Serijal *policy* analiza
Instituta za sigurnosne politike
http://insigpol.hr/

Godina 2020
Broj 004

Elementi za izradu novog Zakona o kritičnim infrastrukturama Republike Hrvatske[1]

Uvod

Izrada novog Zakona o kritičnoj infrastrukturi koja je u tijeku, a čije donošenje je predviđeno za III. tromjesečje 2020. predstavlja nastavak aktivnosti u ispunjavanju strateških smjernica definiranih Strategijom nacionalne sigurnosti Republike Hrvatske. Analizirajući globalne sigurnosne rizike i prijetnje ovo područje postaje sve zahtjevnije i sveobuhvatnije te zahtijeva uključenost svih mogućih aktera na ovom području što i navedena Strategija prepoznaje. Cilj ovog teksta je iznijeti određen broj elemenata, ideja i prijedloga koji bi mogli biti značajni u tom procesu i pomoći stručnim službama resornih ministarstava nadležnim za donošenje Zakona.

Strateška dimenzija

Postojeći Zakon o kritičnim infrastrukturama (Narodne novine, broj 56/13) donesen je 2013. godine, kako bi njime bila preuzeta obveza iz direktive Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite (u daljnjem tekstu Direktiva Vijeća 2008/114/EZ) i kako bi u jednom zakonu Republika Hrvatska objedinila do tada parcijalna nastojanja normativnog uređenja područja zaštite nacionalne kritične infrastrukture. U međuvremenu su se promijenile strateške i sigurnosne okolnosti unutar predmetnog područja na razini Europske unije i Republike Hrvatske, tako da u novom Zakonu o kritičnoj infrastrukturi svakako treba uvažiti novu realnost i promjene.

Direktiva Vijeća 2008/114/EZ predstavlja okosnicu mnogih procesa na razini Europske unije, njom se propisuju postupak utvrđivanja potencijalne europske kritične infrastrukture;

[1] Dio ove analize je objavljen u časopisu Zaštita, XIV. godina, broj X, 2019.
Analiza je napravljana povodom izrade Zakona o kritičnoj infrastrukturi od strane Ministarstva unutarnjih poslova Republike Hrvatske, a u cilju kako bi pomogli radnoj skupini koja radi na izradi predmetnog Zakona.

primjena međusektorskih mjerila (kao što su moguće žrtve, gospodarske posljedice i utjecaj na javnost) i sektorskih mjerila specifičnih za pojedine vrste kritične infrastrukture; suradnja država u utvrđivanju i označavanju europske kritične infrastrukture; materija sigurnosnih planova operatera; važnost časnika za vezu zaduženog za sigurnost kritične infrastrukture; izvješćivanje država svake dvije godine prema Europskoj komisiji o vrstama rizika, prijetnjama i slabostima u zaštiti europske kritične infrastrukture.

Komisija je do sada pokrenula dvije značajne revizije Direktive Vijeća 2008/114/EZ. Nakon prve revizije (u kojoj su utvrđeni izazovi implementacije, suradnje i izvještavanja Komisije), Komisija je 2013. godine u Radnom dokumentu službi (Commission Staff Working Document (SWD(2013) final 318) o novom pristupu Europskom programu zaštite kritične infrastrukture: Učinkovitije osiguravanje europske kritične infrastrukture, naglasila potrebu razvoja zajedničkih alata i pristupa jačanju otpornosti i zaštiti kritične infrastrukture na razini Europske unije, naglašavajući međusobnu ovisnost i važnost dodatne suradnje između vlasnika/upravitelja kritične infrastrukture, industrije i država. Druga revizija je provedena tijekom 2018. i 2019. godine (utvrđena je djelomična učinkovitost glavnih aktera u postizanju zadanih ciljeva), a razultati su objedinjeni u Radnom dokumentu službi (SWD(2019) final 318) o novom pristupu Europskom programu zaštite kritične infrastrukture: Učinkovitije osiguravanje europske kritične infrastrukture, gdje su pružene vrlo korisne preporuke za daljnju suradnju i zaštitu europske kritične infrastrukture. Oba dokumenta pružaju neophodne informacije o promjenama koje se događaju unutar EU konteksta te ih je potrebno sagledati i uvažiti u izradi novog Zakona o kritičnoj infrastrukturi. Pored revizija, potrebno je analizirati naglaske svih EU strategija i procjena, u dijelu jačanja otpornosti i zaštite kritične infrastrukture, koje pored razvojne komponente daju i smjernice vezane uz nove rizike prema kritičnoj infrastrukturi i načine bavljenja njima. Neizostavna komponenta je i suradnja s akademskim i privatnim sektorom u osmišljavanju, razvoju, dizajnu, implementaciji i provedbi mjera jačanja otpornosti i zaštite kritične infrastrukture.

