UPRAVLJANJE S TVEGANJI V KRITIČNI INFRASTRUKTURI

MARINA ĐORĐESKI[1], MIRJANA RADOVANOVIĆ[2], ALEKSANDAR ANDREJEVIĆ[2] & IZTOK PODBREGAR[1]

[1]Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj, Slovenija, e-pošta: marina.djordjeski1@um.si, iztok.podbregar@um.si
[2]Educons University, Faculty of Security Studies, Srbija e-pošta: mirjana.radovanovic@educons.edu.rs, aauc@educons.edu.rs

Povzetek Kritična infrastruktura obsega vse tiste zmogljivosti, ki so ključnega pomena za državo in bi prekinitev delovanja pomembno vplivala ter imela resne posledice za nacionalno varnost, gospodarstvo, zdravje, varnost, zaščito in blaginjo ljudi. Kritično infrastrukturo ljudje jemljejo za samoumevno, vendar jo pestijo velika tveganja. Tveganje je vse kar lahko prepreči doseganje določenih ciljev in ustvari izid, ki ni bil predviden. Samo analiziranje kaj se lahko zgodi in ukrepanje imenujemo upravljanje s tveganji. Ugotavljamo, da upravljanje s tveganji postaja vedno bolj celovita in zahtevnejša aktivnost za zaščito kritične infrastrukture pred izrednimi dogodki zaradi namerne ali nenamerne povzročitve. Z neustreznim upravljanjem lahko negativno vplivamo na uporabnike, lastnike in upravljalce kritične infrastrukture. V raziskavi je bil uporabljen kritični pregled sekundarnih virov ter metoda sinteze, s pomočjo katerih smo opisali zakaj je potrebno uspešno upravljati s tveganji.

Ključne besede: kritična infrastruktura, tveganje, upravljanje s tveganji, negotovost.

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/978-961-286-442-2.13
ISBN 978-961-286-442-2

Risk Management in Critical Infrastructure

Marina Đorđeski[1], Mirjana Radovanović[2], Aleksandar Andrejević[2] & Iztok Podbregar[1]

[1]Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj, Slovenija, e-pošta: marina.djordjeski1@um.si, iztok.podbregar@um.si
[2]Educons University, Faculty of Security Studies, Srbija e-pošta: mirjana.radovanovic@educons.edu.rs, aauc@educons.edu.rs

Abstract Critical infrastructure encompasses those capabilities that are crucial to the state and disruption would have a significant impact and serious consequences for national security, economy, health, safety, security, and human well-being. People take critical infrastructure for granted, but it is fraught with great risks. Risk is anything that can prevent the achievement of certain goals and create an outcome that was not foreseen. Just analysing what can happen and acting is called risk management. We find that risk management is becoming an increasingly comprehensive and demanding activity to protect critical infrastructure from emergencies due to intentional or unintentional causing. Improper management can have a negative impact on users, owners, and operators of critical infrastructure. The research used a critical review of secondary sources and a method of synthesis, with the help of which we described why it is necessary to successfully manage risks.

Keywords: critical infrastructure, risk, risk management, uncertainty

DOI https://doi.org/10.18690/978-961-286-422-2.13
ISBN 978-961-286-422-2
University of Maribor Press

1 Uvod

Tveganje je povezano s skoraj vsako dejavnostjo, ki si jo lahko predstavljamo. Poleg tega tveganje lahko pomeni možen pojav neželenega dogodka. Tveganja ne smemo zamenjevati z nevarnostmi, ki so vzroki za tveganje, kot so požar, poplava in potres. Skoraj vse je lahko nevarno – na primer napolnjena pištola ali skladišče, ki se uporablja za shranjevanje vnetljivih izdelkov. Končni rezultat tveganja je izguba ali zmanjšanje vrednosti (Broder & Tucker, 2012).

