*Iztok PREZELJ**

PREGLEDNI ZNANSTVENI ČLANEK

NACIONALNA KRITIČNA INFRASTRUKTURA V REPUBLIKI SLOVENIJI

Povzetek. *Nacionalna kritična infrastruktura zajema vse podporne sociotehnične sisteme, ki družbi omogočajo nemoteno in stabilno delovanje. Sem sodijo predvsem energetski, prometni, telekomunikacijski, informacijski, finančni, zdravstveni in drugi sistemi, katerih moteno delovanje bi lahko ogrozilo stabilnost in celo varnost sodobne družbe in države. Relevantnost kritične infrastrukture se je v nedavni preteklosti povečala predvsem zaradi terorističnega delovanja, ki se v veliki meri usmerja tudi na tovrstno infrastrukturo. Cilj tega članka je opredeliti varnostni pomen nacionalne kritične infrastrukture ter analitično in sintetično prikazati kritično infrastrukturo v Sloveniji. Avtor je v članku identificiral številne infrastrukture oziroma sektorje, ki bi jih lahko označili kot družbeno in varnostno kritične v Sloveniji. Ti sektorji so večinoma mrežno strukturirani, različno razvejani, kompleksni ter kritični, kar pokaže indeks kritičnosti.*

Ključne besede: *kritična infrastruktura, Slovenija, grožnje, tveganja, objekti, indeks kritičnosti, nacionalna varnost.*

Uvod

Izzivi novega tisočletja vodijo sodobno obramboslovno znanost k novim področjem proučevanja, ki sodobno varnost in zagotavljanje le-te obravnavajo s specifičnega zornega kota.[1] Eno izmed takšnih področij se nanaša na proučevanje ogroženosti in zaščite temeljnih družbenih infrastrukturnih objektov oziroma sistemov. Knight in Sullivan (2000: 1) sta v zvezi s tem ugotavljala, da se je veliko večjih infrastrukturnih sistemov tako razvilo, da so družbe in pripadajoče organizacije postale zelo odvisne od njih. V določenih

* *Dr. Iztok Prezelj, docent na Fakulteti za družbene vede, Univerza v Ljubljani.*

[1] *Novosti v družboslovni znanosti je treba dojemati z rahlim pridržkom. Izkaže se, da marsikaj »novega« dejansko ni povsem novo, saj so se s tem ukvarjali že znanstveniki v preteklosti, vendar v rahlo drugačni preobleki. Tipičen primer je »odkrivanje« t. i. novih groženj varnosti (npr. okoljske, kriminalitetne, gospodarske, imigrantske grožnje) po koncu hladne vojne, kar pa ne pomeni, da te grožnje niso obstajale že prej. Spremenilo se je predvsem človekovo zaznavanje, zaradi katerega so v ospredje lahko prišle druge, prej bolj zapostavljene grožnje.*

primerih so takšni sistemi tako razširjeni in pomembni, da je normalno delovanje družbe povsem odvisno od njihovega stalnega delovanja. Ellison in sodelavci (1999) so dodatno ugotavljali, da družbena odvisnost od kritične infrastrukture vedno bolj narašča, Koubatis in Schonberger (2005: 212) pa sta menila, da brez teh sistemov ni mogoče niti razmišljati o normalnem življenju.

Pojmovanje kritične infrastrukture se je sčasoma spremenilo zaradi razvoja tehnologije in še posebej zaradi vzpona terorizma. Nekoč se je med najpomembnejšo infrastrukturo uvrščalo tiste infrastrukture, katerih daljše motenje bi lahko povzročilo večje vojaške in ekonomske posledice (Dunn, 2005: 264; Moteff v Hellstrom, 2006: 5). Dandanes pa je kritična infrastruktura izjemno široka kategorija. Lewis (2006: 29) celo meni, da je težko identificirati sektorje, ki niso v nekem smislu kritični. Dunnova (2005: 264) ugotavlja, da je delni razlog spreminjanja v tem, da je opredeljevanje kritične infrastrukture subjektivna kategorija (»lies in the eyes of the beholder«), Moteff in Parfomak (2004) pa sta izpostavljala pomen konteksta, ki vpliva na razumevanje kritične infrastrukture. Obe ugotovitvi se po moji oceni odražata v spremenjenih varnostnih okoliščinah in družbenem zaznavanju le-teh. Z drugimi besedami, spremenjene grožnje varnosti in naše zaznavanje tega so privedli do širšega opredeljevanja kritične infrastrukture v sodobnih državah.

Kaj vse torej danes zajema sodobno pojmovanje nacionalne kritične infrastrukture? Schulman in Roe (2006) opredeljujeta kritično infrastrukturo kot temeljne zmogljivosti, tehnične sisteme in organizacije, ki zagotavljajo zmogljivosti. Vse navedeno omogoča zagotavljanje velikega spektra družbenih aktivnosti, dobrin in storitev. Infrastrukture so po svoji naravi večnamenske. Ellison in sodelavci (1999), Boin, Lagadec, Michel-Kerjan in Overdijk (2003: 100), Lewis (2006), Nozickova in Turnquist (2005), Schulman in Roe (2006) in drugi kritične infrastrukture pojmujejo predvsem kot mreže, ki zagotavljajo prometne, finančne, komunikacijske, preskrbne, elektroenergetske in podobne transakcije. Dokaj podobno pojmuje kritično infrastrukturo tudi Michel-Kerjan (2003: 134), ki jo opredeljuje kot kompleksni sistem elementov, ki so med seboj vedno bolj povezani. V kritično infrastrukturo uvršča industrije, institucije in distribucijske mreže ter sisteme, ki zagotavljajo neprekinjen tok dobrin in storitev, ki so nujne za varnost in blagostanje prebivalstva. Obstaja še mnogo drugih avtorjev, ki pa predvsem ponavljajo katero od državnih opredelitev kritične infrastrukture (še posebej pogosto ameriško opredelitev).[2]

[2] *Na tej točki pa je vendarle treba poudariti, da ne obstaja univerzalno mednarodno soglasje o opredelitvi kritične infrastrukture. Področje kritične infrastrukture je namreč razmeroma mlado področje, ki se sooča s številnimi dilemami, kar je posledično pripeljalo do opaznih meddržavnih razlik pri opredeljevanju kritične infrastrukture.*

Ugotovimo lahko, da sodobna znanost in praksa izpostavljata in se usmerjata še posebej na naslednje kategorije oziroma sektorje kritične infrastrukture:

- energetiko (proizvodnja in distribucija nafte, plina ter električne energije),
- promet (cestni, železniški, zračni in pomorski oziroma vodni promet),
- informacijske in komunikacijske sisteme (ICT), kar zajema predvsem internet, fiksne in mobilne telekomunikacije,
- sisteme za preskrbo z vodo, kar zajema zagotavljanje pitne vode, nadzor kakovosti vode in nadzor količine vode,
- sisteme za preskrbo s hrano, kar zajema pridelavo hrane, predelavo, distribucijo in prodajo,
- finančne sisteme za trgovanje, plačila, kliring, poravnave in druge finančne instrumente,
- zdravstvene sisteme, kar zajema predbolnišnično in bolnišnično oskrbo, vključno z laboratoriji,
- kemično industrijo,
- jedrsko industrijo.