Na razini Republike Hrvatske, nakon donošenja Zakona o kritičnim infrastrukturama 2013. godine, bitno je osnažena strateško-sigurnosna dimenzija i arhitektura u kojoj je području kritičnih infrastruktura pridana značajna pažnja. U Strategiji nacionalne sigurnosti Republike Hrvatske iz 2017. godine (Narodne novine, broj 73/17), Republika Hrvatska se odredila

prema četiri strateška nacionalna interesa koje realiza putem devet strateških ciljeva. Jedan od strateških ciljeva je dostizanje najvišeg stupnja sigurnosti i zaštite stanovništva te kritičnih infrastruktura. Dio vezan uz kritičnu infrastrukturu izrazito je kvalitetno postavljen i pruža čitav niz političkih smjernica (neke od njih će biti izdvojene u sljedećem poglavlju), koje je potrebno razraditi i uvrstiti u novi Zakon o kritičnoj infrastrukturi. Jednako važno je da je Strategijom određeno uspostavljanje sustava domovinske sigurnosti koji treba osigurati usklađenu pripremu i provedbu propisa kojima će se određivati sigurnosne mjere i postupci važni za nacionalnu sigurnost, posebno zaštitu kritične infrastrukture. Sustav domovinske sigurnosti uspostavljen je Zakonom o sustavu domovinske sigurnosti (Narodne novine, broj 108/17), koji, pored zaštite kritične infrastrukture kao svrhe donošenja, izdvaja i potrebu ojačavanja funkcije upravljanja u izvanrednim i kriznim stanjima koja su rizik za nacionalnu sigurnost, uključujući i krizna stanja upravljana na razini Organizacije Sjevernoatlantskog ugovora i/ili Europske unije, kao i omogućavanja primjerenog doprinosa javnog i privatnog sektora te civilnog društva u zaštiti i jačanju nacionalne sigurnosti na svim razinama države i društva. Sve su ovo elementi koje je potrebno imati u vidu kod izrade novog Zakona.

Nacionalna strategija kibernetičke sigurnosti (Narodne novine, broj 108/15) donesena 2015. godine snažno naglašava važnost kritičnih infrastruktura općenito, te kritične komunikacijske i informacijske infrastrukture specifično, s ciljem: „povećanja otpornosti/smanjenja ranjivosti komunikacijskih i informacijskih sustava; umanjivanja posljedica negativnih događaja (prirodne i tehničko-tehnološke nesreće) i mogućih napada (namjernih i nenamjernih); omogućavanja brzog i učinkovitog oporavka te nastavka rada.“ Kritičnu komunikacijsku i informacijsku infrastrukturu predstavljaju oni komunikacijski i informacijski sustavi koji upravljaju kritičnom infrastrukturom ili su bitni za njezino funkcioniranje, a pristup njihovoj zaštiti holistički je postavljen sa svrhom integracije postojećih i razvoja novih procedura unutar sustava upravljanja u kibernetičkim krizama EU i NATO-a, kao i dovršetak nacionalnog sustava upravljanja kibernetičkim krizama. Iz ovog je dijela ovdje potrebno izdvojiti kako novi Zakon o kritičnoj infrastrukturi treba obuhvatiti smjernice i rješenja koje Europska unija i NATO Savez razvijaju u predmetnom području (navedeno i u Strategiji nacionalne sigurnosti), a velika količina znanja i iskustva o tomu postoji kako u Ministarstvu unutarnjih poslova, tako i u Ministarstvu obrane Republike Hrvatske i Zavodu za sigurnost informacijskih sustava.