Tveganja povezujemo tudi s kritično infrastrukturo, ki je nujna za zagotavljanje nemotenega delovanja širše družbene skupnosti, torej države, civilne družbe, gospodarstva in nenazadnje tudi prebivalstva. Poleg kibernetskih, terorističnih, kriminalnih in drugih tveganj za delovanje kritične infrastrukture predstavljajo pomembno tveganje tudi neravne nesreče, kot sta žled in poplava, ki sta povzročala težave tudi v Sloveniji. Poudariti je potrebno, da se kritična infrastruktura deli v posamezne sektorje in podsektorje. Si lahko predstavljate življenje brez električne energije in delovanja informacijske tehnologije? Iz primera nesreče z žledom, kjer je bil večji del države brez električne energije in tudi brez delujoče informacijske tehnologije, lahko hitro ugotovimo, da je takšno tveganje zelo resno (Čeleta et al., 2019).

Brezhibno delovanje kritičnih infrastruktur gradi prave odnose med državljani in vlado. Sodobne družbe so zelo občutljive na kakršnekoli motnje v kritični infrastrukturi. Motnje ali škoda ovirajo gospodarsko rast, družbeno blaginjo in trajnostni razvoj naše civilizacije. Iz tega razloga je zelo pomembno ublažiti kakršen koli negativni vpliv na kritične infrastrukture. Upravljanje tveganj, ki ima ključno vlogo pri zaščiti intelektualne lastnine, še vedno ostaja izziv zaradi številnih nerešenih težav (Bialas, 2016).

V letu 2020 je KI pestilo še eno tveganje, ki se je pojavilo nenapovedano in povzročilo pravi kolaps na svetovni ravni. Govorimo o pandemiji korona virusa, ki je povzročila odziv na svetovni ravni (Remuzzi & Remuzzi, 2020). V takšnih situacijah se KI soočajo s posebnimi izzivi zaradi tveganja, da ključno osebje ni na voljo zaradi virusa ali karantene in drugih dolgoročnih vplivov, ki bi lahko vplivali na zagotavljanje stalne razpoložljivosti.

2 Kritična infrastruktura

Krize, hitre spremembe, nepredvidljive situacije in grižnje varnosti so postale stalnica v sodobnem varnostnem okolju, za katero je značilno vedno več ogrožajočih pojavov, njihova vedno večja medsebojna povezanost in transnacionalnost. Terorizem, kriminalitete, informacijske, okoljske, zdravstvene grožnje itd. so v raziskovalnem smislu pomembne zaradi njihovega morebitnega smrtonosnega vpliva na ljudi in na temeljno družbeno infrastrukturo. Prav ta infrastruktura ljudem omogoča opravljanje temeljnih družbenih funkcij, ki pa je vir mnogih tveganj (Prezelj, 2010).

Samo pojmovanje kritične infrastrukture (v nadaljevanju KI) zajema vse objekte in sisteme, katerih nedelovanje oz. omejeno delovanje povzroča družbeno-krizne situacije ali celo ogroža varnost ljudi (Prezelj, 2010).

Luskova in Dvorak (2019) pravita, da je KI del nacionalne infrastrukture (izbrani informacijski sistemi, storitve, organizacije in njihovi pomembni predmeti in zmogljivosti) katerih uničenje ali motenje bo zaradi izpostavljenosti določenemu dejavniku tveganja povzročilo nevarnosti ali motnjo v delovanju družbe ali ogrožanje življenja in zdravja državljanov.

Za pravilno razumevanje KI je potrebno določiti seznam sektorjev KI (Luskova & Dvorak, 2019):

- energija (elektrika, plin, naftna industrija, rudarstvo),
- informacijske in komunikacijske tehnologije (satelitske komunikacije, omrežja, podatkovni centri, viri tajnih informacij, nadzorni in informacijski sistemi infrastruktur),
- prevoz (cestni, železniški, zračni, vodni).

Prezelj (2009) poleg zgoraj naštetih sektorjev dodaja še:

- sisteme za preskrbo z vodo (zagotavljanje pitne vode, nadzor kakovosti vode in nadzor količine vode),

- sisteme za preskrbo s hrano (pridelava hrana, predelava, distribucija in prodaja),
- finančne sisteme (trgovanje, plačila, poravnave),
- zdravstvene sisteme,
- kemično industrijo,
- jedrsko industrijo.

