VARSTVOSLOVJE
leto 2026
letn. 28
str. 1–30

Javno-zasebno sodelovanje za varnost in odpornost kritične infrastrukture v Sloveniji: sistematični pregled literature s poudarkom na energetiki in digitalni infrastrukturi

Matevž Lipovšek, Branko Lobnikar

Namen:

Prispevek prinaša sistematični pregled literature o javno-zasebnem sodelovanju (JZS) pri zagotavljanju varnosti in odpornosti kritične infrastrukture s poudarkom na energetiki in digitalni infrastrukturi. Raziskava izhaja iz omejene razpoložljivosti empiričnih analiz operativne koordinacije in zrelosti sodelovanja v slovenskem prostoru. Cilj raziskave je identificirati ključne mehanizme sodelovanja, ovire pri izmenjavi informacij ter pristope k operacionalizaciji zrelosti in merjenju izidov odpornosti.

Metode:

Raziskava temelji na sistematičnem pregledu literature in tematski sintezi v skladu s smernicami PRISMA 2020. Pregled je zasnovan kot sistematično kartiranje, dopolnjeno s tematsko interpretacijo ugotovitev. Iskanje je bilo izvedeno v bazah Scopus, Web of Science, EBSCO in DKUM za obdobje 2018–2025. Po odstranitvi podvojenih zapisov, presejanju in presoji polnih besedil je bilo v analizo vključenih 119 virov.

Ugotovitve:

Literatura je najizraziteje usmerjena v vprašanja upravljanja in regulacije, upravljanja tveganj in operativne odpornosti ter digitalnega in kibernetskega ekosistema. Formalni institucionalni okvirji sami po sebi ne zagotavljajo učinkovite koordinacije brez operativnih omrežnih mehanizmov, kot so jasno določene vloge, kontaktne točke, protokoli izmenjave informacij in skupne vaje. Ovire za sodelovanje so pravne, organizacijske, tehnične in kulturno-relacijske narave, medtem ko je zrelost sodelovanja pogosteje konceptualno opisana kot sistematično merjena.

Omejitve/uporabnost raziskave:

Raziskava je omejena na izbrane bibliografske baze ter vire v slovenskem in angleškem jeziku. Zaradi omejenega števila empiričnih študij za slovenski prostor ugotovitve predstavljajo predvsem konceptualno osnovo za nadaljnje empirično raziskovanje in validacijo modelov sodelovanja.

Praktična uporabnost:

Prispevek ponuja izhodišča za razvoj modela zrelosti JZS, kazalnikov koordinacije in odpornosti ter izboljšanje operativnih mehanizmov sodelovanja med državnimi organi, regulatorji in upravljavci kritične infrastrukture.

Izvirnost/pomembnost:

Izvirnost prispevka je v povezovanju sistematičnega kartiranja in tematske sinteze literature s poudarkom na slovenskem kontekstu kritične infrastrukture. Ugotovitve so namenjene raziskovalcem, oblikovalcem politik, regulatorjem in operaterjem kritične infrastrukture.

Ključne besede: javno-zasebno sodelovanje, kritična infrastruktura, odpornost, Slovenija, energetika, digitalna infrastruktura

UDK: 005.934

Public–Private Collaboration for the Security and Resilience of Critical Infrastructure in Slovenia: A Systematic Literature Review Focused on the Energy and Digital Infrastructure Sectors

Purpose:

This paper systematically reviews the literature on public–private collaboration (PPC) in the security and resilience of critical infrastructure, with a particular focus on the energy and digital infrastructure sectors. The study is motivated by the limited availability of empirical analyses of operational coordination and collaboration maturity in the Slovenian context. The aim of the review is to identify key collaboration mechanisms, barriers to information sharing, and approaches to the operationalization of collaboration maturity and resilience outcomes.

Methods:

The study is based on a systematic literature review and thematic synthesis conducted in accordance with the PRISMA 2020 guidelines. The review was designed as a systematic mapping study complemented by thematic interpretation of findings. Searches were conducted in Scopus, Web of Science, EBSCO, and DKUM for the period 2018–2025. Following deduplication, screening, and full-text assessment, 119 sources were included in the analysis.

Findings:

The literature is primarily focused on issues of governance and regulation, risk management and operational resilience, as well as the digital and cyber ecosystem. Formal institutional frameworks alone do not ensure effective coordination without operational network mechanisms such as clearly defined roles, contact points, information-sharing protocols, and joint exercises. Barriers to collaboration are legal, organizational, technical, and cultural-relational in nature, while collaboration maturity is more frequently described conceptually than systematically measured.

Research limitations/implications:

The review is limited to selected bibliographic databases and sources published in Slovenian and English. Due to the limited number of empirical studies directly related to the Slovenian context, the findings primarily provide a conceptual basis for further empirical research and validation of collaboration models.

Practical implications:

The paper provides a foundation for the development of a public–private collaboration maturity model, coordination and resilience indicators, and improved operational mechanisms for cooperation among public authorities, regulators, and critical infrastructure operators.

Originality/value:

The originality of the paper lies in combining systematic mapping and thematic synthesis of the literature with a focus on the Slovenian context of critical infrastructure. The findings are intended for researchers, policymakers, regulators, and critical infrastructure operators.

Keywords: public–private collaboration, critical infrastructure, resilience, Slovenia, energy sector, digital infrastructure

UDC: 005.034

1 UVOD

Kritična infrastruktura vključuje medsebojno odvisne sisteme (npr. energija, telekomunikacije, transport, vodovodno omrežje ...), pri katerih se lahko motnje prenašajo med sektorji in sprožijo verižne učinke na delovanje družbe. Nekateri tehnični sektorji, zlasti energija in informacijsko komunikacijske tehnologije, zagotavljajo storitve, od katerih so odvisni tudi drugi družbeno ključni sistemi (zdravstvo, službe sistema zaščite in reševanja, transportne družbe). Prekinitev dobave osnovnih storitev lahko zato povzročijo obsežne posledice. Učinkovita zaščita zahteva stalno vrednotenje tveganj in krepitev odpornosti, pri čemer je pomembna tudi preventivna komponenta (sposobnost infrastrukture), da incident prepreči in s tem zmanjša prenos posledic na odvisne sektorje. S tem dopolnjuje odzivne komponente odpornosti (robustnost, obnovljivost, prilagodljivost). V prispevku je odpornost razumljena kot sposobnost kritične infrastrukture

oziroma kritičnih subjektov, da ob motnjah ohranijo izvajanje bistvenih storitev ter jih po incidentih pravočasno ponovno vzpostavijo (Rehak idr., 2023; European Union, 2022a).

V Sloveniji sta energetika in digitalna infrastruktura opredeljeni kot kritična sektorja v skladu z nacionalnim pravnim okvirom ter direktivama (EU) 2022/2555 (NIS 2) in (EU) 2022/2557 (CER). Sprejetje obeh direktiv pomeni premik od zaščite posameznih infrastrukturnih objektov k zagotavljanju neprekinjenega izvajanja bistvenih storitev in krepitvi odpornosti kritičnih subjektov. Direktivi zato poudarjata sistematično upravljanje tveganj, pripravljenost na incidente, kontinuiteto poslovanja in okrevanje po motnjah. Hkrati direktivi odgovornost za odpornost širita tudi na zasebne upravljavce kritične infrastrukture. Slovenski »Zakon o kritični infrastrukturi (ZKI-1)« (2024) te zahteve prenaša v nacionalni sistem ter vzpostavlja pravno podlago za upravljanje tveganj, krepitev odpornosti in medorganizacijsko koordinacijo (European Union, 2022a, 2022b).

Javno-zasebno sodelovanje (v nadaljevanju JZS) se v literaturi pogosto prepoznava kot pomembni mehanizem za krepitev varnosti in odpornosti kritične infrastrukture, saj je odpornost neposredno odvisna od usklajenega delovanja države (in njenih agencij) ter zasebnih lastnikov oziroma operaterjev kritične infrastrukture. JZS prispeva k zmanjševanju sektorske razdrobljenosti, jasnejšo razmejitev vlog in odgovornosti ter omogoča učinkovitejšo mobilizacijo razpoložljivih virov. V tem okviru literatura kot ključne naloge izpostavlja zlasti izvajanje nacionalnih ocen tveganj in ranljivosti, pripravo nacionalnih načrtov odpornosti ter opredelitev, kaj v posameznem kontekstu šteje kot kritična infrastruktura (Ampratwum idr., 2022).

V literaturi angleški izraz public–private partnership (PPP) ni jasno opredeljen. V infrastrukturnih in finančnih študijah se PPP uporablja predvsem za opis pogodbenih oblik sodelovanja med javnim in zasebnim sektorjem. V literaturi o varnosti in odpornosti kritične infrastrukture pa označuje širšo obliko medorganizacijskega sodelovanja, ki vključuje izmenjavo informacij, krizno koordinacijo, skupne vaje in druge operativne mehanizme (Ampratwum idr., 2022). Prispevek uporablja PPP predvsem v slednjem pomenu, torej kot obliko sodelovalnega in omrežnega upravljanja odpornosti kritične infrastrukture.

Tudi v slovenskem raziskovalnem prostoru je JZS prepoznano kot eden ključnih dejavnikov učinkovitega upravljanja in odpornosti kritične infrastrukture. Čaleta in Rolih (2011) poudarjata, da kompleksnost sodobnih groženj presega pristojnosti posameznih organizacij, zato je za učinkovito upravljanje kritične infrastrukture nujno trajno sodelovanje med državnimi institucijami in upravljavci ter usklajena obravnava fizičnih in kibernetskih tveganj. Podobno Prezelj idr. (2012) ugotavljajo, da funkcionalne povezave in medsebojne odvisnosti infrastrukturnih sistemov zahtevajo celovit medsektorski pristop, ki pomembno vpliva na ocenjevanje tveganj, načrtovanje zaščitnih ukrepov ter krepitev odpornosti kritične infrastrukture.

V okviru prispevka javni sektor predstavljajo pristojna ministrstva, regulatorji in drugi državni organi, odgovorni za oblikovanje politik, nadzor in koordinacijo upravljanja odpornosti kritične infrastrukture. Zasebni sektor predstavljajo upravljavci kritične infrastrukture in izvajalci bistvenih storitev, ki izvajajo zaščitne

ukrepe, upravljajo tveganja ter zagotavljajo neprekinjeno izvajanje storitev. JZS temelji na jasno razmejenih pristojnostih, medsebojni odvisnosti in usklajenem delovanju obeh skupin deležnikov pri načrtovanju, pripravljenosti, odzivanju in okrevanju po motnjah (Ampratwum idr., 2022).

Konceptualni okvir prispevka temelji na pristopu sodelovalnega upravljanja (angl. *network governance*), v okviru katerega je JZS razumljeno kot institucionalno in operativno sodelovanje med javnim in zasebnim sektorjem za skupno upravljanje tveganj, krepitev odpornosti ter zagotavljanje neprekinjenega izvajanja bistvenih storitev (Ansell in Gash, 2007; Provan in Kenis, 2007).

JZS je pri zaščiti kritične infrastrukture pred kibernetskimi napadi pogosto opisano kot osrednji pristop, saj je velik del digitalno odvisnih kritičnih sredstev v zasebni lasti in upravljanju, zato države same ne morejo učinkovito zagotavljati kibernetske varnosti. Za združevanje komplementarne zmogljivosti, virov in informacij med javnimi in zasebnimi akterji so nujni prožni mehanizmi sodelovanja (Pinto idr., 2021).

