
Konceptualni upravljavski model odpornosti kritične infrastrukture in verižnih učinkov: model CIRG

VARSTVOSLOVJE
leto 2026
letn. 28
str. 1–23

Matevž Lipovšek, Miha Dvojmoč

Namen prispevka:

Razviti konceptualni upravljavski model odpornosti kritične infrastrukture (angl. *Critical Infrastructure Resilience Governance* (CIRG)), ki povezuje razumevanje medsektorskih odvisnosti in verižnih učinkov z organizacijskim odločanjem, koordinacijo odziva ter upravljanjem obnove v kompleksnih kriznih razmerah.

Metode:

Prispevek je zasnovan kot konceptualni članek tipa teorije-sinteze. Temelji na strukturirani analitični sintezi literature s področij kritične infrastrukture, organizacijske odpornosti, kriznega upravljanja in medsektorskih odvisnosti. Literatura je bila identificirana v podatkovnih bazah Scopus in Web of Science ter analizirana s primerjalno konceptualno analizo.

Ugotovitve:

Razvit je model CIRG, ki odpornost obravnava kot večnivojski proces zaznavanja kritičnih odvisnosti, razvoja scenarijev verižnih učinkov, upravljanja odziva in koordinacije obnove. Model vključuje tudi odločitvene sprožilce in učno zanko, ki omogočajo prehod med robustnim in odpornim načinom delovanja.

Omejitve/uporabnost raziskave:

Model je konceptualen in še ni empirično preverjen. Nadaljnje raziskave naj razvijejo operativne kazalnike ter model validirajo v različnih sektorjih kritične infrastrukture.

Praktična uporabnost:

Model podpira učinkovitejše odločanje, koordinacijo odziva in upravljanje obnove ob verižnih učinkih.

Izvirnost/pomembnost prispevka:

Prispevek predstavlja izviren integrativni upravljavski okvir, ki povezuje sistemska tveganja z organizacijskimi mehanizmi kriznega upravljanja. Ugotovitve so namenjene raziskovalcem, upravljavcem kritične infrastrukture,

regulatorjem in drugim deležnikom, ki razvijajo sisteme organizacijske odpornosti.

Ključne besede: kritična infrastruktura, odpornost, robustnost, verižni učinki, medsektorske odvisnosti, krizno upravljanje

UDK: 005.334

CIRG: A Conceptual Governance Model for Resilience and Cascading Effects in Critical Infrastructure

Purpose:

The purpose of the paper is to develop a conceptual Critical Infrastructure Resilience Governance (CIRG) model linking interdependencies and cascading effects with organizational decision-making, response coordination, and recovery management during complex crises.

Design/Methods/Approach:

The paper is a conceptual theory-synthesis study based on a structured analytical review of literature on critical infrastructure, organizational resilience, crisis management, and interdependencies. Literature was identified through the Scopus and Web of Science databases and analyzed using comparative conceptual analysis.

Findings:

The CIRG model conceptualizes resilience as a multi-level governance process comprising identification of critical interdependencies, cascading-effect scenario development, response governance, and recovery coordination. The model also incorporates decision triggers and a learning loop that enable transitions between robustness-oriented and resilience-oriented modes of operation.

Research Limitations/Implications:

The model is conceptual and has not yet been empirically validated. Future research should develop operational indicators and test the model across different critical infrastructure sectors.

Practical Implications:

The model provides a governance framework for improving organizational decision-making, response coordination, and recovery management during cascading disruptions.

Originality/Value:

The paper proposes an original integrative governance framework linking systemic risk analysis with organizational crisis management mechanisms. The model provides value for researchers, critical infrastructure operators, policymakers, and practitioners involved in resilience governance.

Keywords: critical infrastructure, resilience, robustness, cascading effects, interdependencies, crisis management

UDC: 005.334

1 UVOD

Sodobna kritična infrastruktura deluje v pogojih visoke kompleksnosti, medsektorske odvisnosti in kibernetsko-fizične prepletenosti. Varnosti zato ni več mogoče razumeti zgolj kot zaščito posameznih sistemov, ampak kot sposobnost organizacij za ohranjanje delovanja in prilagajanje v pogojih sistemske negotovosti (Duchek, 2020; National Institute of Standards and Technology, 2024).