Koncept kritične infrastrukture se razvija. V 80. letih prejšnjega stoletja se je zaradi staranja javnih površin nadzor nad njimi preusmeril v Nacionalni svet za zboljšanje javnih del. Osredotočili so se na infrastrukturo v javnem sektorju, kot so avtoceste, ceste, mostovi, letališča, javni tranzit, objekti za oskrbo z vodo, čistilne naprave, storitve na področju nevarnih odpadkov (O'Rourke, 2007). Sam koncept KI se je dokončno začel razvijati sredi devetdesetih let 20. stoletja v Združenih državah Amerike, kjer so opredelili nabor sredstev in storitev, ki skupaj tvorijo elemente, ki so kritični za ohranjanje stabilnosti države in blaginjo njenih državljanov. Vrste industrij, ki so bile opredeljene kot kritične, so se z leti spreminjale, vendar obstaja splošno soglasje da mednje sodijo: elektrika, voda, skladiščenje in transport nafte in plina, telekomunikacije, prometni sistemi, finančni sektor, reševalne službe in vlada (Murić et al., 2013).

Ocenjevanje, kaj je KI, se ne more kar določiti s tem, katere infrastrukture so pomembne za družbo. Analiza se začne z opredelitvijo sistemske maksimalne referenčne točke za skupno kritičnost specifičnih tehnoloških in družbenih sistemov. Oceni se, kje je tehnološki in družbeni sistem najranljivejši in kako je ranljivost povezana. V kolikor so sektorji KI mreže, lahko uporabimo mrežne analize, s pomočjo katerih določimo kritične točke in njihove povezave. Mreža je skupek točk, ki so med seboj povezane. Mrežna analiza vsak sektor najprej modelira kot mrežo, nato kritične točke opredeli in analizira, vključno s povezavami. Točke predstavljajo točke nadzora, torej gre za točko v sektorju, kjer napad, nesreča povzroči največ škode. Določitev takih točk temelji na številu povezav med njimi, kritičnost pa je največja tam, kjer je največ povezav. Ko imamo kritične točke določene in oblikovano bazo teh točk, je potrebno začeti z njihovo analizo, ki vključuje mrežno analizo, s pomočjo katere določimo kritične povezave. Pretrganje teh povezav pomeni razpad omrežja (Prezelj, 2010).

3 Tveganja kritične infrastrukture

Kritično infrastrukturo ljudje jemljejo za samoumevno. To je ironija KI. Vedno je tu za nas in nas nikoli ne izneveri. Ki je dana; gre za predpostavko. To je izkušnja večine ljudi zahodnega dela sveta. Pitna voda, hrana, močni mostovi, delujoči telefoni, reševalna vozila, policija, možnost nakupa in prodaje blaga ter storitev, napajanje na črpalki, otroške nočne luči in postelje za dvigovanje dedka. Ta izkušnja in samoumevnost je bila ogrožena že konec dvajsetega stoletja z raznimi dogodki, kot je bila leta 1998 ledena nevihta v Kanadi, ki je zahtevala odziv celotnega kontinenta. Tako je zahodni svet videl, kaj se lahko zgodi in kakšne posledice pri tem nosi KI. Dogodki, kot so ledne nevihte, orkani, pandemije, zapiranje meja, strahovi povezavi s hrano, banke, ki prenehajo delovati zaradi okvar sistemov, so in lahko prizadenejo milijone in milijone ljudi širom sveta, posledično pa trpijo prav vse KI (Macaulay, 2008).

Tveganje je opredeljeno kot negotovost rezultatov, ne glede na to, ali gre za pozitivne priložnosti ali negativno grožnjo dejanj in dogodkov. Tveganje je potrebno oceniti glede na verjetnost, da se bo zgodilo in vpliv, ki nastane, če se dejansko zgodi (HM Treasury & Government Finance Function, 2004). Brashear (2019) navaja, da je tveganje funkcija posledic neželenega incidenta in verjetnost njegovega nastanka.

Obvladovanje tveganj vključuje prepoznavanje in oceno tveganj ter njihovo odzivanje nanje. Sredstva, ki so na voljo za obvladovanje tveganj, so omejena, zato je cilj doseči optimalen odziv na tveganje, ki je prednostno postavljen v skladu z oceno tveganj. Vsaka organizacija mora sprejeti ukrepe za obvladovanje tveganj. Količina tveganja, za katero se oceni, da je sprejemljiva in opravičljiva, se imenuje »nagnjenost k tveganju« (HM Treasury & Government Finance Function, 2004).