Čeprav je sistematični pregled osredotočen na slovenski prostor, je njegovo razumevanje smiselno umestiti tudi v širši evropski kontekst. Slovenija je kot članica Evropske unije vključena v skupni evropski regulativni okvir, kjer elektroenergetski sistem (zlasti distribucijsko omrežje) zaradi razogljičenja, decentralizacije proizvodnje, rasti samooskrbe ter elektrifikacije porabe postaja upravljavsko in operativno zahtevnejši. Vzporedno digitalno okolje ostaja izrazito izpostavljeno kibernetskim grožnjam in ranljivostim, pri čemer poročila izpostavljajo tudi pomembne organizacijske izzive (človeški dejavnik, pripravljenost in odzivanje) (SI-CERT, 2025; SODO, 2023).

Primerjalne izkušnje držav članic Evropske unije kažejo, da dolgoročna odpornost kritične infrastrukture ni odvisna zgolj od regulatornega okvira, temveč tudi od institucionaliziranega sodelovanja med javnimi organi in upravljavci kritične infrastrukture. Finski model »Comprehensive Security« temelji na trajnem medsektorskem sodelovanju, redni izmenjavi informacij, skupnem načrtovanju ter vključevanju javnega in zasebnega sektorja v pripravo na krizne razmere (Valtonen in Branders, 2020). Nemški pristop pa poudarja večnivojsko upravljanje kritične infrastrukture, pri katerem so koordinacija med zvezno državo, deželami, lokalnimi oblastmi in upravljavci infrastrukture ter jasno opredeljeni koordinacijski mehanizmi ključni za krepitev odpornosti (Monstadt in Schmidt, 2019).

Kljub posodobitvi pravnega okvira informacijske in kibernetske varnosti z uveljavitvijo »Zakona o informacijski varnosti (ZInfV-1)« (2025) ostaja ključno vprašanje, kako se normativne zahteve učinkovito prevedejo v usklajene operativne prakse med ključnimi deležniki. Da koordinacijske vrzeli niso zgolj teoretične, potrjuje tudi žledolom leta 2014. Ta je razkril pomanjkljivosti v medorganizacijskem usklajevanju pri obvladovanju posledic množičnih izpadov električne energije. Izpadi so pokazali šibko koordinacijo med zasebnimi upravljavci kritične infrastrukture in državnimi organi, zlasti pri usklajevanju med Upravo Republike Slovenije za zaščito in reševanje (URSZR) in elektrodistribucijskimi podjetji. Šibkost se je pokazala pri prioriteti ponovnih

priklopov, namestitve agregatov ter pravočasnega obveščanja lokalnih skupnosti (Uprava Republike Slovenije za zaščito in reševanje, 2019).

Vzroki za omejeno odpornost so pogosto povezani s sektorsko razdrobljenim upravljanjem in kompleksnimi medsebojnimi odvisnostmi (angl. *system of systems*), kar zahteva skupno načrtovanje, dogovorjene prednosti pri obnovi ter varne mehanizme izmenjave informacij med javnimi organi in operaterji (Lewis in Petit, 2019). Dosedanje priložnostne oblike sodelovanja, ki se pogosto opirajo na namenske posameznike in osebne odnose, je smiselno nadgraditi z bolj sistematičnimi in formaliziranimi mehanizmi ter z okvirom za ocenjevanje in spremljanje izboljšav, ki omogoča bolj strukturirano in primerljivo presojo sodelovanja (Rydén Sonesson idr., 2021).

V slovenskem prostoru so pristojnosti za upravljanje kritične infrastrukture razdeljene med več državnih organov, regulatorjev in upravljavcev kritične infrastrukture, kar povečuje pomen usklajenega JZS pri obvladovanju tveganj, izmenjavi informacij in krizni koordinaciji. Slovenska literatura pri tem poudarja, da kompleksnost medsebojno odvisnih infrastrukturnih sistemov zahteva okrepljene koordinacijske mehanizme ter učinkovite mehanizme sodelovanja med javnimi in zasebnimi deležniki (Prezelj idr., 2012; Ministrstvo za obrambo Republike Slovenije, 2019).

NIS 2 vzpostavlja okvir za bistvene in pomembne subjekte ter določa ukrepe za upravljanje kibernetskih tveganj in obveznosti poročanja. Med zahtevanimi ukrepi so tudi obvladovanje incidentov, zagotavljanje kontinuitete (npr. varnostne kopije in okrevanje po nesreči) ter krizno upravljanje, pri čemer se poudarja koordinacija in urejeni mehanizmi izmenjave informacij prek pristojnih struktur (European Union, 2022b)

European Bank for Reconstruction and Development (2024) ugotavlja omejen interes za JZS v Sloveniji ter poudarja potrebo po krepitvi zmogljivosti in ozaveščanja. Zato je upravljanje kritične infrastrukture smiselno analizirati z vidika modelov, ki omogočajo ohranjanje ključnih funkcij, zmanjšanje trajanja izpadov in hitrejše okrevanje. Pri tem okrevanje ne pomeni nujno povratka v prejšnje stanje, temveč lahko vključuje prilagoditev novim razmeram (Ferrari, 2020).

V članku ločujemo med viri, vključenimi v sistematično kartiranje (angl. *included studies N* = 119), in kontekstnimi viri, ki služijo umeščanju teme (npr. strateški dokumenti, regulativni okvir). Kjer je vir uporabljen kot del evidence kartiranja, je obravnavan v rezultatih, kjer pa služi zgolj kontekstu, je to v besedilu jasno označeno.

Zaradi opisanih vrzeli v operativni koordinaciji in omejene empirike za Slovenijo je smiselno najprej sistematično kartirati, kaj literatura ponuja glede mehanizmov sodelovanja, ovir in merljivih izidov odpornosti. Namen prispevka je sistematično pregledati in tematsko sintetizirati literaturo (2018–2025) o JZS na področju varnosti in odpornosti kritične infrastrukture, s poudarkom na energetiki in digitalni infrastrukturi ter na tej osnovi oblikovati izhodišča za nadaljnjo empirično raziskavo in prakso v Sloveniji. V skladu s tem prispevek naslavlja raziskovalna vprašanja o koordinaciji v krizah, ovirah deljenja informacij ter operacionalizaciji zrelosti in izidov (npr. okrevanje).

1.1 Namen in raziskovalna vprašanja

Empirične raziskave kažejo, da medsektorsko sodelovanje in izmenjava informacij pri zaščiti kritične infrastrukture pogosto temeljita na neformalnih mrežah in zaupanju, medtem ko so sistematično razviti koordinacijski mehanizmi in primerljivi kazalniki odpornosti še razmeroma omejeni (Rydén Sonesson idr., 2021).

V slovenskem kontekstu se ob tem odpira vprašanje operativne koordinacije ter razpoložljivosti empiričnih analiz JZS pri upravljanju kritične infrastrukture.

Namen prispevka je sistematično pregledati literaturo o javno-zasebnem sodelovanju pri odpornosti kritične infrastrukture s poudarkom na energetskem in digitalnem sektorju. Prispevek analizira operativne mehanizme sodelovanja, ovire pri izmenjavi informacij ter pristope k operacionalizaciji zrelosti sodelovanja in izidov odpornosti. Poseben poudarek je namenjen koordinaciji med deležniki v kriznih razmerah ter razvoju konceptualnega modela sodelovanja in odpornosti kritične infrastrukture.

Pregled vodi nabor treh raziskovalnih vprašanj:

- RV1: razmerje med institucionalnimi ureditvami, omrežnimi značilnostmi JZS in učinkovitostjo krizne koordinacije,
- RV2: večplastne ovire, ki omejujejo izmenjavo informacij in skupno delovanje, ter
- RV3: obravnava zrelosti sodelovanja v literaturi (upravljanje, deljenje informacij, vaje, neprekinjeno delovanje) in njena povezava z merljivimi izidi odpornosti, kot so časovni kazalniki okrevanja, na primer *Recovery Time Objective* (RTO), ki predstavlja ciljni najdaljši dopustni čas za ponovno vzpostavitev kritične storitve po motnji, ter *Mean Time to Repair* (MTTR), ki označuje dejansko povprečno trajanje odprave okvare oziroma ponovne vzpostavitve normalnega delovanja sistema (Swanson idr., 2010; Torell in Avelar, 2004).

Glavni cilj pregleda je razviti dokazno podlago za nadaljnji razvoj empirično preverljivega modela zrelosti JZS za varnost in odpornost kritične infrastrukture v Sloveniji. Specifični cilji vključujejo identifikacijo praks sodelovanja, razvoj konceptualnih kazalnikovkoordinacije in odpornosti, zasnovo okvirnega modela zrelosti ter načrt nadaljnje validacije (npr. Delphi) (Gharaee idr., 2023).

2 METODE

2.1 Zasnova pregleda

Sistematični pregled literature je bil dokumentiran in poročan v skladu s smernicami PRISMA 2020, s čimer smo zagotovili preglednost, sledljivost in ponovljivost postopka identifikacije ter selekcije virov (Page idr., 2021). Pregled je zasnovan kot sistematično kartiranje (angl. *systematic mapping*), katerega namen je celovito zbrati, opisati in katalogizirati razpoložljive dokaze ter prikazati tematsko porazdelitev raziskav, tipe virov in raziskovalne vrzeli (James idr., 2016).

Sistematično kartiranje je bilo uporabljeno predvsem za deskriptivni prikaz pokritosti področja (teme, sektorji, metodološki pristopi in raziskovalne vrzeli). Za interpretativno povezovanje vsebinskih ugotovitev v odnosu do raziskovalnih vprašanj RV1–RV3 pa je bila uporabljena tematska sinteza. Takšna kombinacija omogoča hkratno kartiranje strukture dokazne baze ter poglobljeno sintezo ponavljajočih se mehanizmov, ovir in konceptov sodelovanja (Petersen idr., 2008; Thomas in Harden, 2008).

Ugotovitve iz heterogenih virov smo integrirali s tematsko sintezo. Analiza je bila omejena na obdobje 2018–2025. Začetna evidenca je obsegala 321 zapisov iz bibliografskih baz in repozitorijev. Po odstranitvi 48 dvojnikov je evidenca obsegala 273 unikatnih zapisov. Po postopku presejanja in presoje celotnih besedil je bil v sistematično kartiranje in tematsko sintezo vključen končni korpus $N = 119$ virov, ki so bili razvrščeni v šest tematskih domen.

2.2 Viri podatkov in iskalna strategija

Iskanje literature je bilo izvedeno v bibliografskih bazah Scopus, Web of Science, EBSCO in repozitoriju DKUM med 15. in 31. januarjem 2026. Iskalna strategija je bila izvedena v več iteracijah, pri čemer so bile uporabljene širše in ožje kombinacije ključnih izrazov. V evidenco selekcije je bilo zajetih 321 zapisov, identificiranih prek navedenih virov. Razporeditev identificiranih zapisov po posameznih bibliografskih bazah je prikazana v tabeli 1.