Motnje se lahko širijo s funkcionalnimi, informacijskimi in logističnimi povezavami ter povzročajo verižne učinke s širšimi družbenimi in gospodarskimi posledicami (Pescaroli in Alexander, 2016). Takšne razmere zahtevajo modele, ki analitično razumevanje medsektorskih odvisnosti pretvarjajo v pravočasno krizno ukrepanje, usklajevanje odzivnih mehanizmov in ponovno vzpostavitev sistema (Rydén Sonesson idr., 2021). Predlagani model pri tem odpornost razume kot upravljavski prehod med rutinskim operativnim delovanjem in kriznim načinom odziva glede na stopnjo sistemske prizadetosti (Boin idr., 2017).

V tem kontekstu razumemo upravljanje (angl. *governance*) kot sistem struktur, procesov in mehanizmov, ki usmerjajo odločanje, koordinacijo ter delitev odgovornosti med deležniki v pogojih kompleksnosti in negotovosti (Rhodes, 1996; Meuleman, 2010). Pri odpornosti kritične infrastrukture upravljanje presega zgolj tehnično zaščito sistemov in vključuje tudi večnivojsko usklajevanje, krizno odločanje in sodelovanje med organizacijami. Namen prispevka je razviti konceptualni okvir – CIRG (angl. *Critical Infrastructure Resilience Governance Framework*), ki povezuje analizo medsektorskih odvisnosti z organizacijskimi mehanizmi kriznega odzivanja, koordinacije med deležniki in ponovne vzpostavitve sistema (Boin idr., 2017; Rydén Sonesson idr., 2021).

2 OPREDELITEV PROBLEMA

Kljub intenzivnemu razvoju raziskav na področju kritične infrastrukture ostaja velika raziskovalna vrzel med analitičnim razumevanjem medsektorskih odvisnosti in širjenja motenj ter njihovo praktično uporabo pri odločanju, usklajevanju odziva in obnovi sistema (Rydén Sonesson idr., 2021; Gordan idr., 2024). Obstoječi pristopi se večinoma osredotočajo na tehnično modeliranje sistemskih povezav in širjenja motenj, medtem ko mehanizmi eskalacije, medorganizacijskega usklajevanja in kriznega odločanja ostajajo manj razviti (Marquez-Tejon idr., 2023; Smith in Shashkina, 2023). Poseben problem predstavlja odsotnost jasno operacionaliziranih mehanizmov, ki bi organizacijam omogočili strukturiran prehod med operativnim odzivanjem in širšim kriznim upravljanjem v pogojih stopnjevanja verižnih učinkov (Boin idr., 2017).

Osrednji problem prispevka je odsotnost integrativnega upravljavskega modela, ki bi sistematično povezoval analitično razumevanje medsektorskih odvisnosti in verižnih učinkov, koncepte robustnosti in odpornosti ter krizno odločanje, odzivne mehanizme in usklajevanje obnovitvenih procesov. Obstoječa literatura kaže, da kompleksne krizne situacije pogosto spremljajo informacijska dvoumnost, organizacijski konflikti in zamude pri odločanju. S tem se dodatno povečuje tveganje širjenja verižnih učinkov (Myers in Sutcliffe, 2022).

Iz opredeljene raziskovalne vrzeli izhajajo naslednja raziskovalna vprašanja, ki usmerjajo razvoj konceptualnega modela CIRG:

- RV1: Kako lahko organizacije kritične infrastrukture analitično zaznavo medsektorskih odvisnosti pretvorijo v učinkovito organizacijsko odločanje?
- RV2: Kako lahko formalizirani odločitveni sprožilci izboljšajo pravočasnost eskalacije kriznega odziva?
- RV3: Kako lahko integrirani upravljavski model izboljša koordinacijo odziva in usklajevanje ponovne vzpostavitve v pogojih kompleksnih verižnih učinkov?