Kritičnost določene vrste infrastrukture ali sistema so običajno določi na podlagi možnih vplivov na skupnost v primeru okvare. Samo en ekstremni dogodek v določenem sistemu kritične infrastrukture lahko na koncu prinese resne posledice, kot so izguba življenj, gospodarske izgube in celo škoda za nacionalno varnost (Ongkowijoyo & Doloi, 2017). Pretekli napadi, kot so teroristični napad februarja 2006 na Abqaiq v Savski Arabiji, iransko-iraška vojna od septembra 1980 do avgusta 1988, iraška invazija na Kuvajt avgusta 1990, predstavljajo primere resničnih in potencialnih tveganj za infrastrukturo, prav tako pa tudi naravni dogodki, kot so

orkani in potresi (Coote & Hopkins, 2017). Glede na velik vpliv uporabnosti storitev KI, je nujno potrebno izboljšati odločanje v zvezi z načrtovanjem in blaženjem zaščite KI z globljim razumevanjem narave tveganja (Ongkowijoyo & Doloi, 2017).

Coote in Hopkins (2017) pravita, da je infrastrukturno tveganje treba obravnavati kot svetovni in multidisciplinarni izziv, ki ga je bolje razumeti in ga obravnavati kot vprašanje odpornosti in ne kot vprašanje varnosti. Analiza tveganj KI bi se morala začeti z oceno ranljivosti, groženj in možnosti zaščite s strani dobro poznanih strokovnjakov.

Tradicionalna orodja za ocenjevanje in obvladovanje tveganja so v zadnjih letih postala zelo izpolnjena kot posledica okoljskih, zdravstvenih in varnostnih predpisov. Kljub temu takšna orodja ostajajo večinoma neustrezna pri soočanju z dogodki z visokim učinkom in z majhno verjetnostjo. Gospodarske in socialne dejavnosti postajajo vse bolj soodvisne, zato bodo ukrepi ene organizacije močno vplivali na druge organizacije. Zato so spodbude za preprečevanje, odzivanje in omilitev tveganj ene same organizacije premalo. Brez globalnega pristopa k problemu bo težko določiti izvor motenj in določiti tveganja takšnih motenj (Auerswald et al., 2005).

Auerswald, Branscomb, La Porte in Michel-Kerjan (2005) opozarjajo, da strategije za zaščito KI niso izvedljive, če niso politično in gospodarsko trajnostne. Trajnost je mogoče izboljšati s premišljeno politiko iskanja možnosti, ki prinašajo koristi, ki obljubljajo javne in zasebne koristi poleg zmanjšanja ranljivosti.

4 Upravljanje s tveganji v kritični infrastrukturi

Da lahko govorimo o tveganju morate biti izpolnjena dva dejavnika – negotovost in izpostavljenost. V kolikor eden izmed njiju ni prisoten, potem ne moremo govoriti o tveganju (lahko smo negotovi glede nekega dogodka, toda, če nismo izpostavljeni, potemtakem tveganj ni; ali obratno; če smo izpostavljeni in z gotovostjo vemo kaj se bo zgodilo, potem za nas tveganje ne obstaja). Tveganje je vse kar lahko prepreči doseganje določenih ciljev in ustvari izidi, ki ni bil predviden (Čeleta et al., 2019).

Koncept tveganja se ukvarja z naslednjimi vprašanji (Čeleta et al., 2019):

- Kaj se lahko zgodi?
- Kakšna je verjetnost, da se bo to zgodilo?
- Kakšne so posledice, če se bo to zgodilo?
- Kako se izogniti posledicami oz. jih zmanjšati?

Analiziranje in ukrepanje na podlagi teh vprašanj imenujemo upravljanje s tveganji. Ta postaja vedno bolj celovita in zahtevnejša aktivnost za zaščito KI pred izrednimi dogodki zaradi namerne ali nenamerne povzročitve. Uspešno upravljanje s tveganji izhaja iz premišljenega predvidevanja verjetnosti nastanka izrednega dogodka in obvladovanje odstopanj od predvidenega. Neustrezno upravljanje s tveganji lahko negativno vpliva na uporabnike, lastnike in upravljalce KI (Čeleta et al., 2019).

Ulieru in Worthington (2006) pravita, da je upravljanje s tveganji širok pojem in se lahko uporablja v številnih različnih disciplinah in v vsaki ima drugačen pomen.