Javno izvješće Sigurnosno-obavještajne agencije Republike Hrvatske za 2018. godinu navodi kako su „članice NATO-a i EU često [su] pod napadima malicioznih kibernetičkih kampanja koje imaju za cilj probijanje u zaštićene informacijske i komunikacijske sustave, pa je tako i Republika Hrvatska bila meta niza kibernetičkih napada posljednjih godina. Radi se o tzv. APT napadima (Advanced Persistent Threat – napredna trajna prijetnja) koje karakterizira visoka razina stručnosti i prikrivenosti u duljem razdoblju, vrlo složena organizacija i plan napada koji obuhvaća pažljivu selekciju mete (vladina tijela, kritična infrastruktura i sl.).“ Javno izvješće za 2017. godinu navodi kako je „uspješnost ovih napada pokazala nedostatak sigurnosnih politika koje bi svojom primjenom, odnosno proaktivnim mjerama i edukacijom povećale otpornost sustava, što je posebno važno u zaštiti kritičnih informacijskih i komunikacijskih infrastruktura.“ Ova dva citirana navoda su izdvojena kako bi pokazala potrebu robusnijeg i sveobuhvatnog pristupa ovom području i kako bi novi Zakon trebao odražavati svjesnost o novim rizicima i potrebnoj suradnji svih segmenata našeg društva.

Dodatno, novi Zakon o kritičnoj infrastrukturi treba naznačiti važnost adaptacije i izgradnje otpornosti na klimatske promjene definirajući obaveze privatnog sektora, znanstvenih institucija i tijela državne uprave kroz odredbe Zakona koje se odnose na moguću povezanost s kritičnim infrastrukturama i uslugama uvažavajući činjenicu da se klimatske promjene već događaju te da imaju značajan utjecaj na kritične infrastrukture. Novi Zakon treba prepoznati ove realnost, naznačiti ju i otvoriti prostor za suradnju i projekte u ovom području.

Normativna dimenzija

Za normativnu dimenziju Zakona potrebno je izdvojiti određena područja koja je nužno razmotriti na koji način ih najbolje uključiti, regulirati i usmjeriti u narednom razdoblju.

Iz Radnog dokumenta službi Komisije (SWD(2017) 0278 final) „Sveobuhvatna procjena sigurnosih politika Europske unije“ potrebno je izdvojiti tri područja koja su važna i novim Zakonom im treba otvoriti prostor za razvoj:

- Privatni sektor je većinski vlasnik glavnih elemenata kritične infrastrukture i kemijsko-bioloških-radioloških-nuklearnih postrojenja, zbog toga treba razviti veće partnerstvo s njim. Mjere sigurnosti i kontrole zahtijevaju uključivanje i privatnih i

javnih interesa. Privatnom sektoru mora se pružiti podrška za razvijanje vlastitih zaštitnih mehanizama na terorističke događaje.

- Kako se sve više oslanjaju na internetske tehnologije, kritične infrastrukture kao što su energetske mreže, satelitske komunikacije i zdravstveni sustavi postaju sve ranjiviji. Ovo je ključan izazov s kojim se suočava Unija i potrebne su zajedničke akcije na razini EU-a.
- Na području zaštite kritične infrastrukture potrebno je ostvariti sveobuhvatni pristup koji uključuje angažiranje znanstvenika, arhitekata i urbanih planera na dizajniranju budućih zgrada, sustava i javnih mjesta koja moraju biti sigurnija i bolje zaštićena.