3 PREGLED LITERATURE IN TEORETIČNI OKVIR

Pregled literature temelji predvsem na znanstvenih objavah iz obdobja 2015–2025, indeksiranih v podatkovnih bazah Web of Science in Scopus. Analiza literature je bila izvedena kot strukturirana konceptualna sinteza, usmerjena v identifikacijo in povezovanje ključnih konceptov s področij kritične infrastrukture, verižnih učinkov, organizacijske odpornosti, robustnosti sistemov ter kriznega upravljanja (Jaakkola, 2020).

Obravnavani problem je izrazito interdisciplinaren. Verižni učinki v kritični infrastrukturi namreč presegajo tehnično raven in vključujejo organizacijske, logistične, komunikacijske ter regulativne razsežnosti. Prispevek zato povezuje literaturo s področij kritične infrastrukture, organizacijske odpornosti, korporativne varnosti, kriznega upravljanja, kibernetско-fizične varnosti in upravljaljskih mehanizmov.

3.1 Odpornost in robustnost

Robustnost in odpornost predstavljata dva komplementarna, vendar konceptualno različna pristopa k zagotavljanju stabilnosti kritične infrastrukture. Robustnost se nanaša predvsem na sposobnost sistema, da ohrani svojo funkcionalnost ob motnji ali incidentu brez bistvenih sprememb strukture ali delovanja. V kontekstu kritične infrastrukture robustnost pomeni sposobnost absorpcije začetnega šoka ter zmanjševanja neposrednih funkcionalnih izgub (Hosseini idr., 2016).

Odpornost presega zgolj ohranjanje funkcionalnosti in vključuje sposobnost prilagoditve, reorganizacije, obnove in učenja po motnji. Sodobni pristopi upravljanja kritične infrastrukture poudarjajo potrebo po integraciji robustnosti in odpornosti v enoten upravljavski okvir. V kompleksnih medsektorsko povezanih sistemih pristopi, ki temeljijo zgolj na robustnosti, pogosto ne zadostujejo, ker ne obravnavajo zadostno organizacijskega prilagajanja, koordinacije deležnikov in kriznega odločanja v pogojih širjenja verižnih učinkov. Inženiring odpornosti, kot navajata avtorja, pa predvsem izpostavlja sposobnost prilagoditve delovanja sistema v pogojih motenj, vendar manj sistematično obravnava upravljaljske mehanizme organizacijske eskalacije, razdelitve pristojnosti in medorganizacijske koordinacije v kritični infrastrukturi (Madni in Jackson, 2009).

3.2 Medsektorske odvisnosti

Kritično infrastrukturo zaznamujejo gosto prepletene funkcionalne in tehnične povezave. Zato lahko incident v enem delu sistema sproži posledice v drugih podsistemih, še posebej takrat, kadar so informacijski in operativni procesi tesno povezani. To je posebej pomembno v okoljih operativnih tehnologij, kjer imajo motnje lahko neposredne tehnične posledice. Kritične infrastrukture zato ni mogoče razumeti kot skupek ločenih enot, temveč kot medsebojno odvisen sistem. Odvisnosti med sektorji omogočajo širjenje motenj prek fizičnih, kibernetskih in organizacijskih povezav. Rinaldijeva tipologija medsektorskih odvisnosti omogoča bolj sistematično analizo poti širjenja motenj ter boljše razumevanje, na katerih ravneh lahko pride do veržnih učinkov (Rinaldi idr., 2001; Stouffer idr., 2023).

Novejši pristopi Rinaldijevo tipologijo nadgrajujejo z operativno usmerjenim modeliranjem odvisnosti. Jovanović idr. (2021a) predlagajo kombinacijo klasičnega matričnega modeliranja odvisnosti (dopolnjenega s scenarijsko-časovno komponento) in indikatorskega pristopa pri katerem vrednosti kazalnikov izhajajo iz ekspertnih ocen, meritev in obsežnih podatkovnih virov. Takšen pristop omogoča spremljanje ravni odpornosti celotne skupine infrastruktur (npr.: v industrijski coni, mestu ali regiji) in ne zgolj posameznega sistema. Metodologija je bila preizkušena tudi na primeru pristaniške infrastrukture, kjer je bil skozi časovno zaporedje dogodkov od zaznave grožnje do zaključka sanacije prikazan razvoj medsebojnih odvisnosti med sredstvi kritične infrastrukture. V okviru modela CIRG lahko takšno dinamično obravnavo odvisnosti razumemo kot analitično podlago za določanje pragov odločitvenih sprožilcev.