Lahko rečemo, da je upravljanje s tveganji stalen postopek, ki vključuje identifikacijo, analizo in oceno možnih nevarnosti v sistemu ali nevarnosti, povezanih z določeno dejavnostjo. Na podlagi prepoznane slike tveganja se predlagajo ukrepi za obvladovanje tveganja – odprava ali zmanjšanje možnih škod za ljudi, okolje ali druga sredstva. ISO 31000 je osnovni standard za obvladovanje tveganj (Bialas, 2016), njemu podporni standard pa je ISO/IEC 31010 (Čeleta et al., 2019). Pri pripravi metodologije upravljanja, obvladovanja in ocenjevanja tveganj za delovanje kritične infrastrukture je standard smiselno in koristno uporabljati v sklopu izbranih metod ocenjevanja tveganj, v sklopu zakonskih zahtev in v sklopu varnostnih standardov. Ena ključnih dejavnosti tega standarda je ocenjevanje tveganj, ki pa zajema prepoznavanje, analiziranje in vrednotenje tveganj.

Čeleta in drugi (2019) navajajo, da omenjeni standard organizacijam omogoča:

- povečuje verjetnost za doseganje ciljev,
- spodbuja proaktivno vodenje,
- izboljšuje organizacijsko učenje in organizacijsko prilagodljivost,
- izboljšuje identifikacijo priložnosti in groženj,

- zmanjšuje škode in izgube,
- se zaveda potrebe po identificiranju in obravnavanju tveganj na vseh ravneh organizacije,
- vzpostavlja zanesljivo podlago za odločanje in načrtovanje,
- uspešno dodeluje in uporablja vire za obvladovanje tveganja.

Težava upravljanja s tveganjem je, da v najboljšem primeru, kadar so težave zapletene in vključujejo različne vrste tveganj, se upravljanje s tveganji v veliki meri opira na intuicijo in srečo. Organizacije so zapleteni sistemi in za učinkovito upravljanje s tveganji je ključnega pomena sistemski pogled – medsebojno povezan kompleks funkcionalno povezanih komponent. Učinkovitost vsake komponente je odvisna o tega, kako se ujema v celoto, učinkovitost celotne komponente pa je odvisna od načina delovanja vsake komponente. Sistemski pristop upošteva širše okolje, ki vpliva na procese in drugo delo (Ulieru & Worthington, 2006).

Bialas (2016) je menja, da ima vprašanje upravljanja tveganj v KI poseben značaj, saj so KI zelo zapletene, raznolike in obstajajo medsebojne povezave med različnimi infrastrukturami. Prav zaradi teh povezav je stanje vsake KI povezano s stanjem druge. Imenujemo jih medsebojne odvisnosti in jih lahko razdelimo v štiri kategorije: fizično, kibernetsko, geografsko in logično soodvisno. Dobro zavarovane KI se lahko upirajo zunanjim in notranjim motnjam in lahko delujejo na sprejemljivi ravni učinkovitosti, tudi ko se pojavijo motnje.

Upravljalci KI izvajajo ocene tveganj za doseganje ciljev poslovanja in svojih potreb pri sprejemanju odločitev, pri tem pa uporabljajo širok nabor metodologij. Metodologije tveganj so po navadi združene v kvalitativne in kvantitativne kategorije, vendar pa samo dobro načrtovani obe vrsti ocen omogočata uporabo analitičnih rezultatov. Seveda so lahko take metodologije tudi nepotrebno zapletene oz. slabo oblikovane. Ob spoznanju, da se številne metodologije ocenjevanja tveganj razvijajo v dinamičnem okolju, analitična načela služijo kot vodilo pri prihodnjih prilagoditvah. Osnovna analitična načela zagotavljajo, da so ocene tveganj dokumentirane, ponovljive in preventivne (Čeleta et al., 2019).

