristi u BiH, osobito među separatistički orijentiranim političarima, kako bi opravdali autonomiju ili secesiju *(Azinović et al., 2012.)*. Rusija koristi hibridne metode za destabilizaciju BiH i usporavanje njenog napretka prema EU i NATO-u, podržavajući političke lidere poput Milorada Dodika *(OHR, 2023.)*[22]. Takve blokade, uključujući one u zakonodavstvu o kritičnoj infrastrukturi, ugrožavaju sigurnost i otpornost zemlje. Nedostatak zakona o kritičnoj infrastrukturi ostavlja ključne resurse nezaštićenima, čime se povećava ranjivost na hibridne prijetnje. Prihvaćanje takvog zakona bi omogućilo usklađivanje s međunarodnim normama i povećalo otpornost na vanjske pritiske. Hibridno ratovanje, koje uključuje napade na infrastrukturu, manipulaciju medijima i podršku neslužbenim vojnim grupama, destabilizira političke i društvene strukture, ciljajući kritičnu infrastrukturu poput energetskih i telekomunikacijskih sustava.

Rusija, na Balkanu, je nastavila koristiti tri glavna instrumenta: nerazriješeno pitanje Kosova, energetsku ovisnost i meku moć kroz popularnost među pravoslavnim narodima *(Fruscione, 2023.)*. Ruski lideri nakon Hladnog rata su koristili Balkan, uključujući Srbiju, za postizanje svojih geopolitičkih ciljeva *(Headley, 2008.)*. Okupacija ukrajinski Krima je veoma dobar primjer. U tim slučajevima Rusija je primijenila kombinaciju kibernetičkih operacija, informacijskog rata i potpore neregularnim snagama kako bi postigla svoje ciljeve bez pribjegavanja otvorenoj vojnoj agresiji *(Muradov, 2022., Lanoszka, 2016.)*. Kroz hibridno ratovanje, Rusija destabilizira regiju, sprječavajući integraciju Balkana u zapadne institucije. Ruski utjecaj u BiH, posebno u entitetu RS-u, podržava proruske orijentacije, čime pridonosi unutarnjim podjelama. EU i SAD nastoje ojačati ekonomsku stabilnost i vojnu prisutnost, kao odgovor na hibridne prijetnje, uključujući jačanje misije EUFOR-a. Hibridna strategija Rusije također uključuje ulogu Rusko-srpskog humanitarnog centra u Srbiji, što izaziva zabrinutost u EU. Sankcije EU-a, uključujući zabranu emitiranja ruskih medija, odgovor su na rusku dizinformacijsku kampanju. Gerasimovova vojna doktrina integrira[23] hibridno ratovanje, kombinirajući konvencionalne vojne akcije, cyber napade, informatičko ratovanje i ekonomske destabilizacije. Rusija koristi ove metode kako bi oslabila protivnike prije otvorenog rata, odgovarajući na širenje NATO-a prema njezinim granicama.

U kontekstu kritične infrastrukture, zaštita od hibridnih prijetnji zahtijeva ne samo fizičku sigurnost, već i sofisticiranu koordinaciju među različitim akterima, dok nedostatak zakonskog okvira ostavlja infrastrukturu ranjivom na vanjske i unutarnje prijetnje.

## ZAKLJUČAK

Zaštita kritične infrastrukture postaje imperativ u kontekstu sve složenijih hibridnih prijetnji i geopolitičkih izazova. Nedostatak zakonskog okvira čini ključne resurse ranjivima, otvarajući prostor za manipulacije i destabilizaciju koja može imati dugoročne posljedice na ekonomsku, političku i društvenu sigurnost države. Primjeri hibridnog ratovanja – kroz kombinaciju cyber napada, informacijskog rata, ekonomske destabilizacije i medijske propagande – pokazuju da je usklađivanje s međunarodnim normama te prihvaćanje zakona o zaštiti kritične infrastrukture, uključujući i prihvaćanje EU zakonodavnih okvira, ključno za otpor vanjskim pritiscima.

[22]https://www.ohr.int/hr/

[23]Bajarūnas E.: Countering hybrid threats and building resilience: Case of Lithuania (Prezentacija u Power Pointu). Zagreb, 2017.

Pored toga, pomoć koju EU nudi pri zaštiti kritične infrastrukture kroz financijsku, tehničku i institucionalnu podršku omogućava bolju koordinaciju između različitih razina vlasti i međunarodnih partnera. Prihvaćanje ovih mjera nije samo administrativni postupak, već strateški potez koji povećava otpornost države na hibridne prijetnje i pridonosi dugoročnoj stabilnosti, osiguravajući pouzdanost ključnih resursa i povjerenje građana.

## LITERATURA


Abazović, D. M.: *Državna bezbjednost: uvod i temeljni pojmovi*, Fakultet kriminalističkih nauka UNSA, Sarajevo, 2002.

Aydinli, E., Rosenau, J.: *Globalisation, Security, and the Nation-State*, State University of New York Press, New York, 2005.

Azinović, V., Kurt, B., Bodo, W.: *Analiza sigurnosnih rizika: procjena potencijala za obnovu etničkog nasilja u Bosni i Hercegovini*, Fakultet političkih nauka Sarajevo i Atlantska inicijativa, Sarajevo, 2012.

Bajarūnas, E.: *Countering hybrid threats and building resilience: Case of Lithuania*, Prezentacija u Power Pointu, Zagreb, 2017.

Bartles, K. C.: *Getting Gerasimov Right*, University of Missouri-Kansas City, 2016.

Beridan, I.: *Politika i sigurnost*, Fakultet političkih nauka UNSA, Sarajevo, 2009.