Model PRECINCT (Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyberphysical Threats) predstavlja enega pomembnejših sodobnih pristopov k simulacijskemu modeliranju veržnih učinkov v kritični infrastrukturi. Omogoča analizo širjenja motenj med medsebojno povezanimi sistemi (Gordan idr., 2024). Kljub visoki analitični vrednosti ostajajo takšni pristopi usmerjeni predvsem v tehnično in simulacijsko razumevanje sistemskih povezav. Mehanizmi kriznega odločanja, aktivacije odziva in medsebojnega usklajevanja so v teh modelih praviloma obravnavani omejeno ali implicitno.

Podobno usmeritev je mogoče prepoznati tudi v novejših evropskih pobudah za ocenjevanje tveganj med sektorji. Gerbec idr. (2025) so v okviru projekta ATLANTIS razvili metodologijo ocenjevanja tveganj, ki eksplicitno upošteva odvisnosti med kritičnimi infrastrukturami ter ocenjuje verjetnosti in posledice motenj na medsektorski in čezmejni ravni. Metodologija je bila preverjena v treh obsežnih pilotnih izvedbah, rezultati pa kažejo izboljšanje pripravljenosti in ozaveščenosti deležnikov za približno 5–55 %, odvisno od scenarija in skupine udeležencev. Avtorji hkrati opozarjajo, da preizkusi zaradi varnostnih omejitev niso temeljili na dejanskih operativnih podatkih, temveč na sintetičnih podatkih. Krepitev pripravljenosti je dolgoročen proces, ki zahteva sistemske in kulturne spremembe v organizacijah. Ta ugotovitev predstavlja eno ključnih konceptualnih izhodišč razvoja modela CIRG, ki poleg sistemskih odvisnosti vključuje tudi organizacijsko pripravljenost, odločanje in koordinacijo odziva.

3.3 Upravljanje odpornosti v kritični infrastrukturi

V tem prispevku razumemo odpornost kritične infrastrukture kot sistem struktur, procesov in mehanizmov, ki usmerjajo odločanje, koordinacijo in delitev odgovornosti med različnimi akterji v razmerah visoke kompleksnosti in negotovosti (Rhodes, 1996; Meuleman, 2010).

V kritični infrastrukturi postaja varnost del širšega upravljanja tveganj, odločanja in organizacijskega odzivanja. Uspešnost obvladovanja motenj je vse bolj odvisna od medorganizacijskega sodelovanja, izmenjave informacij in koordinacije deležnikov v pogojih kompleksnih medsektorskih motenj. Zato je pomembno vprašanje, kako organizacije organizirajo aktivacijo kriznega odziva, razdelitev odgovornosti ter prehod med posameznimi ravni odločanja. Ključni organizacijski sposobnosti sta pravočasna eskalacija kriznega odziva in učinkovito usklajevanje odločanja med operativno, taktično in strateško ravno. Takšen pristop temelji na večnivojski koordinaciji med ključnimi deležniki kritične infrastrukture (Boin idr., 2017; Rydén Sonesson idr., 2021).

Kljub temu številne organizacije obravnavajo varnost razdrobljeno. Varnostne funkcije so pogosto organizirane v ločenih enotah z omejenim medfunkcijskim sodelovanjem. Takšna fragmentacija zmanjšuje celovit pregled nad medsektorskimi odvisnostmi in bistveno otežuje usklajeno odločanje v kompleksnih kriznih situacijah (Marquez-Tejon idr., 2023).