Čeleta in drugi (2019) poudarjajo, da upravljalci KI uporabljajo različne pristope pri upravljanju tveganj, odvisno od njihovih lastnikov, potreb sektorja, varnostnih postopkov in poslovnega okolja. Lastniki in upravljalci KI dajejo prednost in izvajajo dejavnosti za zmanjševanje tveganja na podlagi strokovne učinkovitosti, izvedljivosti in možnosti za zmanjšanje tveganja. Ukrepi za upravljanje tveganj vključujejo postopke in aktivnosti, namenjene odvračanju, zmanjševanju ranljivosti zaradi izrednega dogodka, zmanjševanju posledic in omogočajo pravočasen, učinkovit odziv ter obnovo po izrednem dogodku. Pristop za obvladovanje tveganj se osredotoča na tiste dejavnosti, ki ne da zgolj zmanjšujejo ranljivosti, vendar jih tudi preprečujejo, zaščitijo, obnavljajo in se odzivajo nanje.

5 Ugotovitve in zaključek

Ugotavljamo, da je upravljanje tveganj v organizaciji zelo pomembno, saj brez tega podjejte nikakor ne more določiti svojih ciljev za prihodnost. Če organizacija opredeli cilje, ne da bi upoštevala tveganja, obstaja verjetnost, da bo izgubila smer, ko bo neko tveganje prišlo v ospredje. Upravljanje tveganj ni več posebno ali neobvezno – potrebno ga je upoštevati vsakič, ko so odločamo ali naj pričnemo z neko aktivnostjo.

Politično, socialno in ekonomsko destabilizirana območja, teroristični napadi, kriminal, migracije, takšne in drugače nesreče bodo v prihodnosti temeljni vir ogrožanja kritičnih infrastruktur. Pri upravljanju tveganj v KI govorimo o zelo pomembnih dilemah pred katerimi se nahajajo države (Čeleta et al., 2019). Ugotavljamo, da morajo države imeti razvite sistemske mehanizme za zaščito KI. Pravilno razumevanje posameznih delov sistema KI je nujno, zato moramo v osnovi izvesti učinkovito in metodološko ustrezno ocenjevanje, upravljanja in obvladovanje tveganj za neprekinjeno delovanje KI.

Menimo, da se bodo vse KI, ki se bodo ukvarjale z upravljanjem tveganj, ukvarjale s tveganji, ki imajo tri komponente, in sicer dogodek, verjetnost pojava in vpliv. Poleg tega dobro strukturirana metodologija za upravljanje tveganj lahko učinkovito pomaga pri določanju ustreznih kontrol za zagotavljanje bistvenih zmogljivosti, kar bo pomagalo pri upravljanju teh treh komponent (Ulieru & Worthington, 2006).

Lep primer zakaj je potrebno uspešno upravljati s tveganji KI je pandemija korona virusa. Prav ta nam je pokazala kako so naši KI sistemi pripravljeni na tveganja in kako z njimi upravljajo. Večina KI ima pripravljene načrte za izredne razmere, ki jih je mogoče prilagoditi izzivom sedanje pandemije. Seveda je vsaka organizacija drugačne in se zato tudi odzivi razlikujejo glede na okolje, število primerov Covid-19 in glede na vladne ukrepe. Vsa podjetja pa stremijo k zdravju in varnosti osebja, partnerjev in strank, kontinuiteti poslovanja ter skladnosti s smernicami in predpisi, ki jih izdajajo zdravstvo in vladne agencije (Uptime Institute Intelligence team, 2020).

Moramo se zavedati, da ta pandemija ni zadnja. V zadnjih dvajsetih letih so virusni izbruhi, kot sta SARS in MERS, že povzročali smrt in gospodarske motnje. Globalizacija pomeni, da jih bo še več, nekatere pa bi lahko bile veliko bolj smrtonosne. Zato morajo biti vse KI pripravljene ves čas, tako kot so pripravljene na lokalne motnje (izpad električne energije). To pomeni, da je potrebne vse ukrepe načrtovati in pregledati kot rutinsko dobro prakso (Uptime Institute Intelligence team, 2020). Korona virus bo postal endemičen – ponavlja se vsako leto, podobno kot gripa. KI se soočajo s takojšnjimi izzivi trenutne svetovne zdravstvene krize, vendar pa morajo gledati tudi dolgoročno. Načrte je potrebno posodobiti tako da vključujejo profilaktične ukrepe in pripravljenosti.