Tabela 1
Število zadetkov po posamezni bazi (Scopus, WoS, EBSCO, DKUM)

Baza	Št. zadetkov
Scopus	142
Web of Science	87
EBSCO	61
DKUM	31
SKUPAJ	321

Iskalne poizvedbe so kombinirale izraze, povezane s kritično infrastrukturo (angl. *critical infrastructure* (CI)), javno-zasebnim sodelovanjem (angl. *public-private partnership*, *public-private collaboration*) ter odpornostjo in varnostjo (angl. *resilience*, *security*), z omejitvijo na obdobje 2018–2025 in relevantni EU/nacionalni kontekst. Strategija je potekala v dveh korakih: najprej so bile uporabljene širše poizvedbe za zajem celotnega tematskega polja, nato pa ožje kombinacije izrazov, vezane na energetiko, digitalno infrastrukturo, krizno koordinacijo, deljenje informacij in okrevanje. Vključeni so bili viri v angleškem in slovenskem jeziku; kjer je to omogočala posamezna baza, je bila jezikovna omejitev uporabljena že v fazi iskanja, sicer pa v fazi presejanja.

Metodološko pojasnilo: prikazano število zadetkov po posameznih bazah predstavlja začetni obseg rezultatov iskanja. Diagram PRISMA temelji na dejansko zajetih zapisih, ki so bili vključeni v evidenco selekcije ter nadalje obravnavani pri odstranitvi dvojnikov in presejanju.

2.3 Merila vključitve in izključitve

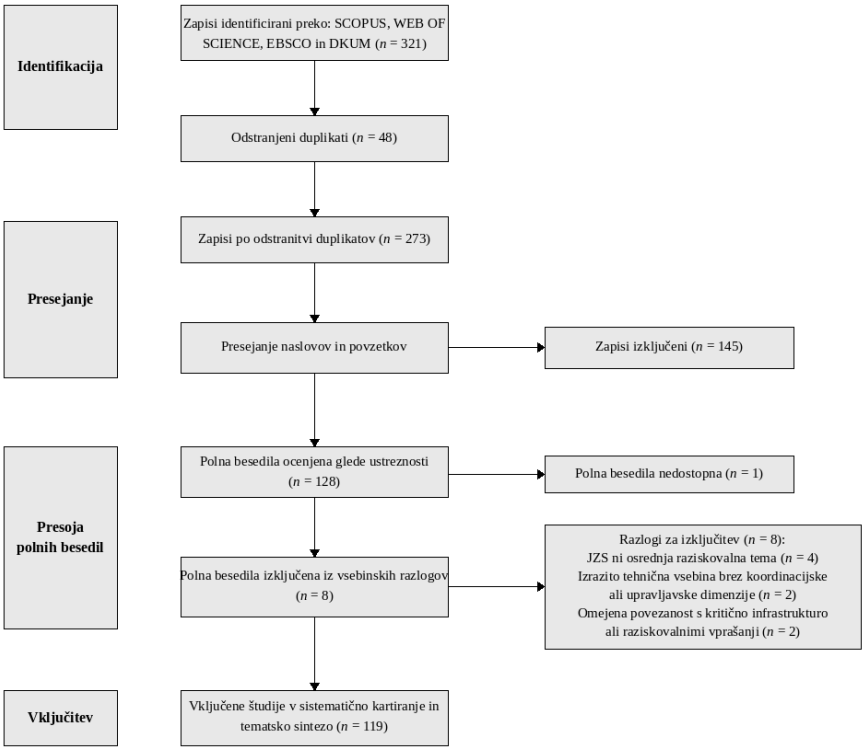
Viri so bili vključeni, če so: časovno umeščeni v obdobje 2018–2025, vsebinsko obravnavali kritično infrastrukturo (energetika in/ali digitalna infrastruktura) v povezavi z JZS, vsebovali elemente, relevantne za odpornost in varnost (koordinacija, deljenje informacij, kontinuiteta, okrevanje, soodvisnosti) ter bili dostopni v obliki, ki je omogočala vsebinsko presojo in kodiranje.

Zaradi narave raziskovalnih vprašanj so bili poleg znanstvenih objav vključeni tudi izbrani strateški in pravni dokumenti, če so neposredno obravnavali JZS, varnost ali odpornost kritične infrastrukture v relevantnem kontekstu. Viri so bili izključeni, če JZS ni predstavljalo osrednje teme, če je šlo za izrazito tehnične prispevke brez koordinacijske razsežnosti ali če dostop do celotnega besedila ni omogočal vsebinske presoje.

2.4 Postopek selekcije virov (PRISMA tok)

V evidenco pregleda je bilo identificiranih 321 zapisov iz bibliografskih baz in repozitorijev. Pred presejanjem je bilo odstranjenih 48 dvojnikov, tako da je bilo v nadaljnji postopek presejanja vključenih 273 unikatnih zapisov. Presejanje naslovov in povzetkov je bilo izvedeno glede na vnaprej določena merila vključitve in izključitve. Na tej podlagi je bilo 128 zapisov izbranih za presojo celotnega besedila. Pri presoji polnih besedil je bilo izključenih 8 virov zaradi vsebinskih razlogov: 4 zaradi nezadostne vsebinske povezanosti z JZS pri kritični infrastrukturi, 2 zaradi izrazito tehnične usmerjenosti brez koordinacijske oziroma upravljavske dimenzije ter 2 zaradi omejene povezanosti s kritično infrastrukturo ali raziskovalnimi vprašanji pregleda. Dodatno 1 vir ni bil vključen zaradi nedostopnosti celotnega besedila. Po zaključeni presoji je bil v sistematično kartiranje in tematsko sintezo vključen končni korpus $N = 119$ virov. Potek selekcije virov je prikazan v diagramu PRISMA (slika 1).

Slika 1
Diagram PRISMA 2020 poteka identifikacije, presejanja in vključitve virov



Vir: lastni prikaz

2.5 Ekstrakcija podatkov in kodiranje

Za vsak vključen vir smo izluščili ključne metapodatke (leto, tip vira, sektor, geografski fokus, metodološki pristop) ter vsebinske elemente, relevantne za RV1–RV3. Kodiranje je potekalo hierarhično na podlagi večnivojskega kodnega okvira. Na ravni kod 1. reda so bile posameznim odlomkom oziroma ugotovitvam dodeljene podrobne vsebinske oznake. Te so bile nato združene v 25 tem 2. reda, ki predstavljajo konceptualne tematske sklope, slednje pa v 6 tematskih domen 3. reda, uporabljenih za kartiranje in sintezo. Thomas in Harden (2008) navajata, da takšna struktura omogoča sledljivost od kodiranih odlomkov do sinteznih tematskih ugotovitev.

Hierarhična struktura kodiranja metodološko sledi logiki Gioia pristopa, vendar je bila uporabljena kot analitični okvir za organizacijo literature in ne za induktivno gradnjo teorije iz primarnih podatkov. Takšna struktura je bila uporabljena predvsem za povečanje preglednosti, sledljivosti in konceptualne koherence analitičnega procesa ter za povezovanje ponavljajočih se mehanizmov sodelovanja, ovir pri izmenjavi informacij in pristopov k operacionalizaciji odpornosti kritične infrastrukture. Hierarhično grupiranje konceptov in tem je omogočilo hkratno opisno kartiranje dokazne baze ter interpretativno sintezo

vsebinskih ugotovitev, povezanih z raziskovalnimi vprašanji RV1–RV3 (Gioia idr., 2013).

Za integracijo ugotovitev je bila uporabljena tematska sinteza, ki omogoča združevanje ugotovitev iz heterogenih virov. Analiza je bila izvedena v dveh korakih: deskriptivno kartiranje in tematska interpretacija v povezavi z RV1–RV3.

2.5.1 Struktura tematskega kartiranja

Na podlagi hierarhičnega kodiranja je bilo vključenih 119 virov, razvrščenih v šest tematskih domen, ki predstavljajo širše konceptualne sklope sistematičnega kartiranja. Posamezne domene vključujejo tematske sklope 2. reda, povezane z upravljanjem, odpornostjo, digitalnim okoljem, sektorsko infrastrukturo, deležniki ter analitičnimi pristopi. Tabela 2 prikazuje razporeditev vključenih virov po tematskih domenah, prevladujočih sektorjih in metodoloških pristopih.

Tabela 2
Tematske domene sistematičnega kartiranja in značilnosti vključenih virov

Tematska domena	Primeri tem 2. reda	Št. virov	Prevladujoč sektor	Metodološki pristopi
Upravljanje, regulacija in institucionalni okvir	pravni in regulativni okvir; upravljanje in institucionalne vloge; strategije, politike in načrtovanje; financiranje in modeli; mednarodno sodelovanje	28	večsektorski	konceptualne študije, analiza politik, sistematični pregled
Upravljanje tveganj in operativna odpornost	ocena tveganj in ranljivosti; odpornost in kontinuiteta poslovanja; krizno upravljanje in odziv; kaskadni učinki in medodvisnosti; fizična varnost	24	energetika, večsektorski	študija primera modeli odpornosti kvalitativna analiza
Digitalni in kibernetski ekosistem	kibernetska varnost in nacionalni centri za koordinacijo odziva (CSIRT); digitalizacija in IT infrastruktura; podatki, standardi in interoperabilnost; umetna inteligenca in nove tehnologije	21	digitalna infrastruktura	tehnično-konceptualne študije, okviri kibernetske varnosti empirične raziskave
Sektorska kritična infrastruktura	energetika; promet; zdravstvo; industrija in tehnološke nesreče; vesoljska infrastruktura	18	energetski sektor	sektorske analize, primerjalne študije
Ljudje, organizacije in deležniki	kapacitete, usposabljanje in HR; komunikacija, javnost in deležniki; organizacijska kultura; medorganizacijsko sodelovanje	15	večsektorski	kvalitativne raziskave, analiza deležnikov, intervjuji
Analitika, modeli in kazalniki odpornosti	modeli zrelosti; ključni kazalniki uspešnosti (KPI) in merjenje odpornosti; MTTR/RTO; metodološki pristopi in analitični modeli	13	večsektorski	modeli zrelosti, analiza KPI, kvantitativni modeli

2.6 Omejitve metodološkega pristopa

Kartiranje in tematska sinteza omogočata širok pregled področja, vendar ne zagotavljata nujno primerljivosti izidov med viri, kadar študije uporabljajo različne definicije, kazalnike ali metodološke pristope. Razlaga ugotovitev je dodatno omejena z razpoložljivostjo empiričnih študij za posamezne nacionalne kontekste ter z neenakomerno porazdelitvijo tem v dokazni bazi. Za slovenski prostor je neposredno primerljivih empiričnih raziskav razmeroma malo, zato ugotovitve pregleda predstavljajo predvsem konceptualno in kartografsko osnovo za nadaljnje raziskovanje.

Dodatno omejitev predstavlja dejstvo, da je presejanje virov, presojo ustreznosti in kodiranje izvedel en raziskovalec. Zaradi tega ni bilo mogoče izračunati medocenjevalske zanesljivosti (npr. Cohenov κ), kar lahko poveča tveganje subjektivne interpretacije pri selekciji in kodiranju virov (McHugh, 2012).

Za zmanjšanje tveganja subjektivne presoje je bil pred začetkom analize pripravljen vnaprej opredeljen kodni okvir. Temeljil je na raziskovalnih vprašanjih (RV1–RV3), jasno določenih merilih vključitve in izključitve ter hierarhičnem postopku kodiranja. Vse odločitve glede vključitve virov in razvrščanja kod so bile dosledno dokumentirane, kar je prispevalo k večji sledljivosti in doslednosti analitičnega postopka (Thomas in Harden, 2008; Page idr., 2021).