Berzinš, J.: Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy, Policy paper, 2014.

Cikotić, S., Smajić, M., Delić, H., Subašić, N.: *Nacionalna sigurnost i privatna zaštita*, Fakultet političkih nauka UNSA, Sarajevo, 2018.

Clausewitz, C.: *On War (Translated and edited by Hans W. Gatzke)*, The Military Service Publishing Company, 1942.

Coffelt, D., Hendrickson, C.: *Fundamentals of the Infrastructure Management*, Third Edition, Pittsburgh, Pennsylvania, USA, 2019.

Ekinci, D.: *Russia and the Balkans after the Cold War*, Libertas, 2013.

*European Parliamentary Research Service:* Russia and the Western Balkans: Geopolitical confrontation, economic influence and political interference, EPRS, 2023.

*FMUP Sarajevo: Prednacrt Zakona o zaštiti kritične infrastrukture u Federaciji BiH*, dostupno na: http://www.fmup.gov.ba/files/Prednacrt%20Zakona%20o%20zastiti%20kriticne%20infrastrukture%20u%20FBiH.doc, pristupljeno: 13.11.2024.

Fruscione, G.: *Europe and Russia on the Balkan Front: Geopolitic and Diplomacy in the EU's Backyard*, Milan, 2023.

Grau, W. L., Bartles, K. C.: *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Force*, Foreign Military Studies Office (FMSO) Fort Leavenworth, KS, 2016.

Gritzalis, D., Theocharidou, M., Stergiopoulos, G.: *Critical Infrastructure Security and Resilience: Theories, Methods.* U: Nikolaos, P., Kotzanikolaou, P. (ur.): Methodologies and Strategies for Critical Infrastructure Protection, Springer, Switzerland, 2019.

Hedenskog, J., Persson, G., Pallin, V. C.: *Russian Military Capability in a Ten-Year Perspective* – 2016, 2016.

Kelley, A. P., Marion, N. E.: *Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective, Taylor and Francis Group*, New York, 2017.

Lanoszka, A.: Russian hybrid warfare and extended deterrence in eastern Europe, *International Affairs*, 2016.

Lewis, G. T.: *Critical Infrastructure Protection in the Homeland Security: Defending a Networked Nation*, Third Edition, John Wiley & Sons, Inc., 2020.

Lisica, D., Bajramović, Z.: *Planiranje u sektoru sigurnosti*, Fakultet političkih nauka UNSA, Sarajevo, 2021.

Lucas, J., Moeller, B.: *The Effective Incident Response Team*, Pearson Education, Inc., Boston, 2003.

Mabee, B.: *The Globalisation of Security*, Palgrave MacMillan, London, 2009.

Mikac, R., Cesarec, I., Larkin, R.: Kritična infrastruktura, platforma uspješnog razvoja sigurnosti nacija, *Naklada Jesenski i Turk*, Zagreb, 2018.

Mitrevska, M., Mileski, T., Mikac, R.: *Critical Infrastructure: Concept and Security Challenges*, Friedrich Ebert Foundation, office Skopje, Skoplje, 2019.

Muradov, I.: The Russian hybrid warfare: the cases of Ukraine and Georgia, *Defence Studies*, 2022.

Nguyen, T. N., Liu, B-H., Nguyen, P., Dumba, B., Chou, J. T.: *Smart grid vulnerability and defense analysis under cascading failure attacks*, 2021.

Reis, C., Lopes, M., Baptista, M. A., Clain, S.: *Towards an integrated framework for the risk assessment of coastal structures exposed to earthquake and tsunami hazards*, 2022.

*Službeni glasnik Republike Srpske:* Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj, dostupno na: https://ruczrs.org/wp-content/uploads/2022/11/ZAKON-O-BEZBJEDNOSTI-KRITICNIH-INFRASTRUKTURA-U-REPUBLICI-SRPSKOJ-Sluzbeni-Glasnik-RS-broj-58.19.pdf, pristupljeno: 22.10.2024.

Tatalović, S.: Nacionalna i međunarodna sigurnost, *Politička kultura*, Zagreb, 2006.

*United Nations University – Institute for Environment and Human Security (UNU-EHS): 5 Things You Need to Know about Critical Infrastructures*, dostupno na: https://unu.edu/ehs/series/5-things-you-need-know-about-critical-infrastructures, pristupljeno: 10.10.2024.

*Vijeće Europske Unije: Direktiva Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite*, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114, pristupljeno: 21.10.2024.

Vukadinović, R.: Globalizacija i globalna američka politika, *Politička misao*, Zagreb, 1999.

Willems, E.: *Cyberdanger: Understanding and Guarding Against Cybercrime*, Springer Nature Switzerland AG, 2019.

## *REASONS FOR NOT ADOPTING A LAW ON CRITICAL INFRASTRUCTURES IN BOSNIA AND HERZEGOVINA*

*SUMMARY: Bosnia and Herzegovina (BiH) is facing serious consequences of not adopting the law on critical infrastructures (CI) at the state level, which threatens the security and stability of key sectors. This law is crucial for the identification, protection and resilience of sectors such as energy, transport and communications. The lack of a unified legislative framework makes coordination between levels of government difficult and increases the risk of natural and security threats. The paper analyzes the political reasons for the non-adoption of the law, the consequences for the infrastructure and the possibility of adaptation to EU standards. The focus is on security implications, including vulnerability to cyber threats and hindered international cooperation. The paper also considers obstacles to the adoption of legislation, including political disagreements and the role of international actors.*

***Key words:*** *critical infrastructure, legislative framework, EU standards, security, cyber threats*

*Subject review*
*Received: 2024-12-09*
*Accepted: 2025-03-18*