S pregledom virov in literature prihajamo do zaključka, da so kritični infrastrukturni sistemi pomembni za preživetje celotne populacije in da jih pestijo števila tveganja. Avtorji poudarjajo, da je upravljanje s tveganji pomembna zadeva in da se jo morajo glavni deležniki KI lotiti preudarno in načrtno. Samo natančna predelitev tveganj in načrt upravljanja ter obvladovanja tveganj bo KI zaščitila pred tveganji, ki jih prinaša okolje.

Poudariti velja, da je zaščito KI in procese ocenjevanja tveganj za delovanje KI treba umestiti v celoviti proces zagotavljanja neprekinjenosti delovanja ključnih nacionalnih sistemov in učinkovito krizno upravljanje držav (Čeleta et al., 2019).

Literatura

Auerswald, P., Branscomb M., L., La Porte M., T., & Michel-Kerjan, E. (2005). The Challenge of Protecting Critical Infrastructure . *ISSUES in Science and Technology*, *XXII*(1). https://issues.org/auerswald/

Bialas, A. (2016). Risk Management in Critical Infrastructure—Foundation for Its Sustainable Work. *Sustainability*, *8*(3). https://doi.org/10.3390/su8030240

Brashear, J. P. (2019). Managing Risk to Critical Infrastructures, Their Interdependencies, and the Region They Serve: A Risk Management Process. In *Optimizing Community Infrastructure* (pp. 41–67). Elsevier. https://doi.org/10.1016/b978-0-12-816240-8.00003-3

Broder, J. F., & Tucker, E. (2012). *Risk Analysis and the Security Survey*.

Čeleta, D., Vršec, M., Bertoncelj, B., Vršec, M., Kandžič, A., & Podgoršek, Ž. (2019). *Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture*. www.mo.gov.si

Coote, B., & Hopkins, K. V. (2017). *Key Risks Companies Face in Petroleum Investment and Operations*.

HM Treasury, & Government Finance Function. (2004). The Orange Book Management of Risk: Principles and Concepts. In *London: HM Treasury* (Issue October).

Luskova, M., & Dvorak, Z. (2019). Applying Risk Management Process in Critical Infrastructure Protection. *Interdisciplinary Description of Complex Systems*, *17*(1), 7–12. https://doi.org/10.7906/indecs.17.1.2

Macaulay, T. (2008). *Critical infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*. https://doi.org/https://doi.org/10.1201/9781420068368

Murić, G., Macura, D., Gospić, N., & Bojovic, N. (2013). Jesan pristup zaštiti kritične informacione infrastrukture - An approach to critical information infrastrukture proteciton. *Konferenca o Bezbednosti Informacija BISEC*. https://www.researchgate.net/publication/251238043

O'Rourke, T. D. (2007). Critical Infrastructure, Interdependencies, and Resilience. *The Bridge*, *37*(1), 22–29.

Ongkowijoyo, C., & Doloi, H. (2017). Determining critical infrastructure risks using social network analysis. *International Journal of Disaster Resilience in the Built Environment*, *8*(1), 5–26. https://doi.org/10.1108/IJDRBE-05-2016-0016

Prezelj, I. (2009). NACIONALNA KRITIČNA INFRASTRUKTURA V REPUBLIKI SLOVENIJI. *Teorija in Praksa*, *46*, 464–484.

Prezelj, I. (2010). *Kritična infrastruktura v Sloveniji*. Fakulteta za družbene vede.

Remuzzi, A., & Remuzzi, G. (2020). COVID-19 and Italy: what next? *The Lancet*, *395*(10231), 1225–1228. https://doi.org/10.1016/S0140-6736(20)30627-9

Ulieru, M., & Worthington, P. (2006). Autonomic risk management for critical infrastructure protection. *Integrated Computer-Aided Engineering*, *13*(1), 63–80. https://doi.org/10.3233/ica-2006-13105

Uptime Institute Intelligence team. (2020). *COVID-19: Minimizing critical facility risk*. https://drift-lp-66680075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bc?mkt_tok=eyJpIjoiTkRNM01HTXpaREF4WW1WbCIsInQiOiJaYkJ2ZUZVbDFPNlQ2dklHcjl5VVRZK1AzWEtxYzJBbWNWc3I1NzI4U2xRZlFBOE9mZ3A3MmVzVEluZlp6bmNoYzZBRlIxU2pBblZBS05xbHEzQ2hncDFsbHFtdlVDcXBpMXNR