Nekateri (avtorji ali pa države) pod kritično infrastrukturo uvrščajo tudi oborožene sile, policijo, sodstvo, kulturne spomenike ipd. Z vidika znanosti in stroke pa je bistveno, da se ohranja odprto opredelitev kritične infrastrukture, v katero bodo sčasoma vstopali novi elementi.[3]

Ključni problem v zvezi z nacionalno kritično infrastrukturo je v njeni večrazsežnosti (mnoštvo sektorjev in podsektorjev) in vzajemni prepletenosti v nacionalnih in mednarodnih okvirih. Kompleksnost celovitega urejanja zaščite kritične infrastrukture v okviru zagotavljanja nacionalne varnosti je posledično tako velika, da je v prvi fazi nujno izvesti celovito analizo kritične infrastrukture, ki izpostavlja medsektorske oziroma čezsektorske podobno-

[3] *Široko pojmovanje kritične infrastrukture je sicer primeren način razumevanja tega področja, saj le kompleksni koncepti lahko pojasnjujejo kompleksno stvarnost. Vendar pa zelo široko razumevanje kritične infrastrukture prinaša s seboj določena analitična in metodološka tveganja, katerih se moramo zavedati. V tem smislu se je na področju varnostnih študij izrazilo opozorilo, da izjemno široki pristopi k razumevanju groženj in varnosti lahko pripeljejo do »inflacije koncepta« (glej Politi, 1997: 13) oziroma da začnejo ogrožati koherentnost koncepta (Terriff, Croft, James in Morgan, 1999: 169; Prins, 1998: 788). Navedeni avtorji ugotavljajo, da so bile varnostne študije na svojem začetku zares specifična smer mednarodnih odnosov, kasneje pa so postale fragmentirane na več perspektiv oziroma pogledov, ki sploh niso v konstruktivnem dialogu – predvsem zaradi razlik v (pred)znanju in odnosu do pojava varnosti. Teoretični pristopi govorijo drug čez drugega, kljub temu da proučujejo isti pojav – varnost družbe. Problem področja kritične infrastrukture je podoben, saj ob uveljavljanju širokega pristopa oziroma razumevanja hkrati obstaja veliko parcialnih disciplinarnih pristopov, ki nekako ne uspejo ustvariti interdisciplinarnega dialoga. Poskusi širokega pristopa na tem področju pa izgubljajo tehnično konkretnost na račun pridobivanja filozofske širine, kar vodi v tveganje inflacije koncepta. Ob zavedanju te nevarnosti pa je vendarle treba priznati, da so analitiki kritične infrastrukture zmanjšali to tveganje z logiko reduciranja analitične, metodološke in varnostne pozornosti samo na najbolj kritične objekte in procese.*

sti in razlike. Zgolj z multi- in interdisciplinarno analizo lahko natančno določimo stanje na področju kritične infrastrukture v konkretni državi. Cilj tega članka je ovrednotiti varnostni pomen kritične infrastrukture in analizirati nekatere njene ključne parametere v Republiki Sloveniji. Preverjena bo predpostavka, da delovanje slovenske družbe temelji na številnih podpornih sistemih, ki so lahko bolj ali manj varnostno kritični. Pri tem gre večinoma za mrežno strukturirane in mednarodno integrirane sektorje oziroma podsektorje, ki so podvrženi dokaj širokemu spektru potencialnih groženj in tveganj ter temeljijo na omejenem številu kritičnih objektov. V sklepnem delu bodo izpostavljene ključne policy dileme, s katerimi se bo morala soočiti Slovenija v bližnji prihodnosti, če bo hotela kredibilno zaščititi svojo kritično infrastrukturo in izpolnjevati pričakovanja ter zahteve EU, izpostavljene v direktivi.

Varnostna kritičnost kritične infrastrukture

Zagotavljanje zaščite kritične infrastrukture naj bi temeljilo na dobro utemeljenem razumevanju kritičnosti infrastruktur. Ena od prvih predpostavk zaščite kritične infrastrukture je namreč v razumevanju, kaj pomeni kritično pri vsaki od relevantnih infrastruktur. Pommerening (2004) ugotavlja, da so infrastrukture kritične zato, ker so nujne za delovanje sodobnih družb in ker gre za velike tehnične sisteme, ki so še posebej ranljivi na raznovrstne motnje. Po Auerswaldu, Branscombu, La Portu in Michel-Kerjanu (2005: 78) pa je infrastruktura vedno kritična, ko so storitve, ki jih zagotavlja, kritične za nacionalno varnost. Reinermann in Weber (2003) menita, da je kritični infrastrukturni sektor tisti, katerega motenje bi lahko imelo resne posledice za javnost. Schulman in Roe (2006) pa v tovrstno pojmovanje kritičnosti prinašata razumevanje, ki izpostavlja kritičnost posameznega sektorja ravno zaradi posledic njegovega nedelovanja na druge družbene dejavnosti in zmogljivosti. Varnostni pomen kritične infrastrukture je torej mogoče videti še posebej v varnostnih razsežnostih posledic njenega nedelovanja oziroma omejenega delovanja. Ko ljudje ne bi imeli na voljo učinkovite preskrbe s hrano, z vodo, s temeljnimi energenti, kot so elektrika, nafta in plin, poleg tega pa ne bi delovali sistemi za izvajanje plačilnih prenosov ali sistemi zdravstvene oskrbe, bi skoraj zagotovo prišlo do specifične družbene krize. V primeru neuspešnega obvladovanja takšne krize bi zagotovo prišlo do varnostnih situacij, v katerih bi bil ogrožen fizični obstoj posameznikov.

Eden od ključnih problemov v zvezi z določanjem kritičnosti je v tem, da se njena opredelitev skozi čas spreminja, kar smo ugotovili že zgoraj. Danes se denimo pod kritično infrastrukturo v ZDA in Kanadi pojmuje tudi nacionalne spomenike (glej Dunn, 2005: 264; Auerswald, Branscomb, La Porte in Michel-Kerjan, 2005). Mnogo avtorjev ugotavlja, da je opredejevanje kritič-

nosti lahko izjemno težka naloga (npr. Moteff in Parfomak 2004). Nekateri, denimo, ugotavljajo, da je izredno težko razlikovati med kritično in nekritično infrastrukturo. Ravno soodvisnost med mrežami kritične infrastrukture napeljuje, da je tovrstno razlikovanje ničvredno oziroma zaman. Tudi motnje infrastruktur, ki jih morda ne označimo kot kritične, namreč lahko pripeljejo do pomembnih posledic. Tako bi npr. dvotedenski zastoj pri delovanju komunalnega sistema v večjem mestu bi lahko povzročil že kaos, ugotavljajo Boin, Lagadec, Michel-Kerjan in Overdijk (2003: 100). Tudi Johnson (2006: 3) ugotavlja, da ravno omenjena soodvisnost med sektorji povratno otežkoča natančno definiranje, kaj je del in kaj ni del kritične infrastrukture. V tem smislu Hellstrom (2006: 5) govori o tveganju, da kritična infrastruktura postane vse, kar je pomembno za delovanje družbe; to z drugimi besedami pomeni: nič specifičnega, na kar bi se lahko osredotočili pri njeni zaščiti. Tudi Lewis (2006) ugotavlja, da vse kritične infrastrukture preprosto ni mogoče zaščititi, zato se je treba osredotočiti na ožje elemente. Johnson (2006: 3) v tem smislu govori o razlikovanju med primarnimi in sekundarnimi sistemi. Med prve uvršča najboj ranljive elemente v nacionalni infrastrukturi.

V literaturi je tako mogoče zaslediti tri povezane pristope v zvezi z zmanjševanjem širine kritične infrastrukture. Izhodišče pristopov je v tem, da v določenem sektorju, ki je označen za kritično infrastrukturo, ni seveda vse kritično v smislu zgornje opredelitve. Kritični so samo nekateri procesi (pristop A) oziroma nekatere točke (pristop B)[4] ali nekateri elementi (pristop C).[5] Po Lewisovem (2006: 16) mnenju je ključni razlog za redukcijo v kasnejši obvladljivosti zaščite kritične infrastrukture. S pomočjo določitve kritičnega v okviru določene infrastrukture v bistvu izjemno kompleksni problem zreduciramo v bolj obvladljiv problem. Če se usmerimo na zaščito kritičnih točk ali procesov, posledično vodi k optimalnejši zaščiti kritične infrastrukture v okviru sektorjev z najmanjšimi stroški.[6]

[4] *Med elementi sistema kritične infrastrukture so po Michel-Kerjanu (2003: 134) le nekateri kritični. To so tisti, katerih uničenje ali onemogočenje bi ohromilo celotne regije, če že ne države.*

[5] *Hellstrom (2006: 12) v tem smislu ugotavlja, da kritične infrastrukture niso kritične samo zato, ker so na splošno pomembne, temveč ker s svojo strateško povezanostjo odražajo popolno družbeno ranljivost na samo nekaj ključnih točkah v sistemu.*

[6] *Dejstvo je, da vse kritične infrastrukture v določeni državi preprosto ni mogoče zaščititi, zato se je treba usmeriti na kaj bolj konkretnega in obvladljivega. Pri tem pa Reinermann in Weber (2003) opozarjata, da govorimo o več ravneh kritičnosti, kot so poslovna, sektorska in družbena raven. S stališča družbe, kar nas v tem članku najbolj zanima, niso relevantni vsi kritični procesi v podjetjih. Vsi kritični procesi na nižji ravni niso nujno kritični tudi na višji ravni. Tako, denimo, onemogočenje delovanja kritičnega procesa v posameznem podjetju zelo verjetno ne bo imelo nobenega resnega učinka na družbo. To pa nujno ne drži, če ima takšno podjetje velik tržni delež v sektorju ali pa celo monopol.*