Vezano uz ova tri područja potrebno je istaknuti značaj javno-privatnog partnerstva, nužnost povezivanja i harmonizaciju budućeg Zakona o kritičnoj infrastrukturi s drugim područjima i zakonima u Republici Hrvatskoj. Prvo, javno-privatno partnerstvo treba sagledati kao platformu istinske suradnje, komunikacije i koordinacije u kojoj će biti uključeni mnogobrojni akteri iz javnog, privatnog, akademskog sektora i civilnog društva (napisano u Strategiji nacionalne sigurnosti) u zaštiti i jačanju nacionalne sigurnosti na svim razinama države i društva. Zakon o javno-privatnom partnerstvu (Narodne novine, broj 78/12, 152/14, 114/18) ne prepoznaje područje kritičnih infrastruktura i navedeno je potrebno mijenjati, a oba zakona povezati. Trenutačno je u proceduri donošenja Zakon o privatnoj zaštiti, koji bi trebao snažnije nego do sada (Zakon je donesen 2013. godine, mijenjan i dopunjavan 2010. godine) otvoriti prostor suradnji javnog i privatnog sektora u području kritičnih infrastruktura. Strategija nacionalne sigurnosti navodi da „jačanje otpornosti nacionalne kritične infrastrukture na suvremene sigurnosne izazove i rizike zahtijeva istodobno održavanje i zaštitu nacionalnih kritičnih civilnih sposobnosti koje će pružiti potporu ukupnim sposobnostima koordiniranim sveobuhvatnim nastupom javnog i privatnog sektora, ponajprije sektora privatne zaštite.“ Također, kod izrade novog Zakona o kritičnoj infrastrukturi svakako treba sagledati i mnogobrojne preporuke Konfederacije europske industrije privatne sigurnosti o sigurnosti i zaštiti kritične infrastrukture. Potrebno je izdvojiti kako je u proceduri donošenja i novi Zakon o sustavu civilne zaštite, tako da bi izradu novog Zakona o kritičnoj infrastrukturi trebalo uskladiti i s rješenjima koja će biti predviđena u novom Zakonu o sustavu civilne zaštite. Bilo bi kvalitetno rješenje kada bi se mogla postići sinergija timova

koji rade na izradi navedenih zakona: Zakona o kritičnoj infrastrukturi, Zakona o privatnoj zaštiti i Zakona o sustavu civilne zaštite.

Zakon o kritičnoj infrastrukturi bi trebao otvoriti prostor i potaknuti promjene kod drugih zakona o načinu i komunikacijskim kanalima razmjene ključnih i osjetljivih informacija između svih dionika u zaštiti kritične infrastrukture (klasificirani podaci u zaštiti kritične infrastrukture). Trenutačno imamo veliki izazov kako takve podatke, odnosno informacije koje su proizvod analiza sigurnosno-obavještajnog sektora mogu doći do krajnjih korisnika, a to je privatni vlasnik odnosno upravitelj nacionalne kritične infrastrukture, koje su im neophodne u projektiranju, planiranju i zaštiti. Strategija nacionalne sigurnosti je stvorila pretpostavke da riješimo navedeno: „Razvit će se modeli razmjene podataka između državnih tijela i agencija i operatora kritične infrastrukture u javnom i privatnom vlasništvu radi pravodobnog upoznavanja s mogućim sigurnosnim prijetnjama i rizicima.“ Navedeni podaci, odnosno informacije su izuzetno značajne u zaštiti kritične infrastrukture i upravljanju u krizama, stoga moramo razviti model njihove sigurne i zaštićene razmjene između svih dijelova sustava – od javnog do privatnog sektora i natrag.

Vezano uz oslanjanje na internetske tehnologije i usluge, u području zaštite kritične komunikacijske i informacijske infrastrukture posebno je važna transpozicija Direktive 2016/1148 Europskog parlamenta i Europskog vijeća o mrežnoj i informacijskoj sigurnosti u zakonodavstvo Republike Hrvatske (NIS Direktiva). U vezi s time, 2018. godine donesen je Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Narodne novine, broj 64/18), kojim su uspostavljeni kriteriji za određivanje nacionalnih operatora ključnih usluga i pružatelja digitalnih usluga te dodatne zadaće pojedinih tijela u području kibernetičke sigurnosti. Predmetni Zakon i Zakon o kritičnoj infrastrukturi trebaju predstavljati dva lica istog novčića, jer normiraju isto područje i međusobno se nadopunjuju. U tom svjetlu treba izrađivati novi Zakon o kritičnoj infrastrukturi. Strateški treba sagledati da li navedena dva zakona u budućnosti pretvoriti u jedan. Isto tako, treba vidjeti je li sada prilika u izradi novog Zakona o kritičnoj infrastrukturi izjednačiti broj sektora u kojima je moguće identificirati i odrediti nacionalnu kritičnu infrastrukturu – s brojem sektora koje regulira Zakon o kibernetičkoj sigurnosti. Postojećim Zakonom o kritičnim infrastrukturama i podzakonskim aktima moguće je identificirati i odrediti nacionalne kritične infrastrukture u