Pregledni protokol pred začetkom raziskave ni bil predregistriran v sistemih PROSPERO ali Open Science Framework (OSF), kar predstavlja omejitev z vidika formalne transparentnosti sistematičnega pregleda, čeprav so bili postopki identifikacije, presejanja in selekcije virov dokumentirani skladno s smernicami PRISMA 2020 (Page idr., 2021)

Pregled literature je bil omejen na bibliografske baze Scopus, Web of Science, EBSCO in DKUM. Čeprav navedene baze pokrivajo pomemben del relevantne znanstvene produkcije, iskanje ni sistematično zajelo širše sive literature in institucionalnih virov (npr. ENISA, NIST, CISA, OSCE), ki na področju varnosti in odpornosti kritične infrastrukture pogosto vsebujejo pomembne operativne usmeritve. Posamezni tovrstni dokumenti so bili vključeni kontekstualno, vendar ne na podlagi ločeno zasnovanega sistematičnega pregleda sive literature.

Dodatno je bil pregled omejen na vire v angleškem in slovenskem jeziku, kar lahko pomeni, da niso bile zajete nekatere relevantne raziskave iz drugih jezikovnih okolij (nemškega, francoskega in nordijskega prostora), kjer so raziskave odpornosti kritične infrastrukture in medorganizacijskega upravljanja razmeroma razvite. Iskanje literature je bilo izvedeno med 15. in 31. januarjem 2026, zato študije, indeksirane po zaključku iskalnega obdobja, niso bile vključene v pregled.

Vsebinsko je bil pregled usmerjen predvsem v energetiko in digitalno infrastrukturo, saj gre za sektorja z izrazitimi medsebojnimi odvisnostmi ter visoko izpostavljenostjo kibernetskim in operativnim tveganjem. Takšna usmeritev omogoča bolj osredotočeno analizo raziskovalnih vprašanj, vendar hkrati pomeni, da pregled ne zajame v enaki meri drugih kritičnih sektorjev (npr.: promet, zdravstvo ali oskrba z vodo), kjer se institucionalne ureditve, operativni modeli in javno-zasebni mehanizmi sodelovanja lahko pomembno razlikujejo.

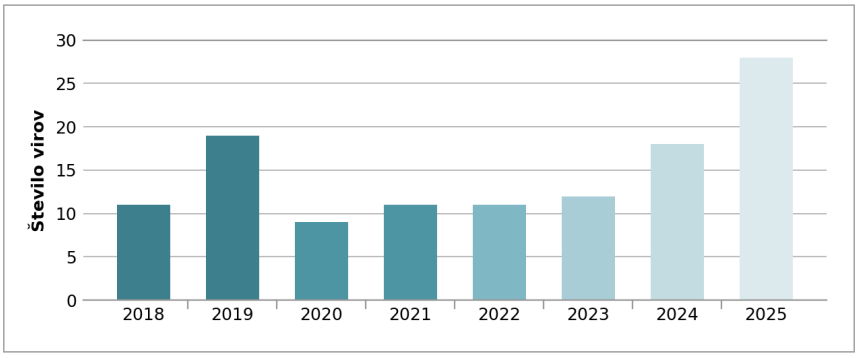
Ker je pregled zasnovan kot sistematično kartiranje, formalna ocena kakovosti posameznih študij oziroma presoja tveganja pristranskosti (angl. *risk of bias assessment*) ni bila izvedena. Posledično je treba ugotovitve interpretirati predvsem kot pregled tematske strukture in raziskovalnih trendov, ne pa kot dokaz o relativni kakovosti ali moči posameznih empiričnih ugotovitev.

3 UGOTOVITVE

3.1 Deskriptivno kartiranje dokazne baze (2018–2025)

Kartiranje literature za obdobje 2018–2025 kaže premik od splošnih, konceptualnih razprav o JZS k bolj operativnim vprašanjem, ki so neposredno povezana z obvladovanjem motenj in okrevanjem kritičnih subjektov. V ospredje stopajo zlasti pravila deljenja informacij in podatkov, koordinacija upravljanja incidentov, poslovna kontinuiteta, načrtovanje okrevanja, skupne vaje ter potreba po bolj sistematičnem vrednotenju učinkovitosti odziva in obnove. Ta usmeritev odraža širše institucionalno okolje, v katerem se odpornost kritične infrastrukture vse bolj obravnava skozi prizmo medsebojnih odvisnosti omrežnih sistemov ter potrebe po usklajenem delovanju javnih organov in zasebnih operaterjev (Ampratwum idr., 2022).

Za boljšo preglednost dokazne baze smo v okviru sistematičnega kartiranja izvedli tudi deskriptivno analizo razporeditve vključenih virov glede na leto objave, raziskovalna vprašanja, sektorje in metodološke pristope. Razporeditev vključenih virov po letih objave prikazuje graf 1.



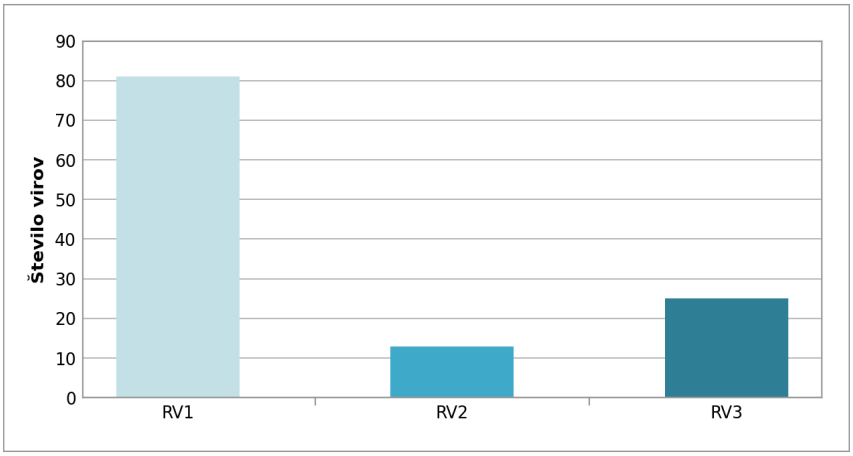
Graf 1
Razporeditev vključenih virov po letih objave (2018–2025)

Vir: lastni prikaz

Časovna razporeditev virov kaže postopno rast števila objav po letu 2020, kar sovpada s povečano regulatorno in raziskovalno pozornostjo področju odpornosti kritične infrastrukture, kibernetske varnosti in krizne koordinacije v okviru evropskih politik odpornosti.

Razporeditev virov glede na raziskovalna vprašanja RV1–RV3 prikazuje graf 2.

Graf 2
Razporeditev virov glede na raziskovalna vprašanja (RV1–RV3)



Vir: lastni prikaz

Kartiranje dokazne baze kaže, da je največji delež vključenih virov obravnaval vprašanja institucionalnega upravljanja, koordinacije in omrežnih značilnosti JZS (RV1), sledijo raziskave o ovirah pri izmenjavi informacij in skupnem odzivanju (RV2), najmanj pa je bilo študij, ki bi sistematično operacionalizirale zrelost sodelovanja in jo povezovale z merljivimi izidi odpornosti (RV3).

Strukturo dokazne baze glede na prevladujoče sektorje in metodološke pristope prikazuje tabela 3.

Tabela 3
Razporeditev virov po sektorjih

Kategorija	Št. virov
Energetika	25
Digitalna infrastruktura	34
Večsektorski pristopi	47
Promet	8
Zdravstvo	3
Industrija/tehnološke nesreče	2
SKUPAJ	**119**

Razporeditev vključenih virov glede na metodološke pristope prikazuje tabela 4.

Tabela 4
Razporeditev po metodoloških pristopih

Metodološki pristop	Št. virov
Konceptualne študije in teoretični okviri	42
Regulativne analize	10
Sistematični pregledi literature	4
Študije primerov	9
Kvalitativne raziskave	2
Kvantitativni modeli in KPI pristopi	52
SKUPAJ	**119**

Deskriptivno kartiranje kaže, da dokazna baza prevladujoče temelji na konceptualnih in kvalitativnih pristopih, empiričnih študij z neposredno operacionalizacijo izidov odpornosti pa je razmeroma malo. V sektorskem smislu prevladujeta energetika in digitalna infrastruktura. To je skladno s povečano izpostavljenostjo teh sistemov kibernetskim grožnjam, regulativnim zahtevam in medsebojnim odvisnostim kritične infrastrukture.

Ta trend je mogoče razumeti kot odraz institucionalnega okolja, v katerem se odpornost kritične infrastrukture vse bolj obravnava skozi prizmo upravljanja in koordinacije ter obvladovanja kaskadnih učinkov. Ti izhajajo iz medsebojnih odvisnosti omrežnih sistemov in so tesno povezani z zanesljivostjo zagotavljanja ključnih storitev (Ferrari, 2020; Rehak idr. 2023).

V evropskem prostoru k temu dodatno prispeva krepitev regulativnega okvira na področju kibernetske varnosti in odpornosti kritičnih subjektov (Direktiva (EU) 2022/2555), ki poleg organizacijskih ukrepov poudarja zahteve po obvladovanju incidentov, kontinuiteti, poročanju ter koordinaciji prek pristojnih organov in mehanizmov izmenjave informacij. Ampratwum idr. (2022) opozarjajo, da zgolj normativna trditev o koristnosti JZS ne zadošča in je treba učinke operacionalizirati skozi jasno opredeljene cilje partnerstva in merljive kazalnike odpornosti (izguba funkcionalnosti in čas obnove) ter jih empirično preveriti.

3.2 Geografski fokus: mednarodni okvir in omejena evidenca za Slovenijo

Geografsko kartiranje dokazne baze kaže, da je pomemben del vključenih študij vsebinsko prenosljiv, saj izhaja iz primerjalnih okolij, mednarodnih politik in omrežnih oblik upravljanja (okviri EU, čezmejne prakse ter standardizacijski pristopi). V teh okoljih se politike oblikujejo in izvajajo prek večnivojskih omrežij, v katerih so javni akterji praviloma dominantni, zasebni pa pogosto sodelujejo prek neformalnih in posvetovalnih mehanizmov (Börzel in Heard-Lauréote, 2009). Tudi kadar so študije umeščene v konkretne nacionalne kontekste, njihove ugotovitve pogosto prispevajo k širšemu razumevanju delovanja, razvoja in učinkovitosti omrežnega upravljanja v medorganizacijskih omrežjih deležnikov (Wegner idr., 2019).

Geografska razporeditev vključenih virov glede na primarni raziskovalni fokus je prikazana v tabeli 5.

Tabela 5
Geografska razporeditev vključenih virov glede na primarni raziskovalni fokus

Država	Število člankov
EU (splošno)	28
Slovenija	32
Francija	6
Švedska	5
Poljska	4
Italija	4
Hrvaška	3
Madžarska	2

Srbija	3
Albanija	1
Bosna	1
Združene države Amerike	14
Avstralija	3
Egipt	2
Kitajska	1
Velika Britanija	1
Drugo (mednarodno)	9
SKUPAJ	**119**

Razporeditev vključenih virov kaže izrazito prevlado evropskega in širšega mednarodnega regulatornega prostora. Pri tem predstavljajo pomemben delež tudi slovenski viri, povezani z nacionalnim pravnim in institucionalnim okvirom kritične infrastrukture. Poleg več državnih evropskih študij so v dokazni bazi prisotni tudi nacionalni primeri iz Združenih držav Amerike ter iz posameznih evropskih držav (nordijske države, srednja in jugovzhodna Evropa), kar potrjuje mednarodno in primerjalno naravo raziskovalnega področja.