Pristop k proučevanju kritične infrastrukture v Republiki Sloveniji

Republika Slovenija se je v okviru zagotavljanja nacionalne in mednarodne varnosti znašla v razmerah, ko bi morala opredeliti lastno kritično infrastrukturo in njene elemente, ki bi jih lahko imenovala za evropsko kritično infrastrukturo (EKI). Ključna spodbuda za to je prišla iz EU. Evropski svet je junija 2004 zaprosil Evropsko komisijo, naj pripravi celovito strategijo za varovanje kritične infrastrukture. Komisija je oktobra 2004 sprejela Sporočilo o varovanju kritične infrastrukture v boju proti terorizmu, v katerem je dala jasne predloge glede okrepitve preprečevanja terorističnih napadov na kritično infrastrukturo in s tem povezano pripravljenostjo v Evropi. Svet je v sklepih o »preprečevanju, pripravljenosti in odzivu na teroristične napade« in v »Solidarnostnem programu EU o posledicah terorističnih groženj in napadov« iz decembra 2004 podprl namero Komisije, da predlaga Evropski program za varovanje kritične infrastrukture (EPCIP), in se strinjal z vzpostavitvijo informacijskega omrežja za opozarjanje o kritični infrastrukturi (CIWIN). Komisija je novembra 2005 sprejela Zeleno knjigo o evropskem programu za varovanje kritične infrastrukture, v kateri so bile določene politične možnosti o načinu, kako bo Komisija vzpostavila EPCIP in CIWIN (glej Green Paper on a European Programme for Critical Infrastructure Protection, 2005). Komisija je decembra 2006 predlagala direktivo Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja. Ta predlog direktive je predstavil ukrepe glede ugotavljanja in določanja evropske kritične infrastrukture (EKI) ter oceno potrebe za izboljšanje njene zaščite in varovanja (glej Predlog direktive Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja, 2006; 2008). Slovenija je za izpolnjevanje obveznosti, ki jih je predvidevala direktiva, ustanovila Medresorsko koordinacijsko skupino za zaščito kritične infrastrukture in razpisala raziskovalni projekt Definicija in zaščita kritične infrastrukture v RS.[7] Ratifikacija evropske direktive se je zapletla zaradi nesoglasij med državami glede lastne EKI,[8] zato je v Sloveniji prišlo do sklepa, da se nacionalno kritično infrastrukturo opredeli v celoti za nacionalne potrebe ter v čim večji meri v skladu s pričakovanimi kriteriji za določitev EKI.[9]

[7] *Projekt sta financirala MO RS in ARRS. Ta članek je nastal v sklopi diseminacije projektnih rezultatov.*

[8] *Nesoglasja so se še najbolj videla med velikimi in majhnimi državami, ki se niso mogle sporazumeti o kriterijih v zvezi z višino škode. Določena višina škode v primeru nedelovanja določene infrastrukture v veliki državi bi se komaj poznala, medtem ko bi v mali državi prišlo že do nacionalne katastrofe.*

[9] *Na koncu izjemno zahtevnega procesa usklajevanja je bila vendarle sprejeta okrnjena direktiva, ki predstavlja prvi korak v postopnem pristopu za ugotavljanje in določanje EKI. Sama direktiva je usmerjena zgolj na energetski in prometni sektor, medtem ko so drugi sektorji za zdaj izpuščeni. To pomeni, da morajo države določiti objekte EKI v podsektorju energetike, nafte, plina, cestnega, železniškega, zračnega in vodnega prometa. Države članice in lastniki oziroma upravljavci te infrastrukture morajo imeti varnostne*

V okviru omenjenega raziskovalnega projekta je bil tako oblikovan vprašalnik, na katerega so na osemnajstih podsektorskih delavnicah odgovarjali številni državni in zasebni upravljalci najpomembnejše infrastrukture iz RS. Delavnice so bile od januarja in marca 2008.[10] V nadaljevanju predstavljamo medsektorsko sintezo stanja kritične infrastrukture v RS po nekaterih ključnih parametrih, ki jo je avtor opravil v okviru projekta. Sinteza gradi na rezultatih delavnic in jih analitično povezuje ter v tem smislu presega. Zaradi potrebe po utemeljitvi pristopa se podajanje rezultatov prepleta tudi z nekaterimi bistvenimi teoretičnimi izhodišči.

Kritični infrastrukturni sektorji v Sloveniji

Kritična infrastruktura v Sloveniji je zelo razvejana in kompleksna. Analiza pokaže, da so vsi zgoraj opredeljeni sektorji in njihovi podsektorji utemeljeno kritični. Na splošno lahko relevantnost in kritičnost posameznih sektorjev utemeljimo tako, kot je prikazano v nadaljevanju.

- Sektor promet omogoča prehajanje prebivalstva, tovora in drugih kategorij v prostoru po kopnem, zraku in morju. Nemoteno gibanje prebivalstva je prvi pogoj za normalno delovanje katere koli družbe.
- Sektor IKT (informacijska in komunikacijska tehnologija) omogoča zbiranje, prenos, obdelavo in prikaz podatkov v podporo odločanju, nadziranju in analiziranju. V informacijski družbi vedno več dejavnosti temelji na nemotenosti tega procesa.
- Sektor finance omogoča izvajanje plačilnega prometa med akterji, kot so država, poslovni subjekti, banke, prebivalstvo ipd. Sodobna razvita družba temelji na nemotenem delovanju plačilnih instrumentov, kar z drugimi besedami pomeni nemoteno poslovanje nedržavnih in državnih subjektov.

načrte, varnostne uradnike, kontaktno točko z EU, poleg tega pa morajo tudi ocenjevati tveganja, groženje in ranljivosti. Po pregledu te direktive, ki se bo izvedel tri leta po začetku njene veljavnosti, se lahko torej po potrebi določijo še drugi sektorji, v katerih se bo ta direktiva izvajala (Council Directive on the Identification and Designation of European Critical infrastructures and the Assessment of the Need to Improve their Protection, 2008). Iz razprav pri sprejemanju direktive je razvidno, da bi bilo pri tem treba nameniti prednost sektorju informacijske in komunikacijske tehnologije.

[10] Delavnice so bile izvedene v naslednjih sektorjih in pripadajočih podsektorjih: energetika (preskrba z nafto, preskrba s plinom in preskrba z elektriko), promet (cestni, železniški, pomorski in zračni promet), zdravje (predbolnišnična oskrba, bolnišnična oskrba in podsektor zdravil, serumov, cepiv, farmacevtskih proizvodov, biolaboratorijev in bioagensov), jedrsko gorivo, informacijska in komunikacijska tehnologija (IKT-informatika, IKT-komunikacije in strojna oprema), voda (zagotavljanje pitne vode, nadzor kakovosti vode in nadzor količine vode), preskrba s hrano, finance (infrastruktura za trgovanje, plačila, kliring in poravnave ter sistemi finančnih instrumentov) in kemična industrija. Vprašalnik je vključeval enajst sklopov vprašanj kvalitativne in kvantitativne narave. Delavnice je nadzirala vladna Medresorske koordinacijske skupine za zaščito kritične infrastrukture in resornih ministrstev. Na delavnicah so v vsakem podsektorju sodelovali vsi odgovorni upravljavci javnega in zasebnega značaja, za samo izvedbo pa je bilo odgovornih več raziskovalcev.