Upravljanje odpornosti kritične infrastrukture dodatno oblikujejo tudi sodobni evropski regulatorni pristopi, ki poudarjajo celostno odpornost, medsektorsko koordinacijo ter upravljanje sistemskih tveganj. V zadnjih letih je Evropska unija okrepila regulativni okvir na področju odpornosti kritične infrastrukture, predvsem zaradi povečane kompleksnosti kibernetских groženj ter vse večje medsektorske povezanosti kritične infrastrukture. Poseben poudarek je namenjen pravočasni zaznavi motenj, koordiniranemu odzivanju, zagotavljanju kontinuitete delovanja in učinkovitemu ponovnemu vzpostavljanju kritičnih funkcij.

Pomemben del evropskega regulatornega okvira predstavlja Direktiva CER (Directive on the Resilience of Critical Entities – Direktiva (EU) 2022/2557) o odpornosti kritičnih subjektov. Direktiva poudarja obveznosti držav članic in kritičnih subjektov glede izvajanja ocen tveganj, zaščite kritičnih funkcij, zagotavljanja organizacijske odpornosti ter krepitve pripravljenosti na kompleksne motnje in krizne situacije. Pomembno dopolnitev predstavlja tudi Direktiva NIS2 (Network and Information Security Directive 2 – Direktiva (EU) 2022/2555) o ukrepih za visoko skupno raven kibernetiske varnosti v Evropski uniji. Direktiva NIS2 uvaja strožje zahteve glede upravljanja kibernetских tveganj, poročanja incidentov, kriznega upravljanja ter odgovornosti vodstvenih struktur organizacij kritične infrastrukture (European Union, 2022a; 2022b).

Poleg zahtev znotraj posameznih držav članic postaja vse pomembnejša tudi mednarodna oziroma čezmejna razsežnost odpornosti kritične infrastrukture. Čaleta (2025) na primeru sredozemskega varnostnega okolja opozarja, da so infrastrukturni sistemi izpostavljeni sočasnemu delovanju več vrst groženj, ki preizkušajo tako robustnost kot prilagodljivost infrastrukture in presegajo zmožnosti posamezne države ali operatorja. Avtor v tem okviru opredeli tudi

upravljavsko dilemo: evropske direktive sicer poenotijo pristope, njihovo izvajanje pa poteka v okviru nacionalne zakonodaje in lokalnih praks. S tem se ustvarja napetost med nadnacionalnim usklajevanjem in prilagodljivostjo nacionalnega konteksta. Ta razsežnost je pomembna tudi za model CIRG, saj se lahko verižni učinki razširijo čez državne meje, kar zahteva koordinacijske mehanizme zunaj nacionalne ravni.

Evropski regulatorni pristopi vse bolj obravnavajo odpornost kot kombinacijo tehnične zaščite, organizacijske pripravljenosti, kriznega odzivanja in večnivojske koordinacije med deležniki kritične infrastrukture. Vsebinsko se takšno razumevanje odpornosti odraža tudi v modelu CIRG, ki obravnava odpornost kot dinamičen proces organizacijskega prilagajanja, krizne eskalacije ter koordinacije odziva in obnovitvenih procesov v pogojih kompleksnega širjenja motenj (Boin idr., 2017; Rydén Sonesson idr., 2021).

3.4 Sinteza raziskovalne vrzeli

Primerjalna analiza literature kaže, da raziskave kritične infrastrukture potekajo v več med seboj povezanih, vendar razmeroma ločenih raziskovalnih tokovih. Prvi je usmerjen v analizo medsektorskih odvisnosti in širjenja verižnih učinkov, drugi v organizacijsko odpornost in prilagodljivost sistemov, tretji pa v krizno upravljanje, koordinacijo ter organizacijsko odločanje (Rydén Sonesson idr., 2021; Marquez-Tejon idr., 2023). Čeprav posamezni raziskovalni tokovi pomembno prispevajo k razumevanju odpornosti kritične infrastrukture, med njimi ostaja omejena konceptualna povezanost.