čak jedanaest sektora (što do danas nije realizirano), dok normativnim okvirom Zakona o kibernetičkoj sigurnosti je to moguće u osam sektora. Kao i što treba voditi računa o fleksibilnosti u određivanju sektora u kojima se mogu identificirati kritične infrastrukture i usluge, jer rapidan razvoj informacijskih i komunikacijskih tehnologija će vjerovatno stvoriti nove sektore koji danas ne postoji, a koji će postati značajni s aspekta novih kritičnih infrastruktura i usluga.

Isto tako, novi Zakon treba sagledati smjernice Europske komisije iz Zajedničke komunikacije Europskom parlamentu i Vijeću (JOIN(2016) 18 final) Zajednički okvir za suzbijanje hibridnih prijetnji – odgovor Europske unije iz 2016. godine, koje naglašavaju sve veću hibridnu opasnost i ugrožavanje europske kritične infrastrukture. Za Republiku Hrvatsku bi bilo korisno izraditi snažan normativan okvir suprostavljanju hibridnim ugorzama, a do tada treba se poslužiti smjernicama iz navedene Komunikacije i ovom području posvetiti pozornost pri izradi novog Zakona o kritičnoj infrastrukturi.

Kako bi novi Zakon o kritičnoj infrastrukturi bio ne samo usklađen s EU smjernicama i harmoniziran s hrvatskim normativnim rješenjima, već bio i proaktivan u smislu otvorenosti prema znanosti, novim znanjima i tehnologijama, trebalo bi otvoriti prostor suradnji s domaćim tvrtkama, znanstvenicima, arhitektima i urbanim planerima (gdje imamo u pojedinim područjima svjetsku ekspertizu) na dizajniranju budućih fizičkih i virtualnih kritičnih infrastruktura i usluga. Rješenja i znanje o tome postoje u Republici Hrvatskoj, a korisna su iskustva i Zajedničkoga istraživačkog centra Europske komisije u Ispri, Italija, koja do sad nismo koristili na adekvatan način. Potom, suradnja mora biti otvorena i prema gradovima jer se sva naša nacionalna kritična infrastruktura i usluge pretežno nalaze u gradovima pa je nužna suradnja državne i lokalne razine vlasti u ovom području.

Za izradu novog Zakona bitno je izdvojiti još dvije političke smjernice za razvoj javnih politika koje su dane u Strategiji nacionalne sigurnosti. Prva se odnosi na traženi diskurs da se zaštita kritične infrastrukture usmjeri „na prevenciju, uklanjanje ili ublažavanje rizika koji mogu izazvati ranjivost kritičnih infrastruktura te jačanje njihove otpornosti. Sustav upravljanja i nadzora nad pojedinim kritičnim infrastrukturama potrebno je kontinuirano nadograđivati i poboljšavati, uz primjenu najboljih iskustava koja na tom području imaju druge države.“ Ovdje se otvara prostor raspravi koja je šira od onog što si je zakonodavac

zadao da će novim Zakonom normirati, regulirati i urediti, a tiče se upravljanja u krizama (ili upravljanja krizama). Područje upravljanja u krizama je mnogostruko šire od samog predmeta zaštite kritične infrastrukture, gdje su kritične infrastrukture dio procesa upravljanja u krizama. Naznake potrebe razvoja nacionalnog sustava upravljanja u krizama dane su u Strategiji nacionalne sigurnosti, Nacionalnoj strategiji kibernetičke sigurnosti, Zakonu o sustavu domovinske sigurnosti te njegovog povezivanja na sustave upravljanja u krizama NATO Saveza i Europske unije. Novi Zakon treba otvoriti i navedeno područje, a kao primjer možemo uzeti zakone Češke i Poljske koje su jednim zakonom regulirale materiju upravljanja u krizama i zaštite kritične infrastrukture. Stoga bi politička razina sustava domovinske sigurnosti trebala odlučiti hoće li se ova dva područja regulirati u jednom ili dva odvojena zakona.