Za slovenski kontekst to pomeni pomembno omejitev posploševanja. Čeprav je prispevek motiviran s slovenskimi izzivi, je empiričnih analiz delovanja JZS v Sloveniji, zlasti takšnih, ki bi omogočale ocenjevanje na podlagi merljivih izidov in primerljivih kazalnikov, razmeroma malo. Zato so ugotovitve pregleda najmočnejše pri oblikovanju konceptualnega okvira področja, opisu pokritosti (kaj je raziskano in kako) ter identifikaciji vrzeli in prioritet za nadaljnje empirično raziskovanje, manj pa pri trditvah o merljivih izidih ali dejanski zrelosti JZS v Sloveniji brez dodatne empirične validacije, kar je skladno z namenom sistematičnega kartiranja (Petersen idr., 2008).

V skladu s tem prispevek dosledno ločuje med viri, vključenimi v kartiranje (angl. *included studies*), in kontekstnimi viri, ki služijo umeščanju teme, ne pa dokazovanju izidov.

3.3 Povezanost institucionalnih ureditev, omrežnih značilnosti JZS in koordinacije (RV1)

Literatura prikazuje, da so formalni institucionalni okviri nujni pogoj za delovanje JZS na področju kritične infrastrukture, vendar sami po sebi ne zagotavljajo učinkovite koordinacije v krizah. Vključene študije pogosto poudarjajo, da formalni institucionalni okvirji brez operativnih omrežnih mehanizmov (jasne vloge, pravila sodelovanja, kontaktne točke in ustaljene komunikacijske poti) ostanejo premalo učinkoviti v praksi (Ansell in Gash, 2007; Provan in Kenis, 2007).

Literatura JZS pogosto obravnava kot obliko omrežnega upravljanja (angl. *network governance*), kjer učinkovitost izhaja predvsem iz sposobnosti omrežja, da vzpostavi usklajena pravila, mehanizme odločanja in reševanja sporov. Literatura kot pomemben dejavnik izpostavlja organiziranost omrežja. Ključno vprašanje je, ali temelji na relativno stabilni strukturi z jasno opredeljenimi

vozlišči koordinacije ali pa ostaja pretežno *ad hoc* in odvisno od posameznikov, kar zmanjšuje predvidljivost in ponovljivost koordinacije v kriznih razmerah (Provan in Kenis, 2007).

V vključeni literaturi se med pogosteje obravnavanimi mehanizmi pojavljajo formalizirane koordinacijske forume (sektorske skupine, stalna delovna telesa, skupni operativni centri ali jasno določene točke stika). Njihov namen je zagotoviti, da se informacije in odločitve v krizi pretakajo po predvidljivih poteh, z vnaprej dogovorjenimi odgovornostmi in pragovi eskalacije (Department of Homeland Security, 2013).

V energetiki se operativna kompleksnost povečuje predvsem zaradi naraščajočega vključevanja razpršene proizvodnje ter širšega prehoda v bolj decentralizirane in digitalno podprte omrežne arhitekture (mikroomrežja, prožnost porabe), kar zahteva bolj usklajene pristope k upravljanju in zagotavljanju odpornosti sistema (Borysiak idr., 2025). V digitalni infrastrukturi sta v ospredju interoperabilnost in čezmejno usklajevanje, pri čemer evropska pravila spodbujajo standardizacijo izmenjave informacij in koordinirane odzive (Leitner idr., 2024).

Kartiranje dokazne baze (2018–2025) kaže, da so razprave, relevantne za RV1, najizraziteje povezane z vprašanji upravljanja in institucionalnih vlog, pravnega in regulativnega okvira, digitalizacije in IT infrastrukture, ocene tveganj in ranljivosti ter odpornosti in kontinuitete poslovanja. To je skladno z delom literature, ki koordinacijo obravnava kot rezultat omrežnih odnosov in operativnih mehanizmov, ne zgolj formalnih pravil (Rydén Sonesson idr., 2021).

3.4 Ključne ovire za izmenjavo informacij in skupno odzivanje (RV2)

Ovire za izmenjavo informacij in skupno odzivanje v javno-zasebnih omrežjih kritične infrastrukture so praviloma večplastne in se medsebojno krepijo. Pravna nejasnost, organizacijska zadržanost, tehnične omejitve ter kulturni dejavniki zmanjšujejo pripravljenost za hitro in sledljivo deljenje podatkov ter usklajeno ukrepanje v krizi (Ampratwum idr., 2022).

Na pravni ravni se ovire kažejo kot negotovost glede razmejitve odgovornosti, dopustnih obsegov deljenja informacij in pogojev posredovanja podatkov, kar povzroča zadržanost pri posredovanju informacij (Lewis in Petit, 2019; »ZKI-1«, 2024). Na organizacijski ravni je izmenjava informacij pogosto omejena zaradi strahu pred izgubo konkurenčne prednosti oziroma razkritjem lastnih ranljivosti. K zadržanosti prispevajo tudi neusklajene spodbude in nejasna razdelitev stroškov zaščite pri JZS (Giacomello, 2021).

Na tehnični ravni ovire izvirajo predvsem iz pomanjkljive interoperabilnosti, ki zajema usklajevanje podatkovne sintakse in pomenov na informacijskem sloju ter standardizacijo protokolov in podatkovnih tokov na komunikacijskem sloju. Varnostni vidiki obenem zahtevajo segmentacijo omrežij in nadzorovane povezave, podprte z mehanizmi, kot so požarni zidovi in koncept varnostnih con in komunikacijskih povezav (angl. *zones and conduits*), kar omogoča varno in sledljivo izmenjavo med sistemi (Sellitto idr., 2021).

Na kulturni ravni so pomembni zaupanje, razlike v organizacijskih kulturah in pričakovanja glede transparentnosti. V nekaterih omrežjih se izmenjava deloma

opira na neformalne komunikacijske kanale, kar lahko pospeši *ad hoc* usklajevanje, vendar otežuje dosledno standardizacijo postopkov (Sienkiewicz-Małyjurek in Owczarek, 2020).

Sektorsko se poudarki razlikujejo. V energetiki so v krizah ključne operativne informacije o stanju omrežja ter usklajevanje obnovitvenih aktivnosti, v digitalni infrastrukturi pa prevladujejo časovno kritični in pogosto občutljivi podatki incidentov, povezani z bolj strukturiranimi postopki poročanja in koordinacije. Ker so energetski in digitalni sistemi prepleteni, motnja v enem sektorju hitro sproži učinke v drugem, zato dogovorjeni protokoli izmenjave podatkov ter skupno razumevanje medsebojnih odvisnosti predstavljajo jedro učinkovitega skupnega odzivanja (Rydén Sonesson idr., 2021; Volk, 2024).

V literaturi se kot pogost pristop za zmanjševanje ovir pri skupnem odzivanju pojavljajo jasno opredeljene vloge, vnaprej dogovorjeni postopki deljenja informacij, redne skupne vaje ter spremljanje učinkovitosti odziva z vnaprej določenimi kazalniki uspešnosti (Nelson idr., 2025).

3.5 Konceptualizacija in operacionalizacija zrelosti ter povezava z izidi (RV3)

Zrelost JZS pri kritični infrastrukturi je mogoče opredeliti kot večdimenzionalni konstrukt, ki vključuje upravljanje in jasnost vlog, pravila deljenja informacij, skupne vaje in učenje ter prakse neprekinjenega delovanja oziroma pripravljenost na motnje (Pettit idr., 2010). Ponavljajoča se ugotovitev v literaturi o JZS je, da je zrelost pogosto opisana na konceptualni ravni, redkeje pa dosledno operacionalizirana v primerljive kazalnike, kar otežuje kumulativno primerjavo med študijami in sektorji (Ampratwum idr., 2022).

Ko študije zrelost merijo s kazalniki, jo praviloma operacionalizirajo prek procesnih, izvedbenih ter neposrednih kazalnikov uspešnosti (npr. stopnja formaliziranosti postopkov, pogostost in kakovost vaj). Nasprotno pa so širše končne razsežnosti odpornosti, kot so sistemski oziroma kaskadni učinki, v literaturi večinoma zajete zgolj posredno. Številne študije zrelost sodelovanja merijo predvsem s procesnimi kazalniki, kot so formaliziranost protokolov, režimi izmenjave informacij, pogostost vaj, prakse neprekinjenega delovanja. Zato je povezava s končnimi merami odpornosti (npr. obseg motenj, čas do obnove) pogosto posredna in metodološko manj trdna. To dodatno poglablja neenotnost sistemov kazalnikov. Soodvisnosti in kaskadni učinki so pogosto premalo sistematično zajeti, kar zmanjšuje primerljivost izidov (Yang idr., 2023; Brezavšček in Baggia, 2025).

Čeprav je raziskav, ki neposredno povezujejo zrelost JZS z merljivimi kazalniki odpornosti, malo, razpoložljivi dokazi kažejo več ponavljajočih se ugotovitev. Učinkovita odpornost kritične infrastrukture ni odvisna zgolj od tehničnih rešitev ali formalnih institucionalnih ureditev, temveč predvsem od učinkovite izmenjave informacij, medorganizacijskega sodelovanja, jasno opredeljenih vlog in odgovornosti ter usklajenega delovanja javnih in zasebnih deležnikov. Trajnejše izboljšanje odpornosti zato zahteva sočasni razvoj organizacijskih, tehnoloških in socialnih zmogljivosti, saj posamezni ukrepi sami po sebi ne zadostujejo za

učinkovito krizno odzivanje in okrevanje kritične infrastrukture (Petrenj idr., 2013).

To kaže, da raziskovalna vrzel ni več toliko v ugotavljanju pomena JZS za odpornost kritične infrastrukture, temveč predvsem v razvoju primerljivih kazalnikov, ki bi omogočili njegovo zanesljivo empirično vrednotenje.

Nekateri novejši prispevki kot dopolnilo zrelostnim pristopom predlagajo analitiko in umetno inteligenco za podporo zaznavanju, odločanju in optimizaciji odziva (npr. napredna zaznava anomalij, določanje prednostnih opozoril in avtomatizirane analize incidentov). Vendar so ti pristopi pogosto še razvojni in so omejeni z razpoložljivostjo in kakovostjo podatkov ter z zahtevami po razložljivosti in odpornosti, zato zahtevajo dodatno empirično validacijo v realnih okoljih kritične infrastrukture (Volk, 2024).

V literaturi se pogosto pojavljata poudarek na potrebi po bolj sistematični operacionalizaciji zrelosti sodelovanja ter njena empirična povezava z merljivimi izidi v konkretnih omrežjih kritične infrastrukture, pri čemer je treba posebej upoštevati medsebojne odvisnosti in kaskadne učinke.

Sodelovalno upravljanje pojasni, kako se institucionalna ureditev sodelovanja (RV1) in komunikacijsko-koordinacijske ovire pri izmenjavi informacij (RV2) medsebojno prepletajo. Sodelovalni procesi, kot so dialog, gradnja zaupanja in razvoj skupnega razumevanja, postopno vodijo do stabilnejših in zrelejših praks. Te se lahko odražajo tudi v boljših izidih odpornosti (RV3). Pri tem je zrelost sodelovanja pogojena z začetnimi pogoji (npr. začetno zaupanje in razmerja moči), institucionalno zasnovo ter ponavljajočimi se procesi skupnega učenja (Ansell in Gash, 2007).