Enaka ugotovitev velja tudi za novejše evropske raziskovalne pobude na področju sistemskih tveganj. Giunta idr. (2025) upravljanje sistemskih tveganj obravnavajo kot izziv razumevanja kritične infrastrukture kot kompleksnega omrežja posameznih in institucionalnih akterjev z različnimi ter pogosto nasprotujočimi si interesi, vrednotami in pogledi. Poudarjajo pomen sodelovanja med upravljavci kritične infrastrukture in pristojnimi organi ob ohranjanju njihove avtonomije. Med pričakovanimi rezultati projekta je tudi opredelitev operativnih postopkov zasebnih in javnih upravljavcev ter pristojnih organov ob obsežnih motnjah kritične infrastrukture. Model CIRG to usmeritev nadgrajuje z upravljavskim okvirom, ki organizacijsko eskalacijo in koordinacijo odziva obravnava kot strukturiran proces z opredeljenimi odločitvenimi sprožilci.

Obstoječa literatura redkeje razvija upravljavske okvire, ki bi analitično razumevanje medsektorskih odvisnosti sistematično povezali z organizacijskim odločanjem, formalizirano eskalacijo odziva ter usklajevanjem obnovitvenih procesov (Boin idr., 2017). Opredeljena raziskovalna vrzel predstavlja izhodišče za razvoj modela CIRG. Namen modela ni nadomestiti obstoječih pristopov, temveč jih povezati v enoten upravljavski okvir, ki omogoča sistematičen prehod od zaznave sistemskih tveganj do koordiniranega organizacijskega odzivanja.

Prilagodljivo upravljanje poudarja institucionalno prilagodljivost in večnivojsko sodelovanje, inženiring odpornosti pa sposobnost prilagoditve delovanja sistema v pogojih motenj (Hollnagel, 2015; Folke idr., 2005). CIRG

te pristope povezuje z organizacijskim odločanjem, koordinacijo odziva in upravljanjem obnove v pogojih kompleksnih medsektorskih odvisnosti.

Posebnost modela CIRG je obravnava odpornosti kot proces prilagajanja in odzivne eskalacije glede na širjenje sistemske motnje. Model zato ne obravnava odpornosti zgolj kot sposobnosti absorpcije motenj, temveč kot formaliziran mehanizem aktivacije organizacijskega odločanja, koordinacije deležnikov in prilagajanja upravljalvske logike glede na stopnjo sistemske prizadetosti (Folke idr., 2005; Boin idr., 2017).

4 METODOLOGIJA KONCEPTUALNE SINTEZE

Prispevek temelji na analitični matriki literature, ki omogoča sledljivo povezovanje prepoznanih konceptov s strukturnimi elementi modela CIRG. Viri so bili sistematično obravnavani glede na raziskovalno področje, ključne koncepte ter njihovo funkcionalno vlogo pri oblikovanju modela. Takšen pristop zmanjšuje tveganje arbitrarnosti ter povečuje sledljivost in ponovljivost raziskovalnega postopka (Jaakkola, 2020).

4.1 Raziskovalni pristop

Prispevek je zasnovan kot konceptualna sinteza teorije (angl. *theory synthesis*) (Jaakkola, 2020), katerega namen je razvoj integrativnega upravljalvskega modela odpornosti kritične infrastrukture. Raziskovalni pristop temelji na sistematični sintezi literature s področij medsektorskih odvisnosti, organizacijske odpornosti, upravljalvskih mehanizmov in kriznega upravljanja.

Analiza literature je temeljila na primerjalni analizi, pri kateri so bili viri sistematično razvrščeni glede na njihov osrednji raziskovalni prispevek in organizacijsko funkcijo v procesu upravljanja odpornosti. Analiza je potekala v več fazah. Najprej smo identificirali ključne koncepte posameznih virov (npr. medsektorske odvisnosti, organizacijska eskalacija, krizna koordinacija in organizacijsko učenje). Sledila sta primerjalna klasifikacija ter združevanje konceptov v širše funkcionalne kategorije, ki so predstavljale osnovo za oblikovanje glavnih elementov modela CIRG. Struktura modela je nastala na podlagi primerjalne analize treh osrednjih raziskovalnih tokov – medsektorskih odvisnosti, organizacijske odpornosti in upravljanja kriznega odziva. Te ugotovitve so predstavljale osnovo za oblikovanje štirih glavnih elementov modela CIRG ter omogočile njihovo povezovanje v integriran upravljalvski okvir organizacijske odpornosti.