- Sektor energetika omogoča proizvodnjo, prenos oziroma distribucijo in skladiščenje temeljnih energentov, kot so elektrika, nafta in zemeljski plin. Distribucija energentov v določenih primerih vključuje tudi uvoz (npr. v primeru nafte in zemeljskega plina, ker nimamo lastne proizvodnje, in deloma tudi v primeru električne energije). Delovanje sodobne družbe v veliki meri temelji na uporabi navedenih energentov.
- Jedrski sektor v RS ne zagotavlja proizvodnje in predelave jedrskih cepljivih snovi, ampak temelji na skladiščenju teh snovi in njihovi uporabi za proizvodnjo elektrike. Dejavnost zagotavljanja pravilnosti in nemotenosti procesa skladiščenja nizko, srednje in visoko radioaktivnih snovi je družbeno kritična, prav tako pa tudi proizvodnja električne energije na osnovi jedrskega goriva.
- Sektor hrana zagotavlja hrano in njeno neoporečnost v RS. Gre za zagotavljanje temeljnega življenjskega sredstva za vsakega posameznika, pri čemer smo v 60 odstotkih odvisni od uvoza (RS ni samozadostna v tem pogledu).
- Sektor voda zagotavlja vodo in nadzor nad njeno kvaliteto in kvantiteto. Voda je temeljno življenjsko sredstvo za vsakega posameznika in temeljni vir pri pripravi hrane ter v industriji.
- Sektor zdravje zagotavlja predvsem predbolnišnično in bolnišnično oskrbo, proizvodnjo, transport in shranjevanje zdravil ter laboratorijsko dejavnost. Zdravje je fizično in duševno stanje vsakega posameznika, ki je nujen predpogoj za doseganje kakršnih koli bolj ali manj družbeno relevantnih ciljev.
- Sektor kemična industrija omogoča proizvodnjo, shranjevanje (skladiščenje) in predelavo kemičnih snovi. Delovanje družbe v marsičem temelji na uporabi kemičnih snovi. Kritičnost se lahko izpostavi predvsem na točki skladiščenja nevarnih kemičnih snovi, čeprav se zaradi razdrobljenosti kemične industrije porajajo dvomi o njeni dejanski kritičnosti.

Ugotovimo lahko, da je treba kakršno koli razdelitev kritične infrastrukture na podsektorje jemati z rahlim pridržkom. Nekateri podsektorji so namreč med seboj tako povezani, da lahko celo trdimo, da je njihovo ločevanje v določenem smislu umetno.[11] Ravno zato je pričujoča medsektorska analiza še toliko bolj relevantna, saj le na ta način lahko zajamemo celoto. Naj vendarle še posebej poudarimo specifični položaj sektorja informacijske in komunikacijske tehnologije (IKT-sektor). Sam proces izvajanja projek-

[11] *Jedrska proizvodnja električne energije, denimo, sodi v energetski in v jedrski sektor. Proizvodnja pitne vode lahko v nekem smislu sodi tudi v sektor hrana, saj pitno ustekleničeno vodo distribuirajo prehranski trgovinski sistemi. Kam sodi železniška infrastruktura na območju Luke Koper: pod železniško infrastrukturo ali pomorsko infrastrukturo? Slednje je problem, če vemo, da Luka Koper upravlja z železniškimi tiri na njenem območju, in ne Slovenske železnice.*

ta je pokazal, da je vprašljiva smiselnost zgolj sektorskega pristopa pri proučevanju IKT v RS in tudi širše. Zelo težko je obravnavati IKT kot ločeni sektor, saj gre za sestavni element vseh drugih proučevanih sektorjev (sektor finance, denimo, ne more delovati brez delovanja pripadajoče informacijske infrastrukture, podsektor železniški promet razpolaga s svojimi optičnimi informacijskimi povezavami, ki jih zakupijo zunanji IKT-partnerji). Posledično ni nekega povsem enotnega sistema regulacije IKT-sistemov v državi. S tem pa se potrjuje pravilnost nizozemskega pristopa, kjer IKT niso opredelili kot ločenega sektorja, ampak so mu namenili poseben poudarek v okviru analize vseh drugih sektorjev.[12] Iz tega izhaja nauk, ki bi ga morali upoštevati v RS in tudi na ravni EU. Nauk se nanaša na omejeno vrednost sektorskega pristopa in na nujnost medsektorskega pristopa do kritične infrastrukture na področju IKT. Past, ki čaka analitike, raziskovalce in oblikovalce politik, ki bodo sektorsko pristopili k IKT, je velika.

Obravnavani sektorji so različno razvejani in kompleksni. Število podsektorjev v sektorjih je različno. Nekateri sektorji temeljijo samo na enem podsektorju, medtem ko nekateri drugi na štirih ali celo več podsektorjih. Poleg tega pa so tudi podsektorji različno razvejani in kompleksni. Razvejanost podsektorjev in sektorjev po eni strani pripomore k večji razpršitvi tveganj, kakršna koli že obstajajo, poleg tega pa lahko povečuje akomodacijo in kompenzacijo kakršnih koli motenj. Slednje pomeni, da sama razvejanost omogoča, da se določene blokade dokaj lahko zaobidejo in kompenzirajo znotraj podsektorja ali pa celo med podsektorji, kar je še posebej značilno za cestni in letalski podsektor, IKT-komunikacije in strojno opremo. Obstaja torej tudi možnost kompenzacij med podsektorji v smislu, da se blokade v enem podsektorju kompenzirajo z večjim obremenjevanjem drugih podsektorjev v okviru istega sektorja (seveda ne brez posledic). V večini sektorjev pa ni mogoče nikakršno prilagajanje. Sistem nadzora kakovosti vode, denimo, ne more nadomestiti sistema za zagotavljanje vode, lahko samo do določene mere kompenzira slabšo kakovost zagotovljene vode. Laboratorijska dejavnost in proizvodnja ter distribucija zdravil ne morejo nadomestiti motenj v predbolnišnični ali bolnišnični oskrbi. Možnost akomodacije motenj v okviru sektorja energetika pa je dokaj majhna. Za sektor je namreč značilna nizka stopnja zamenljivosti energentov. V bistvu lahko govorimo o nezamenljivosti energentov, kar pomeni, da, denimo, z nafto in plinom ne moremo nadomestiti velikih izpadov elektrike in obratno.

Sektorji in podsektorji kritične infrastrukture v RS so načeloma sestavljeni iz omrežij. Nekatere stroke govorijo v tem smislu tudi o verigah. Še posebej vidna omrežja so v naslednjih sektorjih:

[12] *Za več informacij o nizozemskem pristopu, ki vključuje IKT v vse sektorje, glej Critical Infrastructure Protection in the Netherlands, 2003: 14; International CIIP Handbook 2006, 2006: 198; Report on Critical Infrastructure Protection, 2005: 56.*

- sektor promet: objekti (mostovi, predori, letališča, pristanišča, usmerjevalni in nadzorni informacijski sistemi) in povezave (ceste, železnice, zračni koridorji, plovne poti) med njimi v geografskem prostoru RS;
- sektor IKT: strojna oprema (računalniki), programska oprema in njihove povezave (fiksne telekomunikacije, mobilne telekomunikacije, internet ipd.);
- sektor energetika: proizvodni obrati (elektrarne), omrežje, ki omogoča prenos (daljnovodi, plinovodi), s pripadajočimi nadzornimi sistemi, transport (nafta, plin) in skladiščni objekti (plin, nafta);
- sektor finance: subjekti, ki omogočajo izvajanje plačilnega prometa oziroma plačilne transferje, vključno s pripadajočo IKT-opremo;
- sektor hrana: proizvajalci hrane (poljedelstvo, živinoreja), nadzorni organi (veterinarski, fitosanitarni, zdravstveni), živilsko-predelovalna industrija in distribucijske trgovinske verige;
- sektor voda: zajetja vode, sistemi za oskrbo (vodovodi), mehanizmi za nadzor kakovosti in mehanizmi za nadzor količine vode (npr. pregrade, zadrževalniki vode, nasipi ipd.).

Po drugi strani pa v nekaterih sektorjih ni bilo mogoče identificirati obstoja močnih mrež, kar pa seveda zahteva bolj natančno sektorsko proučitev. V sektorju kemične industrije, denimo, ni bilo mogoče identificirati relevantnega omrežja, saj je slovenska kemična industrija majhna in razdrobljena.

Grožnje kritični infrastrukturi v Sloveniji

Grožnje kritični infrastrukturi izhajajo iz potencialnega ogrožajočega vpliva na človeka, ki je odvisen od te infrastrukture. Ta vpliv je lahko neposreden ali posreden. Boin, Lagadec, Michel-Kerjan in Overdijk (2003: 100) so v tem smislu ugotavljali, da je problem predvsem v naraščajoči človekovi odvisnosti od povezanih mrež in naraščajoči povezanosti mrež. Oboje vpliva na povečevanje družbene ranljivosti. Odvisnost od tovrstnih mrež je dandanes večja, kot si večinoma predstavljamo.