3.6 Razporeditev tem in raziskovalne vrzeli: mehanizmi brez robustne operacionalizacije izidov

Prečna ugotovitev kartiranja je, da literatura razmeroma pogosto opisuje in obravnava mehanizme JZS, kot so: standardizirane koordinacijske prakse, izmenjava informacij, pripravljenost in kontinuiteta ter učenje in sodelovanje, bistveno redkeje pa te mehanizme poveže s primerljivimi, kvantificiranimi izidi odpornosti. S tem nastaja praznina med mehanizmi (kaj vzpostaviti) in izidi (kakšne so posledice), kar otežuje kumulativno primerjavo med študijami, sektorji in državami. Težavo dodatno poglabljajo neenotni merilni sistemi in različno interpretirane metrike z različnimi predpostavkami, npr. MTTR, zato postopkovno usmerjene presoje niso nujno vezane na operativne in merljive učinke. (Pettit idr., 2010; Torell in Avelar, 2004).

4 RAZPRAVA

4.1 Interpretacija ugotovitev: od institucionalnega okvira k operativni koordinaciji

Ugotovitve potrjujejo, da formalni institucionalni okvir predstavlja nujni pogoj za delovanje JZS, vendar sam po sebi ne zagotavlja učinkovite koordinacije v kriznih dogodkih, saj je uspešnost partnerstev odvisna od kombinacije formalnih (pogodbenih) in relacijskih upravljavskih pogojev. (Warsen idr., 2019).

Ključna razlika med formalno skladnostjo in dejansko operativno koordinacijo se pokaže tam, kjer institucionalne zahteve niso prevedene v izvedljive omrežne mehanizme, ki delujejo v realnem času (npr. stabilne kontaktne točke, jasne vloge, protokoli izmenjave informacij in pragovi eskalacije) ter omogočajo ponovljivost sodelovanja tudi pod pritiskom. V tem smislu je JZS pri kritični infrastrukturi smiselno razumeti kot omrežno upravljanje, kjer učinkovitost izhaja iz arhitekture sodelovanja in zmožnosti omrežja, da ohranja predvidljive kanale odločanja in izmenjave informacij (Warsen idr., 2019; Leitner idr., 2024).

4.2 Implikacije za energetsko in digitalno infrastrukturo v Sloveniji: kritika in izvedljive izboljšave

V Sloveniji obstaja tveganje, da se JZS pri kritični infrastrukturi udejanja predvsem skozi formalne zahteve (dokumenti, imenovanja, poročanje), medtem ko je operativna koordinacija manj sistematično razvita.

Slovenski sistem upravljanja kritične infrastrukture vključuje več medsebojno povezanih javnih in zasebnih akterjev, med drugim URSZR, Ministrstvo za obrambo, Ministrstvo za notranje zadeve, SI-CERT ter sektorsko pristojne regulatorje in upravljavce infrastrukture. Na področju energetike in digitalne infrastrukture imajo pomembno vlogo tudi deležniki, kot so ELES, SODO, Telekom Slovenije, A1 Slovenija in drugi operaterji kritičnih storitev. Takšna institucionalna in sektorska razpršenost povečuje pomen stabilnih koordinacijskih mehanizmov, standardizirane izmenjave informacij ter jasno opredeljenih operativnih vlog v kriznih razmerah (Prezelj, 2009; Ministrstvo za obrambo Republike Slovenije, 2019).

To je posebej relevantno v energetiki in digitalni infrastrukturi, kjer medsebojne odvisnosti povečujejo tveganje kaskadnih učinkov, zato so ključni pravočasni in varni mehanizmi medsektorske izmenjave informacij ter vnaprej dogovorjeni protokoli sodelovanja (Rydén Sonesson idr., 2021).

Evropski okviri v tem kontekstu ne delujejo zgolj kot regulativni pritisk, temveč kot usmeritev k operativni odpornosti: upravljanje incidentov, kontinuiteta in okrevanje ter koordinacija postanejo preverljivi elementi upravljanja (European Union, 2022b).

Na tej podlagi se kot minimalen in izvedljiv paket izboljšav izlušči kombinacija treh operativnih intervencij, ki povezuje ovire RV2 z izidi RV3: redne skupne vaje, s katerimi utrdijo vloge, komunikacijske poti in pragove eskalacije, jasno opredeljeni režimi deljenja informacij in podatkov (kaj, komu, kdaj, po kateri poti

in v katerem formatu). Vključuje tudi dogovor o izmenjavi s tretjimi deležniki in spremljanje učinkovitosti odziva z vnaprej določenimi kazalniki uspešnosti, kar omogoča primerljivost in dokazovanje izboljšav skozi čas (Nelson idr., 2025, Min in Kwak, 2025).

Ugotovitve sistematičnega pregleda kažejo, da je nadaljnji razvoj JZS v Sloveniji smiselno obravnavati tudi v primerjalnem evropskem kontekstu. To potrjuje tudi Čaleta (2025), ki poudarja, da odpornost kritične infrastrukture zaradi čezmejnih medsebojnih odvisnosti zahteva usklajeno izvajanje evropskih politik ter tesno sodelovanje med javnim in zasebnim sektorjem.

Primerjalna analiza Nemčije in Finske kaže, da dolgoročna odpornost kritične infrastrukture ni odvisna zgolj od regulatornega okvira, temveč predvsem od stopnje institucionaliziranega sodelovanja med javnimi organi, upravljavci kritične infrastrukture ter drugimi ključnimi deležniki. Nemški pristop poudarja večnivojsko upravljanje kritične infrastrukture, pri katerem so učinkovita koordinacija med zvezno državo, deželami, lokalnimi oblastmi in upravljavci infrastrukture, redna izmenjava informacij ter skupno upravljanje medsebojnih odvisnosti ključni pogoji za krepitev odpornosti, hkrati pa opozarja, da razdrobljene pristojnosti lahko zmanjšujejo učinkovitost kriznega upravljanja (Monstadt in Schmidt, 2019).

Valtonen in Branders (2020) navajata, da finski model Comprehensive Security temelji na še širšem konceptu sodelovanja, ki poleg javnih organov sistematično vključuje tudi gospodarske subjekte, nevladne organizacije in državljane. Osrednji elementi tega modela so skupno načrtovanje pripravljenosti, stalna izmenjava informacij, redne skupne vaje, jasno določene odgovornosti posameznih deležnikov ter dolgoročna izgradnja medsebojnega zaupanja, kar omogoča učinkovitejše upravljanje kompleksnih in medsebojno povezanih tveganj. V primerjavi s tema pristopoma slovenski pravni okvir z uveljavitvijo ZKI-1 ter implementacijo CER in NIS2 zagotavlja primerljive regulatorne temelje za razvoj odpornosti kritične infrastrukture. Učinkovito izvajanje teh zahtev bo odvisno predvsem od nadaljnje krepitve institucionalnih mehanizmov sodelovanja, skupnega upravljanja tveganj, redne izmenjave informacij ter razvoja medorganizacijskega zaupanja med javnim in zasebnim sektorjem.

Primerjava tako kaže, da je Slovenija normativno usklajena z evropskim regulatornim okvirom, medtem ko Finska in Nemčija večji poudarek namenjata institucionalizaciji operativnega sodelovanja, redni skupni pripravi ter trajnim koordinacijskim mehanizmom med javnim in zasebnim sektorjem. Za nadaljnji razvoj slovenskega sistema to pomeni predvsem redno izvajanje skupnih ocen tveganj, vzpostavitev trajnih mehanizmov izmenjave informacij, skupna usposabljanja, izvajanje skupnih vaj ter krepitev medsebojnega zaupanja med ključnimi deležniki. Izkušnje Finske in Nemčije zato ne predstavljajo modelov, ki bi ju bilo mogoče neposredno prenesti v slovenski prostor, temveč uporabna izhodišča in primere dobrih praks za nadaljnji razvoj slovenskega sistema odpornosti kritične infrastrukture.

Predlagane izboljšave so usmerjene predvsem v krepitev operativne koordinacije, standardizacijo komunikacijskih postopkov ter povečanje pripravljenosti organizacij za skupno odzivanje v kriznih razmerah.

Ugotovitve sistematičnega pregleda potrjujejo tudi izkušnje žledoloma leta 2014 v Sloveniji, ki je v praksi pokazal pomen učinkovite medorganizacijske koordinacije in usklajenega delovanja javnih organov ter upravljavcev kritične infrastrukture (Uprava Republike Slovenije za zaščito in reševanje, 2019).

Z vidika RV1 so se kot posebej pomembne pokazale omejitve koordinacije med različnimi organizacijami, nejasnosti pri prioritetah ponovnega priklopa ter razmeroma omejena institucionalizacija operativnih kontaktnih točk. Z vidika RV2 so bile pomembne ovire povezane z izmenjavo informacij, situacijskim pregledom nad stanjem omrežja ter usklajevanjem potreb po agregatih in drugih obnovitvenih virih med različnimi ravnmi odločanja. Takšne ugotovitve so skladne tudi z literaturo o omrežnem upravljanju in medsektorsko odpornostjo kritične infrastrukture, ki poudarja pomen jasno definiranih komunikacijskih poti, koordinacijskih struktur ter stabilnih medorganizacijskih odnosov za učinkovito odzivanje v kriznih razmerah (Provan in Kenis, 2007; Rydén Sonesson idr., 2021).

Posledice koordinacijskih omejitev so se odražale tudi v procesu obnove oskrbe, podaljšanem času ponovne vzpostavitve delovanja posameznih sistemov ter neenakomerni hitrosti okrevanja med različnimi območji in organizacijami, kar dodatno poudarja pomen operativne pripravljenosti, skupnih vaj in vnaprej dogovorjenih režimov sodelovanja za zmanjševanje trajanja motenj in izboljšanje odpornosti kritične infrastrukture (Uprava Republike Slovenije za zaščito in reševanje, 2019; Rehak idr., 2023).

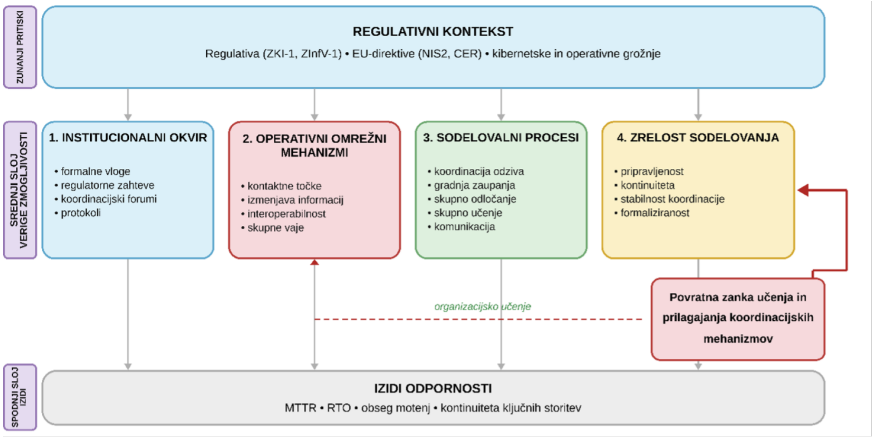
Dogodek tako potrjuje eno osrednjih ugotovitev tega pregleda: odpornost kritične infrastrukture ni odvisna zgolj od formalnih pravil in regulatornih zahtev, ampak predvsem od kakovosti operativnih omrežnih mehanizmov sodelovanja, ki omogočajo hitro usklajevanje informacij, virov in odločitev v kriznih razmerah.