Druga važna politička smjernica iz Strategije nacionalne sigurnosti se odnosi na „izradu dokumenata koji definiraju politiku i metodologije upravljanja kritičnim infrastrukturama i ograničenim nacionalnim dobrima, jasno odrediti koji njihovi dijelovi moraju ostati u većinskom vlasništvu države, čime će se onemogućiti ugrožavanje vitalnih funkcija važnih za državu i stanovništvo u slučajevima poslovnih nestabilnosti.“ Ovo je izuzetno važno i ključno područje koje novi Zakon o kritičnoj infrastrukturi mora obuhvatiti i razraditi. Kao država više nismo vlasnici dijela infrastruktura i usluga (bankarski i financijski sektor, komunikacijske i informacijske usluge, itd.) koje su nam bitne i neophodne o pitanjima nacionalne i javne sigurnosti stoga moramo ojačati suradnju s vlasnicima odnosno upraviteljima tih infrastruktura i usluga te svakako regulirati kako postupati s dijelom nacionanih kritičnih infrastruktura i usluga koje su još uvijek u državnom vlasništvu.

Operativna dimenzija

Novi Zakon, pored analize strateškog, sigurnosnog i razvojnog okruženja, prihvaćanja EU i NATO smjernica, potrebe konkretnije suradnje s međunarodnim organizacijama i domaćim partnerima, slijeđenja nacionalnih prioriteta i politika, mora biti dobro balansiran i u dimenzijama kojima će se baviti, poput: prevencije, pripravnosti, odnosno reakcije u stvaranju i djelovanju mreža, objekata i sustava od nacionalne važnosti. Možda će zakonodavac odlučiti staviti veći naglasak na jednu od navedenih dimenzija. Ako se odluči veću pažnju posvetiti

prevenciji, onda svakako treba razmotriti elemente jačanja otpornosti kritičnih infrastruktura koje će postići naglašavajući potrebu osmišljavanja, dizajna, izgradnje, rada i nadzora nad novim kritičnim infrastrukturama i uslugama koje ćemo razvijati u budućnosti, kao i rekonceptualizaciju postojećih metoda i rješenja upravljanja trenutačnim kritičnim infrastrukturama i uslugama. U slučaju naglaska na pripravnost funkcioniranja kritičnih infrastruktura i usluga naspram sektorskih i međusektorskih rizika potrebno je istaknuti dio zaštite kritičnih infrastruktura sa svim elementima koji nam kao državi i društvu stoje na raspolaganju. S druge strane, u dijelu reakcije naglasak treba staviti na razvoj sustava upravljanja u krizama u kojem će budući sustav zaštite kritične infrastrukture biti integralni dio.

Novi Zakon svakako treba naznačiti problematiku upravljanja, koordiniranja, zapovijedanja u krizama i katastrofama u odnosu na kritičnu infrastrukturu, i koje su poveznice, odnosno odnosi prema drugim zakonima i koordinativnim sustavima koje su drugi zakoni uspostavili / povezali. Treba napraviti poveznicu i odnos prema odredbama Zakona o sustavu domovinske sigurnosti (i Koordinaciji za sustav domovinske sigurnosti i Vijeću za nacionalnu sigurnost), kao i odredbama Zakona o sustavu civilne zaštite (i Stožeru civilne zaštite na državnoj razini). Isto tako, treba sagledati izazove i rizike koji nastaju unutar granica Republike Hrvatske, kao i prekogranične utjecaje, a koji mogu utjecati na kritičnu infrastrukturu te potrebi da sustav jačanja otpornosti i zaštite se različito modelira ovisno o rizicima s kojima se susrećemo.