Resnost potencialnih groženj kritični infrastrukturi narašča (Auerswald, Branscomb, La Porte in Michel-Kerjan, 2006: 9). To je očitno, saj se je o kritični infrastrukturi na konceptualni in operativni ravni začelo govoriti predvsem v luči terorističnega ogrožanja. Če pogledamo natančneje zadnje večje teroristične napade (New York, Madrid in London), potem lahko ugotovimo, da so vsi vključevali objekte kritične infrastrukture. Boin, Lagadec, Michel-Kerjan in Overdijk (2003: 101) ugotavljajo, da je problem v tem, da teroristi lahko poskušajo izkoristiti družbeno odvisnost od kritične infrastrukture oziroma mreže. V tem smislu teroristom sploh ni treba uničiti določene mreže, ampak jo lahko uporabijo kot orožje proti družbi ali državi. Michel-

Kerjan (2003: 133) dodaja, da so teroristi v preteklih napadih v bistvu izkoristili oziroma uporabili mreže kot orodje za razširjanje grožnje. Mreže so bile tako uporabljene kot orožje. Tako je npr. ameriški poštni sistem poskrbel za razpošiljanje pisem, ki so bila okužena z antraksom. Flynn (2004) je v zvezi s tem menil, da motivacija teroristov za napad na kritično infrastrukturo zajema neposredno škodo in tudi kolateralno škodo, še posebej v obliki zmanjšanja zaupanja javnosti v storitveno dejavnost, ki jo infrastruktura zagotavlja. Lewis (2006: 62) dodaja, da je kritična infrastruktura razmeroma enostavna tarča za teroriste – zaradi njenega obsega in relativno nizkega vložka za doseganje velikih učinkov.

Sintetični pregled zaznavanja ogrožanja infrastrukturnih podsektorjev v RS pokaže, da lahko razlikujemo med skupnimi grožnjami in podsektorsko specifičnimi grožnjami. Večina kategorij groženj je skupnih – torej zaznanih v vseh podsektorjih. Ključne skupne kategorije groženj so:

- naravne grožnje (nastale npr. zaradi poplav, potresov, plazov ter drugih naravnih nesreč, ki prizadenejo infrastrukturo),
- namerne grožnje, kot so npr. kriminal, terorizem, informacijski napadi, sabotaže, zlonamerno delovanje in drugi napadi, vojna, pri čemer večina akterjev zaznava zunanje namerne grožnje,
- nenamerne grožnje (npr. napake pri uporabi tehnologije, sistemske napake ter nesreče ipd.).

Zgornja zaznava ogrožanja je v skladu s pričakovanji, saj tudi mednarodno priznani znanstveniki omenjajo podobne kategorije (glej Le Grand, Springinsfeld in Riguidel, 2003: 5; Auerswald, Branscomb, La Porte in Michel-Kerjan, 2006: 5). Naj navedemo še nekatere »neklasične« in sektorsko specifične grožnje, ki so jih identificirali respondenti:

- grožnja pomanjkanja usposobljenih kadrov, izražena v sektorju IKT (notranji zaposleni kot grožnja) in v sektorju zdravje (nezadostna številčnost in usposobljenost kadrov za delo v kriznih razmerah);
- neizpeljani ali neprimerno izpeljani projekti na področju zagotavljanja plačilnega prometa v finančnem sektorju, kar bi lahko povzročilo velike motnje v njegovem delovanju;
- zgrešena politika oskrbe z vodo in neizvajanje zakonodaje v sektorju voda;
- prekomerna obremenitev infrastrukture, kar se nanaša na informacijsko infrastrukturo, prekomerno trgovanje in prenos električne energije; to lahko privede do kolapsa omrežij;
- soodvisnost od drugih sektorjev, kar se vidi na točki, ko sektor IKT izpostavi odvisnost od energetike, sektor hrana od vode (v smislu kontaminacije), sektor zdravje od energentov in transportnega sistema in sektor finance od fiksnih telekomunikacij – IKT;

– prekinitev dobave surovin: npr. elektroenergetski sektor izpostavlja grožnje prekinitve dobave energentov.

Primerjava zgornjih zaznav ogrožanja z dejanskimi izkušnjami RS pokaže, da imamo največ izkušenj z naravnimi nesrečami in določenim segmentom namernih groženj. V bistvu pa v Sloveniji ne pomnimo večjih motenj delovanja kritične infrastrukture v času njene neodvisnosti. Veliko podsektorjev navaja osamosvojitveno vojno kot večjo motnjo v delovanju. Po osamosvojitvi pa je v podsektorjih zaznati sorazmerno veliko majhnih – družbeno nekritičnih – motenj, ki so predvsem lokalnega značaja.

Relevantnost teroristične grožnje se na podlagi izvedbe delavnic izkaže kot dokaj teoretična v znatnem številu sektorjev. Vsi akterji se zavedajo potencialnosti teroristične nevarnosti, vendar nekateri ostajajo pri abstraktnem zavedanju, medtem ko so drugi podsektorji že »prisiljeni« izvajati dokaj specifične ukrepe. Ključna ločnica med abstraktnim razmišljanjem o terorizmu in konkretnim protiterorističnim delovanjem je predvsem mednarodna vpetost celotnega sektorja. Izrazito nacionalni sektorji, kot je npr. oskrba z vodo, se v preteklosti niso znatno ukvarjali s terorizmom.

Ugotovimo lahko tudi, da je slovenska kritična infrastruktura lahko po eni strani pod vplivom prenosa groženj iz kritične infrastrukture sosednjih držav, medtem ko po drugi strani lahko sama s svojim nedelovanjem povzroča podobne grožnje v teh državah. Sintetična analiza pokaže, da imamo v RS dve skupini sektorjev: inherentno mednarodne sektorje in tiste, ki so manj vpeti v mednarodne transferje, lahko pa povzročijo tudi čezmejne vplive. Za inherentno mednarodne podsektorje in sektorje je značilno, da brez vpetosti v mednarodne tokove sploh ne bi mogli delovati, kar načeloma pomeni, da imajo zelo verjetno tudi povratni vpliv na mednarodno skupnost. Vendar je povratni vpliv odvisen od dokaj različnih dejavnikov. Takšni sektorji so:

– sektor promet: čez Slovenijo gredo pomembni prometni koridorji v cestnem, železniškem, pomorskem in tudi zračnem prometu. Mednarodnost značaja je še posebej vidna v podsektorju zračnega prometa, kjer je pri kontroli letenja vidno, da sama mejna črta države ne igra enako pomembne vloge kot, denimo, pri cestnem ali železniškem prometu;
– sektor IKT: slovensko IKT-omrežje je sestavni del mednarodnega IKT-omrežja, vendar kompleksnost tega omrežja omogoča dokaj veliko število obhodnih poti (kompenzacija). Zanimiva je situacija, ko gre elektronska pošta iz enega dela države v drugi del prek omrežja sosednje države;
– sektor zdravje: mednarodni prenos nalezljivih bolezni zaradi motenega delovanja sektorja je zelo verjeten. Ravno tako obstaja verjetnost prenosa iz tujine v RS;
– jedrski sektor sodi med inherentno mednarodne zaradi velike vpetosti v mednarodne nadzorne mehanizme in izrazito čezmejnih posledic v pri-

meru nesreč. Vsak izredni dogodek je sporočen na EUROATOM in IAEA, poleg tega pa dokaj vznemiri tudi mednarodno javnost. NEK je poleg tega zelo blizu meje s sosednjo Hrvaško;
- energetski sektor: slovensko elektroenergetsko omrežje je sestavni del evropskega elektroenergetskega omrežja, kar pomeni, da se motnje iz Slovenije lahko prenašajo na sosednje države (južno Avstrijo, Italijo in države Jugovzhodne Evrope[13]). Nedelovanje plinskega omrežja bi se čutilo predvsem na Hrvaškem. Pri nafti bi bil vpliv najmanjši;
- sektor hrana je v določenem segmentu dokaj mednarodno pomemben, po drugi strani pa ne. RS je na zunanji meji EU, kar pomeni, da predstavlja obrambni pas EU pred vnosi patogenov iz mednarodne okolice. Moteno delovanje fitosanitarnih in veterinarskih služb bi lahko imelo tudi izrazito mednarodne posledice v okviru EU. Po drugi strani pa je izvoz hrane v tujino tako majhen, da njegov izpad ne bi imel posebnega učinka na sosednje države. Prej bi bilo obratno, saj je Slovenija neto uvoznik hrane;
- sektor voda je prav tako mednarodno pomemben le v določenih segmentih. Najbolj močan mednarodni vpliv bi imela porušitev nekaterih pregrad na Soči, Dravi in Savi, saj bi prišlo do poplavnega vala na Hrvaškem in v Italiji. Z vidika nadzora kakovosti vode bi lahko o čezmejnih posledicah govorili le v primeru, če bi prišlo do velikega onesnaženja nekaterih površinskih in podzemnih voda v Sloveniji, kar bi se preneslo v tujino (Hrvaška).