Takšni izidi so vsebinsko skladni s kazalniki operativne odpornosti, kot sta MTTR in čas ponovne vzpostavitve ključnih funkcij, ki ju literatura pogosto uporablja za operacionalizacijo učinkovitosti okrevanja kritične infrastrukture (Pettit idr., 2010; Rehak idr., 2023).

4.3 Predlagani konceptualni model: od institucionalnega okvira do izidov odpornosti

Na podlagi kartiranja je mogoče oblikovati konceptualni model, ki RV1–RV3 poveže v empirično preverljivo razlagalno verigo. Model izhaja iz predpostavke, da institucionalni okvir in način omrežnega upravljanja (samoupravljanje, vodilna organizacija ali namenski administrativni organ) oblikujeta nabor operativnih omrežnih mehanizmov, kot so razmejitev vlog, standardizirani protokoli, koordinacijski forumi ter stabilne kontaktne točke, ki omogočajo ponovljivost sodelovanja tudi pod pritiskom (Provan in Kenis, 2007). Ti mehanizmi se nato udejanjajo skozi sodelovalni proces (dialog, gradnja zaupanja, razvoj skupnega razumevanja in vmesni rezultati), kar postopno vodi v stabilnejše in zrelejše prakse sodelovanja (Ansell in Gash, 2007).

Predlagani konceptualni model povezovanja institucionalnega okvira, operativnih mehanizmov sodelovanja in izidov odpornosti je prikazan na sliki 2.



Slika 2
Konceptualni model JZS in odpornosti kritične infrastrukture

Vir: lastni prikaz

Zrelost sodelovanja se kaže v kakovosti in sledljivosti deljenja informacij, sistematični izvedbi skupnih vaj ter utrjenih praksah kontinuitete in pripravljenosti, hkrati pa lahko posredno prispeva k merljivim izidom odpornosti tudi prek zmanjševanja pravnih, organizacijskih, tehničnih in kulturnih ovir, ki sicer zavirajo skupno odzivanje (Ampratwum idr., 2022).

Takšna zasnova omogoča analitično razlikovanje med razlagalnimi spremenljivkami RV1, posrednimi dimenzijami RV2 in izidi RV3, kar je metodološko uporabno za nadaljnjo empirično validacijo in primerjalne analize.

Na podlagi konceptualnega modela in ugotovitev sistematičnega kartiranja je mogoče oblikovati niz predpostavk, ki predstavljajo empirično preverljive povezave med institucionalnimi ureditvami, operativnimi mehanizmi sodelovanja ter izidi odpornosti kritične infrastrukture. Predpostavke predstavljajo izhodišče za nadaljnjo Delphi validacijo in empirično testiranje modela.

4.3.1 Predpostavke za empirično validacijo modela

Na podlagi konceptualnega modela in ugotovitev sistematičnega kartiranja je mogoče oblikovati niz predpostavk, ki predstavljajo empirično preverljive povezave med institucionalnimi ureditvami, operativnimi mehanizmi sodelovanja ter izidi odpornosti kritične infrastrukture. Predlagane predpostavke (P1–P5) omogočajo strukturirano zasnovo Delphi vprašalnika ter kasnejše empirično preverjanje povezav med omrežnimi mehanizmi sodelovanja in merljivimi izidi odpornosti:

- P1: Višja raven stabilnosti kontaktnih točk, formaliziranosti protokolov izmenjave informacij in izvajanja skupnih vaj je pozitivno povezana s krajšim časom obnove delovanja pri kriznih dogodkih in kaskadnih incidentih (Rydén Sonesson idr., 2021; Nelson idr., 2025).
- P2: Višja raven formaliziranosti institucionalnih okvirov je pozitivno povezana z učinkovitostjo krizne koordinacije, pri čemer je povezava posredovana prek operativnih omrežnih mehanizmov, kot so

koordinacijski forumi, standardizirane komunikacijske poti in vnaprej določeni pragovi eskalacije. Pričakuje se, da bo povezava šibkejša v odsotnosti operativnih mehanizmov sodelovanja med akterji (Provan in Kenis, 2007; Ansell in Gash, 2007).

- P3: Večja stopnja medorganizacijskega zaupanja in intenzivnosti izmenjave informacij med javnimi in zasebnimi deležniki je pozitivno povezana z učinkovitejšo koordinacijo odziva ter večjo operativno odpornostjo v kriznih razmerah (Sienkiewicz-Małyjurek in Owczarek, 2020; Rydén Sonesson idr., 2021).
- P4: Večja stopnja interoperabilnosti in standardizacije podatkovnih ter komunikacijskih postopkov je pozitivno povezana s hitrejšo izmenjavo informacij in učinkovitejšim medsektorskim usklajevanjem pri incidentih kritične infrastrukture (Sellitto idr., 2021; Leitner idr., 2024).
- P5: Višja raven razvitosti praks kontinuitete poslovanja, skupnega učenja in rednih medorganizacijskih vaj je pozitivno povezana z višjo ravnjo operativne odpornosti ter manjšim obsegom motenj ob kriznih dogodkih (Pettit idr., 2010; Rehak idr., 2023).

4.4 Operacionalizacija in načrt empirične validacije: instrument, izidi, SNA in Delphi

Za slovenski kontekst se zato kaže smiselna raziskovalna agenda, ki združuje razvoj merskega instrumenta za ključne dimenzije sodelovanja, sistematično zbiranje končnih kazalnikov odpornosti (MTTR, RTO, obseg motenj …), omrežno analizo (SNA) za opis strukture, centralnosti, vlog in pozicij akterjev v koordinaciji. Vključuje tudi Delphi validacijo instrumenta, vključno s presojo vsebinske veljavnosti in po potrebi uravnavanjem dimenzij, kar je posebej relevantno zaradi omejitev majhnega vzorca kritičnih subjektov (Linstone in Turoff, 2002; Prell, 2012).

Priporočljivo je, da se instrument in kazalniki najprej validirajo (Delphi) in nato pilotno testirajo pri izbranih organizacijah, preden se razširijo na celoten sektor. Za empirično testiranje predlaganega modela je smiselna kombinacija metod in podatkovnih virov:

1. Potreben je merski instrument (vprašalnik) za dimenzije sodelovanja in zrelosti (upravljanje, deljenje informacij, vaje, kontinuiteta).
2. Zbirati je treba podatke o izidih (npr. časi incidentov, doseganje RTO, trajanje okrevanja, obseg motenj).
3. Pri operacionalizaciji izidov okrevanja literatura pogosto uporablja časovne kazalnike na ravni sistemov, kot sta RTO in MTTR. RTO opredeljuje največji še dopusten čas nedosegljivosti storitve, medtem ko MTTR označuje povprečni realizirani čas, potreben za vzpostavitev normalnega delovanja na podlagi več dogodkov v opazovanem obdobju. Razlikovanje med ciljno mejo (RTO) in dejansko doseženim povprečjem (MTTR) omogoča natančnejše spremljanje učinkovitosti ukrepov in koordinacije. Kadar MTTR vztrajno presega določeni RTO, je to mogoče interpretirati kot kazalnik neskladja med načrtovanimi cilji in dejanskimi

obnovitvenimi zmogljivostmi ter kot podlago za prilagoditev zaščitnih mehanizmov, virov ali postopkov (Storage Networking Industry Association, 2025).
4. Omrežna analiza (SNA) omogoča opis strukture omrežja in vlog (npr. centralnost, gostota, posredništvo) (Prell, 2012).
5. Zaradi majhnega števila kritičnih subjektov v Sloveniji je smiselna Delphi validacija kazalnikov pred pilotnim merjenjem (Linstone in Turoff, 2002).

Podporne tehnologije (npr. analitika ali orodja na osnovi umetne inteligence) so lahko smiselno dopolnilo, vendar le ob jasnih pravilih uporabe, urejenih podatkovnih tokovih in opredeljenih odgovornostih, sicer lahko povečajo kompleksnost brez izboljšanja merljivih izidov (Volk, 2024).

5 ZAKLJUČEK

Sistematični pregled literature za obdobje 2018–2025 kaže, da JZS predstavlja pomemben dejavnik varnosti in odpornosti kritične infrastrukture. Formalni institucionalni okvirji sami po sebi ne zagotavljajo učinkovite koordinacije, temveč jih morajo dopolnjevati operativni mehanizmi sodelovanja, kot so jasno opredeljene vloge, stalne kontaktne točke, dogovorjeni režimi izmenjave informacij ter redne skupne vaje (Ansell in Gash, 2007; Provan in Kenis, 2007). Hkrati pregled potrjuje, da ostaja ena ključnih raziskovalnih vrzeli pomanjkanje študij, ki bi zrelost JZS sistematično povezovale z merljivimi izidi odpornosti (Pettit idr., 2010; Torell in Avelar, 2004).

Za slovenski prostor ugotovitve podpirajo razvoj institucionaliziranega JZS, ki presega formalno izpolnjevanje regulatornih zahtev in temelji na trajni medorganizacijski koordinaciji. To vključuje vzpostavitev ponovljivih operativnih mehanizmov sodelovanja ter uporabo skupnih procesnih in končnih kazalnikov, ki omogočajo spremljanje učinkovitosti odzivanja in okrevanja kritičnih subjektov (Lewis in Petit, 2019; European Union, 2022a, 2022b).

Osrednji prispevek članka je sistematično kartiranje in tematska sinteza literature ter oblikovanje konceptualnega modela, ki povezuje institucionalne ureditve, operativne mehanizme sodelovanja, zrelost JZS in izide odpornosti. Model predstavlja podlago za empirično preverjanje razmerij med kakovostjo sodelovanja in merljivimi kazalniki odpornosti ter prispeva k zapolnjevanju vrzeli med normativnimi priporočili in njihovim empiričnim vrednotenjem (Provan in Kenis, 2007; Pettit idr., 2010).

Na tej podlagi članek predlaga nadaljnji razvoj empiričnega modela za slovensko okolje, ki vključuje kombinacijo procesnih kazalnikov sodelovanja (npr. jasnost vlog, režimi izmenjave informacij, kontaktne točke in skupne vaje) ter končnih kazalnikov odpornosti (npr. MTTR, RTO in obseg motenj). Takšen pristop omogoča primerljivo spremljanje razvoja JZS skozi čas ter predstavlja uporabno podlago za nadaljnje raziskave in podporo upravljavskim odločitvam pri krepitvi odpornosti kritične infrastrukture (Russo idr., 2025; Aguilar, 2023).