To nas dovodi do razmatranja poveznice sa središnjim tijelom državne uprave ili sustavom domovinske sigurnosti koji bi trebao biti sistemski nadležan za cjelokupno upravljanje i koordinaciju jačanja otpornosti i zaštite kritične infrastrukture i usluga. S aspekta razvoja područja kritičnih infrastruktura i usluga kao platforme neophodne za održavanje postojećeg stanja i napredak u budućnosti, potrebno je razmotriti ulogu Ministarstva mora, prometa i infrastrukture, koje je već zaduženo za upravljanje i koordinaciju ključnim infrastrukturnim područjima od državnog značaja, te bi moglo koordinirati i područjem kritičnih infrastruktura. Ako će naglasak u Zakonu biti na upravljanju kritičnim infrastrukturama s pozicije njihove zaštite onda je prirodno da to područje bude dio poslova i obveza koordinacije Ministarstva unutarnjih poslova. Dok, ako postoji vizija sveobuhvatnog pristupa svim dimenzijama kojima se bave kritične infrastrukture i usluge i koje navedene pružaju i omogućavaju, tada bi

Zakonom trebalo dati veću poveznicu prema koordinaciji unutar sustava domovinske sigurnosti. Ovdje se otvaraju i dodatna pitanja, koja su izuzetno važna, a odnose se na uspostavu primjerenoga organizacijskog modela sustava upravljanja kritičnim infrastrukturama, koje će imati znatne posljedice za razvoj ovog područja.

Dodatno, Zakon treba regulirati i unaprijediti područje edukacije i osposobljavanja svih ključnih dionika ovog područja, od vlasnika odnosno upravitelja kritičnih infrastruktura, svih segmenata javnog sektora koji je vezan uz ovo područje, predstavnika regulatornih agencija, sigurnosnih menadžera i pogotovo časnika za vezu, donositelja odluka, akademskog i civilnog sektora. Zakon mora urediti partnerski odnos s privatnim vlasnicima odnosno upraviteljima kritičnih infrastruktura i usluga. Važno područje je i zajedničko ulaganje – kao i podjela odgovornosti – javnog i privatnog sektora u sustave jačanja otpornosti i zaštite kritične infrastrukture. Modeli su poznati (poput Finske i nekih drugih država), gdje se obveze koje zakonodavac propisuje privatnom vlasniku zajednički dogovaraju i uspostavljaju, gdje postoje određeni benefiti za privatnog vlasnika (jer se postavlja pitanje zašto bi privatni vlasnik pristao biti nacionalnom kritičnom infrastrukturom ako mu navedeno donosi samo financijski trošak) i/ili gdje se zajednički uspostavlja fond iz kojeg se financiraju strukturne promjene ili nadogradnja u sustavu.

Zaključak

Ova analiza je imala višestruke ciljeve: prikazati trenutačno područje razvoja područja jačanja otpornosti i zaštite kritične infrastrukture (i usluga) u Republici Hrvatskoj, predložiti određene elemente i ideje zakonodavcu pri izradi novog Zakona o kritičnoj infrastrukturi, i skrenuti pozornost na strateške, zakonodavne i operativne dimenzije i otvorena pitanja o kojima je potrebno voditi računa u tom procesu.

Izrada novog Zakona je prilika napraviti snažniji i robusniji normativni okvir, uključiti sve aktere našeg društva, otvoriti dijalog s privatnim i akademskim sektorom te civilnim društvom, napraviti kvalitetan i sveobuhvatan Zakon koji će biti suvremen i moderan jer znanje za to postoji kako u resornim ministarstvima tako i u stručnoj i znanstvenoj javnosti.

doc. dr. sc. Robert Mikac
zamjenik predsjednika Instituta za sigurnosne politike

Kako navoditi ovu analizu kao izvor:

Mikac, Robert (2020), Elementi za izradu novog Zakona o kritičnim infrastrukturama Republike Hrvatske, Institut za sigurnosne politike, godina 2020, broj 004, dostupno na: http://insigpol.hr/download-file/8234/