Najbolj kritični objekti ali vrste objektov

Posamezen kritični sektor ali podsektor seveda ni kritičen v celoti, ampak so kritični predvsem posamezni objekti ali procesi. Sinteza stanja v RS pokaže, da lahko razlikujemo med določenimi kritičnimi objekti, kritičnimi povezavami, kritičnimi križišči istovrstne ali raznovrstne infrastrukture in kritičnimi procesi, ki se odvijajo v okviru objektov ali njihovi okolici. V nadaljevanju lahko navedemo splošen pregled kategorij kritičnih objektov v sektorjih:
- promet: avtoceste, hitre ceste, glavne ceste I. in II. reda, regionalne ceste I., II., in III. reda, nekatera križišča (še posebej krožišče okrog Ljubljane, ker predstavlja križišče V. In X. Evropskega transportnega koridorja), predori, ki so daljši od 500 metrov, predor Ljubelj, določeni mostovi in viadukti, mednarodna letališča (Ljubljana, Maribor in Portorož – v njihovem okviru so najbolj kritične steze (pristajalna steza še posebej), ploščad, kjer se izvaja oskrba, nadzorna sredstva, terminal in oskrbovalna tehni-

[13] *Prenos elektroenergetskih motenj iz Slovenije v Jugovzhodno Evropo je možen, ker osnova nekdanjega jugoslovanskega elektroenergetskega omrežja še obstaja.*

ka), kontrolni centri za vodenje zračnega prometa, Luka Koper in plovne poti, enotirne proge, mostovi, predori, signalno-varnostne naprave, elektroenergetske naprave in telekomunikacijske naprave;
- IKT: komunikacijski centri, nadzorni centri, mednarodni centrali v Ljubljani in Mariboru, strežniki, bazne postaje, radijske povezave;
- finance: Uprava RS za javna plačila, Banka Slovenije, objekti večjih poslovnih bank, še posebej NLB, trezorji z večjimi količinami gotovine, računalniška oprema v objektih, s pomočjo katere se izvaja plačilni promet;
- zdravje: reševalne postaje, vsi zdravstveni domovi, telekomunikacijski, dispečerski in informacijski sistemi, splošne bolnišnice, ki imajo kirurške in rentgenske oddelke, UKC Ljubljana, UKC Maribor, laboratoriji, lekarne, veledrogisti, IVZ, Zavod RS za transfuzijsko medicino itd.;
- kemična industrija: skladišča, v katerih se shranjujejo večje količine kemičnih snovi, cevovodi, po katerih se znotraj objektov pretakajo kemične snovi, komercialna pretakališča kemičnih snovi, interni informacijsko-komunikacijski sistemi za uravnavanje pretoka kemičnih snovi;
- jedrski sektor: JEK Krško z bodočim skladiščem srednje in nizko radioaktivnih odpadkov, IJS-reaktor TRIGA Brinje, Centralno skladišče srednje in nizko radioaktivnih odpadkov (CSNRAO);
- energetika: elektrarne (vključno z JEK), elektroenergetsko omrežje, razdelilno transformatorske postaje (RTP), skladišča nafte in plinovodi;
- hrana: pomembnejši živilskopredelovalni objekti (npr. večje mlekarne, večji mesnopredelovalni objekti, večje pekarne), večja trgovska distribucijska središča, večje prašičje in perutninske farme;
- voda: objekti v vodovodnih sistemih, prek katerih se zagotavlja pitna voda največjemu številu prebivalcev (črpališča, vodohrani in cevovodi)[14], visokovodne pregrade – jezovi in zadrževalniki akumulacijskih jezer itd.

Pregled zgoraj izpostavljenih kategorij znova potrjuje tezo, da je IKT sestavni del praktično vseh kritičnih sektorjev. IKT je bil namreč večkrat izpostavljen kot kritičen v okviru sektorjev. Opozoriti je treba še na izjemno pomembno specifiko. V zračnem in pomorskem podsektorju kot sestavni del infrastrukture navajajo nekatere manj materialne kategorije kritičnih objektov, kot so zračne in plovne poti. Gre za manj oprijemljive kategorije kritične infrastrukture, brez katerih pa oba podsektorja seveda ne bi delovala. V tem smislu je treba dopolniti materialistično razumevanje kritične infrastrukture tudi s kategorijo zračnih in plovnih poti.

[14] *Problematično je celotno vodovodno omrežje, ker je mogoče skozi vsak vodovodni priključek ali hidrant vnesti strupene snovi.*

Indeks kritičnosti

Nedelovanje oziroma večje motenje posameznega podsektorja povzroča specifično neposredno in posredno družbeno škodo. V okviru projekta je bila na delavnicah ocenjena neposredna škoda v primeru nedelovanja oziroma velikega motenja za vsak podsektor. Ocenjevala se je neposredna škoda za prebivalstvo (število žrtev – mrtvih in težko ranjenih), gospodarstvo (gospodarska škoda v evrih), javnost (vpliv na državne storitve, javno zaupanje, družbeni red, končne uporabnike in geopolitični vpliv) ter okolje (površina prizadetega ozemlja ali delež prebivalstva, ki mora zapustiti domove). Neposredna škoda se je ocenjevala na lestvici od 0 do 4 z naslednjimi pomeni:

- 0: nikakršna ali zelo majhna škoda,
- 1: majhna škoda,
- 2: srednja škoda,
- 3: velika škoda,
- 4: zelo velika škoda.

Neposredna škoda se je ocenila za primer nedelovanja celotnega podsektorja, čeprav se vsi zavedamo, da do takšne situacije skorajda ne more priti. Onesposobitev oziroma nedelovanje proučevanih podsektorjev se nanaša na hipotetično situacijo, po kateri le-ti ne morejo več opravljati svojih temeljnih funkcij. Pri tem se ni razpravljalo o vzrokih, ki bi lahko pripeljali do takšne situacije, ampak samo o posledicah takšne situacije (o škodi oziroma vplivu). Ocena škode prav tako ni temeljila na kakšnem specifičnem scenariju, kar je sicer običajno, ko razmišljamo o posledicah in ukrepanju v primeru kriznih razmer. Pri odgovarjanju na konkretna vprašanja je torej šlo za splošno oceno ob kakršnem koli zlomu, onesposobitvi ali resnem motenju delovanja infrastrukture ne glede na vzrok oziroma razlog. Razlog za takšen pristop je v tem, da je to edini način ocenitve absolutnega pomena posameznega podsektorja za družbo. Uporaba scenarijev bi bila seveda bolj realna, vendar z njimi ne bi mogli oceniti absolutnega pomena podsektorja za družbo (njegovo kritičnost). Pri tem je bila ključna usmerjevalna logika, ki pravi: večji je absolutni pomen podsektorja za družbo, večja je njegova kritičnost.

Pri ocenjevanju potencialne neposredne škode je bil izločen tudi kakršen koli vpliv zaščitnih ukrepov. Preventivni zaščitni ukrepi mnogokrat preprečujejo razvoj krize do svojih ekstremov. Razmišljanje o maksimalnem dometu onesposobitve podsektorja je onemogočeno, če imamo stalno v mislih številne zaščitne ukrepe. Takšno razmišljanje je seveda realno, vendar pa bi znova preprečilo oceno absolutnega pomena posameznega podsektorja za družbo.

Naslednja tabela prikazuje ocene škode po posameznih podsektorjih in škodnih kategorijah. Iz te osnove je bil izpeljan absolutni in relativni (normalizirani) indeks kritičnosti za vsak podsektor. Pri tem je treba poudariti, da gre za kritičnost na podlagi samoocene strokovnjakov iz podsektorjev.