LITERATURA

Aguilar, A. I. (2023). Lowering mean time to recovery (MTTR) in responding to system downtime or outages: An application of lean six sigma methodology. In *13th Annual International Conference on Industrial Engineering and Operations Management, Manila, Philippines*. https://doi.org/10.46254/AN13.20230039

Ampratwum, G., Osei-Kyei, R. in Tam, V. W. Y. (2022). Exploring the concept of public-private partnership in building critical infrastructure resilience against unexpected events: A systematic review. *International Journal of Critical Infrastructure Protection, 39*, Article 100556. https://doi.org/10.1016/j.ijcip.2022.100556

Ansell, C. in Gash, A. (2007). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571. https://doi.org/10.1093/jopart/mum032

Borysiak, O., Brych, V., Manzhula, V., Lechowicz, T., Dluhopolska, T. in Putsenteilo, P. (2025). Synergy of energy-efficient and low-carbon management of the logistics chains within developing distributed generation of electric power: The EU evidence for Ukraine. *Energies*, *18*(20), Article 5512. https://doi.org/10.3390/en18205512

Börzel, T. A. in Heard-Lauréote, K. (2009). Networks in EU multi-level governance: Concepts and contributions. *Journal of Public Policy*, *29*(2), 135–151. https://doi.org/10.1017/S0143814X09001044

Brezavšček, A. in Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems*, *13*(1), Article 52. https://doi.org/10.3390/systems13010052

Čaleta, D. in Rolih, G. (2011). Kibernetska varnost v družbi in delovanje kritične infrastrukture – analiza stanja na obrambnem področju v Republiki Sloveniji. *Sodobni vojaški izzivi*, *13*(3), 4–20. https://doi.org/10.33179/BSV.99.SVI.11.CMC.13.3.3

Čaleta, D. (2025). International dimension of critical infrastructure resilience: Challenges of the Mediterranean security environment. *International Journal of Euro-Mediterranean Studies, 18*(2), 177–205. https://doi.org/10.70908/2232-6022/18.177-205

Department of Homeland Security. (2013). *NIPP 2013: Partnering for critical infrastructure security and resilience*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf

European Bank for Reconstruction and Development. (2024). *Slovenia Country Strategy 2024–2029*. https://www.ebrd.com/content/dam/ebrd_dxp/assets/pdfs/country-strategies/slovenia/EBRD-Latest-Slovenia-Strategy.pdf

European Union. (2022a). *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*. *Official Journal of the European Union, L333*, 164–198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

European Union. (2022b). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L333*, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Ferrari, M. (2020). Reflexive governance for infrastructure resilience and sustainability. *Sustainability, 12*(23), Article 10224. https://doi.org/10.3390/su122310224

Gharaee, H., Dewey, R. S., Gholami, A. H. in Azami-Aghdash, S. (2023). Developing a public-private partnership framework for managing the adverse health effects of environmental disaster (a case study of Lake Urmia – Iran). *Journal of Water and Health*, *21*(2), 251–260. https://doi.org/10.2166/wh.2023.239

Giacomello, G. (2021). A perfect storm: Privatization, public–private partnership and the security of critical infrastructure. V G. Giacomello, F. N. Moro in M. Valigi (ur.), *Technology and International Relations* (pp. 173–192). Edward Elgar Publishing. https://doi.org/10.4337/9781788976077.00017

Gioia, D. A., Corley, K. G. in Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15–31. https://doi.org/10.1177/1094428112452151

James, K. L., Randall, N. P. in Haddaway, N. R. (2016). A methodology for systematic mapping in environmental sciences. *Environmental Evidence, 5*, Article 7. https://doi.org/10.1186/s13750-016-0059-6

Leitner, M., Skopik, F. in Pahi, T. (2024). Operational cyber incident coordination revisited: Providing cyber situational awareness across organizations and countries. *Information Security Journal: A Global Perspective, 33*(5), 486–507. https://doi.org/10.1080/19393555.2024.2334787

Lewis, D. in Petit, F. (2019). *Critical infrastructure interdependency analysis: Operationalising resilience strategies*. United Nations Office for Disaster Risk Reduction. https://www.undrr.org/publication/critical-infrastructure-interdependency-analysis-operationalising-resilience-strategies

Lichte, D., Torres, F. S. in Engler, E. (2022). Framework for operational resilience management of critical infrastructures and organizations. *Infrastructures, 7*(5), Article 70. https://doi.org/10.3390/infrastructures7050070

Linstone, H. A. in Turoff, M. (ur.). (2002). *The delphi method: Techniques and applications*. New Jersey Institute of Technology. https://www.foresight.pl/assets/downloads/publications/Turoff_Linstone.pdf

McHugh, M. L. (2012). Interrater reliability: The kappa statistic. *Biochemia Medica*, *22*(3), 276–282. https://doi.org/10.11613/bm.2012.031

Min, C.-H. in Kwak, J. (2025). RMF-A: An availability assurance framework for quantitative evaluation of operational resilience. *Electronics*, *14*(23), Article 4644. https://doi.org/10.3390/electronics14234644

Ministrstvo za obrambo Republike Slovenije. (2019). *Kritična infrastruktura v Republiki Sloveniji*. https://www.gov.si/assets/ministrstva/MO/Publikacije/Kriticna-infrastruktura-v-Republiki-Sloveniji.pdf

Monstadt, J. in Schmidt, M. (2019). Urban resilience in the making? The governance of critical infrastructures in German cities. *Urban Studies, 56*(11), 2353–2371. https://doi.org/10.1177/0042098018808483

Nelson, A., Rekhi, S., Souppaya, M. in Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P. In Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, Article n71. https://doi.org/10.1136/bmj.n71

Petersen, K., Feldt, R., Mujtaba, S. in Mattsson, M. (2008). Systematic mapping studies in software engineering. V *12th International Conference on Evaluation and Assessment in Software Engineering (EASE 2008).* https://doi.org/10.14236/ewic/EASE2008.8

Petrenj, B., Lettieri, E. in Trucco, P. (2013). Information sharing and collaboration for critical infrastructure resilience: A comprehensive review on barriers and emerging capabilities. *International Journal of Critical Infrastructures, 9*(4), 304–329. https://doi.org/10.1504/IJCIS.2013.058171

Pettit, T. J., Fiksel, J. in Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics, 31*(1), 1–21. https://doi.org/10.1002/j.2158-1592.2010.tb00125.x

Pinto, A. J., Borgeaud Dit Avocat, A., Lulcheva, E. In Dietrich, P. (2021). *Public-Private partnerships: Preventing cyberattacks on critical infrastructure in the OSCE region*. FES Regional office for cooperation and peace in Europe. https://cdn.osce.org/sites/default/files/f/documents/6/0/506930.pdf

Prezelj, I., Kopač, E., Svete, U. in Žiberna, A. (2012). Cross-sectoral scanning of critical infrastructures: From functional differences to policy-relevant similarities. *Journal of Homeland Security and Emergency Management, 9*(1), Article 19. https://doi.org/10.1515/1547-7355.1901

Prell, C. (2012). *Social network analysis: History, theory and methodology*. Sage Publications.

Provan, K. G. in Kenis, P. (2007). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, *18*(2), 229–252. https://doi.org/10.1093/jopart/mum015

Rehak, D., Flynnova, L., Hromada, M. in Fuggini, C. (2023). The importance of resistance in the context of critical infrastructure resilience: An extension of the CIERA method. *Systems*, *11*(10), Article 506. https://doi.org/10.3390/systems11100506

Russo, N., São Mamede, H. in Reis, L. (2025). An approach to business continuity self-assessment. *Technologies*, *13*(6), Article 242. https://doi.org/10.3390/technologies13060242

Rydén Sonesson, T., Johansson, J. in Cedergren, A. (2021). Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Safety Science*, *142*, Article 105383. https://doi.org/10.1016/j.ssci.2021.105383

Sellitto, G. P., Masi, M., Pavleska, T. in Aranha, H. (2021). A cyber security digital twin for critical infrastructure protection: The intelligent transport system use case. V E. Serral, J. Stirna, J. Ralyté in J. Grabis (ur.), *The Practice of Enterprise Modeling* (str. 230–244). Springer International Publishing. https://doi.org/10.1007/978-3-030-91279-6_16

SI-CERT. (2025). *Poročilo o kibernetski varnosti za leto 2024*. https://www.cert.si/letna_porocila/porocilo-o-kibernetski-varnosti-za-leto-2024/

Sienkiewicz-Małyjurek, K. in Owczarek, T. (2020). Complementarity of communication and coordination in ensuring effectiveness of emergency management networks. *Sustainability, 13*(1), Article 221. https://doi.org/10.3390/su13010221

SODO. (2023). *Razvojni načrt distribucijskega sistema električne energije 2023–2032*. https://sodo.si/sl/objave/razvojni-nacrt-distribucijskega-sistema-elektricne-energije-od-leta-2023-do-leta-2032

Storage Networking Industry Association. (2025). *Data protection best practices (Version 2.0)*. https://www.snia.org/educational-library/data-protection-best-practices-2025-0

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D. in Lynes, D. (2010). *Contingency planning guide for federal information systems* (NIST Special Publication 800-34 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-34r1

Thomas, J. in Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. BMC *Medical Research Methodology, 8*, Article 45. https://doi.org/10.1186/1471-2288-8-45

Torell, W. in Avelar, V. (2004). *Mean time between failure: Explanation and standards* (White Paper No. 78, Rev. 1). APC by Schneider Electric. https://www.researchgate.net/publication/251895269_Mean_Time_Between_Failure_Explanation_and_Standards

Uprava Republike Slovenije za zaščito in reševanje. (2019). *Razvojno raziskovalni projekt oblikovanja modela vodenja odziva na nesreče*. https://www.gov.si/zbirke/projekti-in-programi/razvojno-raziskovalni-projekt-oblikovanje-celovitega-modela-vodenja-odziva-na-nesrece-za-vse-ravni-vodenja-na-podrocju-zascite-resevanja-in-pomoci-v-republiki-sloveniji/

Uredba o ugotavljanju kritičnih subjektov. (2025). *Uradni list RS*, (42/25).

Valtonen, V. in Branders, M. (2020). Tracing the Finnish Comprehensive Security Model. V S. Larsson in M. Rhinard (ur.), *Nordic Societal Security: Convergence and Divergence* (str. 91–108). Routledge. https://doi.org/10.4324/9781003045533

Volk, M. (2024). A safer future: Leveraging the AI power to improve cybersecurity in critical infrastructures. *Elektrotehniški vestnik, 91*(3), 73–94. https://ev.fe.uni-lj.si/3-2024/Volk.pdf

Warsen, R., Greve, C., Klijn, E. H., Koppenjan, J. F. M. in Siemiatycki, M. (2020). How do professionals perceive the governance of public–private partnerships? Evidence from Canada, the Netherlands and Denmark. *Public Administration*, *98*(1), 124–139. https://doi.org/10.1111/padm.12626

Wegner, D., Teixeira, E. K. in Verschoore, J. R. (2019). "Modes of Network Governance": What advances have been made so far? *Base - Revista de Administração e Contabilidade da Unisinos*, *16*(1), 2–26. https://doi.org/10.4013/base.2019.161.01

Yang, Z., Barroca, B., Weppe, A., Bony-Dandrieux, A., Laffréchine, K., Daclin, N., November, V., Omrane, K., Kamissoko, D., Benaben, F., Dolidon, H., Tixier, J. in Chapurlat, V. (2023). Indicator-based resilience assessment for critical infrastructures – A review. *Safety Science*, *160*, Article 106049. https://doi.org/10.1016/j.ssci.2022.106049

Zakon o kritični infrastrukturi (ZKI-1). (2024). *Uradni list RS*, (102/24).

Zakon o informacijski varnosti (ZInfV-1). (2025). *Uradni list RS*, (40/25).

O avtorjih:

Matevž Lipovšek, doktorski študent, Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija. E-pošta: matevz.lipovsek@student.um.si

Prof. dr. Branko Lobnikar, redni profesor za varnostne vede, Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija. E-pošta: branko.lobnikar@um.si