Indeks kritičnosti (IK) je vsota ocen škode v kategoriji prebivalstvo, gospodarstvo, javnost in okolje. Pri večdimenzionalnih kategorijah (javnost in okolje) se upošteva le maksimalna ocena škode, ki je bila podana v tem okviru. Maksimalna vrednost indeksa je torej 16, minimalna pa 0. Zaradi primerljivosti med podsektorji je bil izračunan tudi normalizirani oziroma relativni indeks (NIK), ki je odstotek vrednosti indeksa glede na maksimalno možno škodo. V oklepaju ob NIK je zapisan tudi rang kritičnosti (vrstni red med sektorji po kritičnosti). V zadnji vrstici je navedena vsota po škodnih kategorijah.

Tabela: Ocene škode po posameznih podsektorjih in škodnih kategorijah ter absolutni (IK) in relativni oz. normalizirani indeks kritičnosti (NIK).

SEKTOR	**PODSEKTOR**	**ŠKODA ZA:**		**Javnost**					**Okolje**			
		Prebivalstvo	Gospodarstvo	Državne storitve	Javno zaupanje	Družbeni red	Končni uporabn.	Geopolitični vpliv	Ozemlje	Prebivalstvo	**IK**	**NIK**
Energetika	Nafta	0	3	0	4	4	3	2	0	0	7	0,43 (8)
	Plin	0	3	0	4	2	0	4	0	0	7	0,43 (8)
	El. energija	2	4	4	4	4	4	3	0	0	10	0,62 (5)
Jedrska industrija	Jedrske snovi	1	1	0	4	3	0	2	0	0	6	0,37 (9)
IKT	IKT informatika	0	4	4	3	0	3	2	0	0	8	0,5 (7)
	IKT komunikacije in strojna oprema	0	3	2	4	1	3	3	0	0	7	0,43 (8)
Voda	Pit. voda	2	4	2	4	1	4	3	0	0	10	0,62 (5)
	Kakovost vode	1	3	1	3	1	2	2	0	0	7	0,43 (8)
	Nadzor količine	2	4	2	4	2	0	3	2	0	12	0,75 (3)
Hrana	Hrana	4	4	4	4	4	4	3	0	3	15	0,93 (1)
Zdravje	Predbolnišnična nega	4	3	0	4	1	1	0	0	0	11	0,68 (4)
	Bolnišnična nega	4	4	1	2	4	0	3	0	0	12	0,75 (3)
	Zdravila in laboratoriji	4	4	4	4	4	2	4	0	1	13	0,81 (2)
Finančni	Finančna infrastruktura	0	4	1	3	1	0	0	0	0	7	0,43 (8)
Promet	Cestni	2	4	0	3	0	2	2	0	0	9	0,56 (6)
	Železniški	0	3	1	3	0	0	1	0	0	6	0,37 (9)
	Zračni	0	1	1	3	0	0	2	0	0	4	0,25 (11)
	Pomorski	0	2	0	3	0	0	1	0	0	5	0,31 (10)
Kemična	Kemična industrija industrija	2	2	0	4	1	0	2	0	0	8	0,5 (7)
Vsota		28 (5)	60 (2)	27 (6)	67 (1)	33 (4)	28 (5)	42 (3)	2 (8)	4 (7)		

Vsota po škodnih kategorijah pokaže, da se ob nedelovanju kritične infrastrukture pojavi daleč največja škoda v kategorijah javno zaupanje in gospodarstvo. To pomeni, da najhitreje pride do negativnega medijskega pokritja – kritike in gospodarske škode. Po občutljivosti sledijo kategorije:

geopolitični vpliv, vpliv na družbeni red in končne uporabnike ter vpliv na prebivalstvo (žrtve) in državne storitve. Najmanjši vpliv ob nedelovanju kritične infrastrukture se izkaže v primeru okolja (v nobenem primeru ni škoda zajela največje kategorije). Na tej podlagi lahko ugotovimo, da bi nedelovanje kritične infrastrukture v osnovi pomenilo večjo korist kot škodo za okolje. Tudi humanocentrični test škode za okolje nas vodi k potrjevanju te teze.

Zgornji rezultati kažejo tudi, da sektorji niso koherentni v smislu enake kritičnosti podsektorjev. Določeni podsektorji so dosegli bistveno večji rang kot drugi podsektorji iz istega sektorja. To dejstvo bi morale upoštevati kakršne koli nadaljnje sektorske analize.

Ob pogledu na zgornjo tabelo se zastavlja vprašanje, kje potegniti črto, ki bi ločevala dejansko kritične in nekritičnih podsektorjev. Rezultati tega ne omogočajo. Z veliko gotovostjo lahko trdimo samo to, da so vsi od proučevanih sektorjev družbeno kritični, tabela pa prikazuje njihovo različno stopnjo kritičnosti glede na samopercepcijo upravljavcev. Zaradi medsektorske (oziroma medpodsektorske) povezanosti bi ekstremna motnja v enem od podsektorjev kmalu vplivala na delovanje drugih podsektorjev.

Sklepne misli

V sintetičnem smislu lahko ugotovimo, da je relevantnost nacionalne kritične infrastrukture in njene zaščite neizpodbitna, kar se še posebej nanaša na nacionalne in mednarodne varnostne vidike. Ključni problem se pojavi že pri opredelitvi nacionalne ali evropske kritične infrastrukture, ki nastane zaradi njene večrazsežnosti in razširjenosti v celotni družbi. V nobeni državi ni mogoče zaščititi celotnih sektorjev, ki so bili ali bodo označeni kot kritični, ampak je treba zaščitne in varnostne ukrepe osredotočiti zgolj na najbolj kritične objekte, točke ali procese. Določitev teh procesov je zapletena naloga, s katero se soočajo evropske države in tudi EU. Še posebej so relevantni kriteriji za določitev kritične infrastrukture, ki smo jih v Sloveniji na znanstvenem področju že opredelili.

Članek je pokazal, da ima Slovenija številne infrastrukture, ki bi jih lahko označili kot družbeno in varnostno kritične. Ti sektorji so večinoma mrežno strukturirani in so različno razvejani ter kompleksni. IKT je sestavni del skoraj vseh sektorjev, zato bi v prihodnje kakršen koli sektorski pristop na tem področju prinesel dokaj pičla spoznanja. Sektorji se soočajo s številnimi skupnimi in sektorsko specifičnimi grožnjami, med katerimi izstopajo izkušnje z naravnimi nesrečami. Večina kritičnih sektorjev je inherentno mednarodnih, kar pomeni, da lahko hitro pride do prenosa motenj delovanja v Slovenijo ali iz nje. V vsakem sektorju obstajajo številni bolj kritični objekti ali kategorije objektov, na katere bi se v fazi zaščite morali bolj osredotočiti. Še

posebej problematične so manj materialne kategorije objektov, kot so plovne in zračne poti. Indeks kritičnosti je dodatno pokazal, da vsi podsektorji vendarle niso enako kritični, kar bi moralo vplivati na prioritizacio nacionalnih zaščitnih ukrepov.

Slovenija se v tem trenutku sooča s številnimi policy dilemami na področju kritične infrastrukture in njene zaščite. Naj navedemo nekaj ključnih dilem in nakažemo pot možnega reševanja.

1) V državi ne obstaja niti en zakonski ali podzakonski akt ter strateški dokument, ki bi uporabljal termin kritična infrastruktura, kar pa ne pomeni, da se država s tem področjem ne ukvarja. To pomeni, da Slovenija še nima razvite politike na tem področju, kar jo postavlja v zamudo v primerjavi s številnimi drugimi evropskimi državami. Na nacionalni ravni bi se zato morala oblikovati politika zaščite kritične infrastrukture, ki bi obsegala opredelitev konteksta, ciljev, načel, smernic in mehanizmov. To bi bilo mogoče izvesti na več načinov. Mogoče je, denimo, nadgraditi Strategijo nacionalne varnosti s konceptom kritične infrastrukture in njene zaščite. Možno bi bilo sprejeti posebno strategijo zaščite kritične infrastrukture v RS, ki bi opredeljevala zgoraj omenjene elemente. Sektorji in podsektorji bi morali pri svojem delovanju in preoblikovanju upoštevati enotne nacionalne smernice. Poleg tega pa bi država morala to področje umestiti v okvir kriznega upravljanja oziroma zagotavljanja nacionalne varnosti. Področje bi bilo treba predstaviti kot kompleksno večinstitucionalno področje, kjer je potrebna sinergija.

2) Zazdaj Slovenija nima opredeljene kritične infrastrukture, zato bi bilo treba vse v članku identificirane podsektorje opredeliti kot kritične ali vitalne. Prednost pri urejanju naj bi imeli tisti, ki so bolj kritični. Poleg tega bi bilo treba dodatno razmisliti o razdelitvi na podsektorje. Obstoječi razdelitvi bi bilo mogoče dodati še kake podsektorje (npr. transport nevarnih snovi, kulturno dediščino, vojaško infrastrukturo, morda pravosodni sistem ipd.) ali pa nekatere združiti (npr. v primeru zagotavljanja pitne vode in nadzora kakovosti pitne vode, v primeru IKT). Morebitne nove podsektorje bi bilo ravno tako treba pregledati najprej s »quick scan« analizo.

3) Oblikovati bi bilo treba nacionalni organ, ki se na medresorski ravni ukvarja z preglednimi analizami, izmenjavo mnenj in pogledov, iniciranjem projektov, mehanizmov ipd. To bi lahko opravljala obstoječa Medresorska koordinacijska skupina za zaščito kritične infrastrukture, ki bi lahko za specifična področja ustanavljala medresorske podskupine. Še posebej pomembno je, da ima določeno telo v državi pregled nad stanjem zaščite kritične infrastrukture (tveganji, procesi, akterji, zakonodajo, vajami itd.). Večja preglednost hkrati pomeni večjo sposobnost za identificiranje problemov in posledično njihovo reševanje. Pomembno je tudi oblikovati kontaktni mehanizem med javnimi in zasebnimi akterji za reševanje specifičnih dilem (PPP). Takšnih kompetenc pa obstoječa skupina trenutno nima.

4) Slovenija nima natančno proučenih podsektorjev in sektorjev po ključnih parametrih zaščite kritične infrastrukture. Raziskovalni projekt FDV, iz katerega izhaja ta članek, predstavlja le hitri pregled (»quick scan«). Zato bi bilo treba zasnovati nadaljnje bolj poglobljene sektorske oziroma podsektorske analize. Bolj primerne bi bile celo podsektorske analize, saj se je izkazalo, da obstajajo dokaj velike razlike med nekaterimi podsektorji v okviru nekaterih sektorjev. Analize bi morale biti izvedene v skladu z upoštevanjem temeljnih načel zaščite kritične infrastrukture in logike medsektorske povezanosti. Priporočljivo bi bilo tudi uporabiti enotne kriterije za izdelovanje podsektorskih analiz kljub dokaj različni namembnosti in ustrojenosti (kompleksnosti). S tem bi se izognili subjektivnemu poudarjanju ali zmanjševanju lastne kritičnosti, kar se je dogajalo tudi v našem projektu. Po zaključenih sektorskih analizah bi bilo treba znova opraviti medsektorsko analizo, ki bi bila prilagojena dobljenim rezultatom iz sektorskih analiz. Izjemno pomembno področje nadaljnjih analiz je nedvomno medsektorska povezanost.

LITERATURA

Auerswald, Philip, Branscomb, Lewis, La Porte, Todd in Michel-Kerjan, Erwann (2005): The Challenge of Protecting Critical Infrastructure. Issues in Science and Technology (Fall): 77–87.

Auerswald, Philip, Branscomb, Lewis, La Porte, Todd in Michel-Kerjan, Erwann (2006): When Private Efficiency Meets Public Vulnerability: The Critical Infrastructure Challenge. Paper presented at the workshop Protecting Critical Infrastructures: Vulnerable Systems, Modern Crises, and Institutional Design, Conference on Future Challenges for Crisis Management in Europe, 4–5 May, Stockholm.

Benoit, Robert (2004): A Method for the Study of Cascading Effects within the Lifeline Networks. International Journal of Critical Infrastructure (let. 1, št. 1), 32–46.

Boin, Arjen, Lagadec, Patrick, Michel-Kerjan, Erwann in Overdijk, Werner (2003): Critical Infrastructures under Threat: Learning from the Antrax Scare. Journal of Contingencies and Crisis Management (let. 11, št. 3): 99–104.

Council Directive on the Identification and Designation of European Critical infrastructures and the Assessment of the Need to Improve their Protection (2008): 8. 12., Official journal of the EU, 23. 12., Brussels.

Critical Infrastructure Protection in the Netherlands (2003): Ministry of the Interior and Kingdom Relations. First Report. Hague.

Dunn, Myriam (2005): The Socio-political Dimensions of Critical Information Infrastructure Protection. International Journal of Critical Infrastructures (let. 1, št. 2/3): 258–268.

Ellison, Robert et al. (1999): Survivability: Protecting Your Critical Systems. Research Paper, CERT Coordination Center, Carnegie Mellon University, Pittsburgh.

Flynn, Stephen (2004): The Neglected Front. Foreign Affairs (let. 83, št. 5).
Green Paper on a European Programme for Critical Infrastructure Protection (2005): EC, 17. 11., Brussels.
Hellstrom, Tomas (2006): Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework. Research paper, Safety Science.
International CIIP Handbook 2006 (2006): An Inventory of 20 National and 6 International Critical Infromation Infrastructure Protection Policies, Vol. 1, Center for Security Studies, ETH Zürich.
Johnson, Chris (2006): Understanding the Interaction between Public Policy, Managerial Decision-Making and the Engineering of Critical Infrastructures. Research paper, Reliability Engineering and System Safety.
Knight, John in Sullivan, Kevin (2000): On the Definition of Survivability, Research Paper, Department of Computer Science, University of Virginia.
Koubatis, Andrew in Schonberger, Jorge Yerena (2005): Risk Management of Complex Critical Systems. International Journal of Critical Infrastructures (let. 1, št. 2/3): 195–215.
Le Grand, Gwendal, Springinsfeld, Franck in Riguidel, Michel (2003): Policy Based Management for Critical Infrastructure Protection. Research report, ACIP Project, funded by the European Commission.
Lewis, Ted (2006): Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. New Jersey: Wiley Interscience.
Michel-Kerjan, Erwann (2003): New Challenges in Critical Infrastructures: A US Perspective. Journal of Contingencies and Crisis Management (let. 11, št. 3): 132–141.
Moteff, John in Parfomak, Paul (2004): Critical Infrastructure and Key Assets: Definition and Identification. CRS Report for Congress, Congressional Research Service, D.C.: The Library of Congress.
Nozick, Linda in Turnquist, Mark (2005): Assessing the Performance if Interdependent Infrastructures and Optimising Investments. International Journal of Critical Infrastructures (let. 1, št. 2/3), 133–140.
Peerenboom, James (2001): Infrastructure Interdependencies: Overwies of Concepts and Terminology. Research paper, Infrastructure Assurance Center, Argonne.
Politi, Alessandro (1997): European Security: The New Transnational Risks. Chaillot Papers, št. 29, Paris: Institute for Security Studies WEU.
Pommerening, Christine (2004): A Comparison of Critical Information Infrastructure Protection in the US and Germany: An Institutional Perspective, Conference Paper – American Political Science Association, Annual Meeting – Chicago.
Predlog Direktive o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja (2008), Svet EU, Bruselj, 22. 5.
Predlog direktive Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja (2006), Svet EU, Bruselj, 18. 12.
Prins, Gwyn (1998): The Four-Stroke Cycle in Security Studies. International Affairs, 74(4).

Radvanovsky, Robert (2006): Critical Infrastructure: Homeland Security and Emergency Preparedness. New York: Taylor in Francis.
Reinermann, Dirk in Weber, Joachim (2003): Analysis of Critical Infrastructures: the ACIS Methodology. Federal Office for Information Security, Bonn, Germany.
Report on Critical Infrastructure Protection (2005), The Ministry of Interior and Kingdom Relations, The Netherlands, The Hague.
Schulman, Paul in Roe, Emery (2006): Future Challenges for Crisis Management in Europe. Paper presented at the workshop Protecting Critical Infrastructures: Vulnerable Systems, Modern Crises, and Institutional Design, Conference on Future Challenges for Crisis Management in Europe, 4–5 May, Stockholm.
Terriff, Terry, Croft, Stuart, James, Lucy in Morgan, Patrick (1999): Security Studies Today. Cambridge: Polity Press.