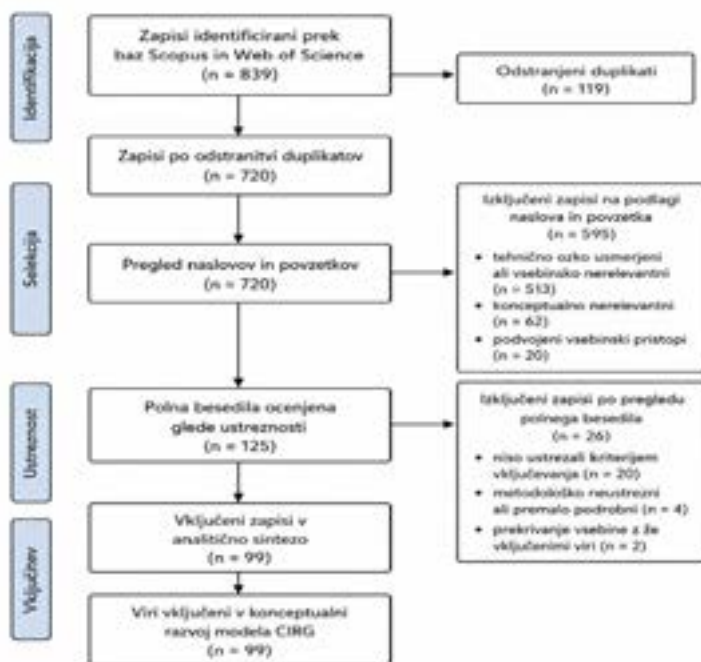
Konceptualni raziskovalni pristop je bil izbran zaradi kompleksnosti in interdisciplinarnosti obravnavanega problema, pri katerem obstoječi raziskovalni tokovi ostajajo razvejani med tehničnimi modeli verižnih učinkov in organizacijskimi pristopi kriznega upravljanja. Konceptualna sinteza zato omogoča integracijo heterogenih raziskovalnih pristopov v enoten upravljalvski okvir organizacijske odpornosti (Jaakkola, 2020).

4.2 Izbor in analiza literature

Korpus literature vključuje znanstvene članke, sistematične preglede, konferenčne prispevke, standarde, smernice in regulativne dokumente, ki obravnavajo kritično infrastrukturo, odpornost, verižne učinke, upravljaljske mehanizme in kibernetško-fizično varnost (Mottahedi idr., 2021).

Identifikacija literature je temeljila na strukturirani opredelitvi ključnih pojmov, ki so bili sistematično zbrani in organizirani v analitični matriki. Ta vključuje tri tematske sklope: varnost in upravljanje varnosti, odpornost in robustnost ter kritično infrastrukturo (kot kontekst obravnave). Na tej podlagi so bili oblikovani kombinirani iskalni nizi, ki povezujejo pojme iz vseh treh sklopov.

Iskanje je potekalo v znanstvenih bazah Scopus in Web of Science (v naslovih, povzetkih in ključnih besedah). Pri tem sta bila uporabljena Boolova operatorja AND in OR. Poudarek je bil na delih, objavljenih med letoma 2015 in 2025. Starejši viri so vključeni le v primerih, kjer predstavljajo temeljne teoretične koncepte ali izhodiščne modele, ki so še vedno relevantni za razumevanje obravnavanega problema.



Slika 1

Prilagojeni postopek identifikacije, selekcije in vključevanja literature

Vir: lastni prikaz

Slika 1 prikazuje prilagojen postopek izbora literature, ki uporablja elemente sledljivosti in transparentnosti, povzete po logiki PRISMA 2020. Zaradi konceptualne narave prispevka postopek ni bil izveden kot formalni sistematični pregled, temveč kot strukturiran in sledljiv pristop k identifikaciji, selekciji ter

analitični sintezi relevantnih virov. Postopek dokumentiranja in sledljivosti kljub temu sledi ključnim elementom PRISMA 2020, prilagojenim za konceptualno sintezo (Page idr., 2021; Jaakkola, 2020).

V končno analitično sintezo je bilo vključenih 99 virov, izbranih na podlagi njihove relevantnosti za tri osrednje raziskovalne tokove (medsektorske odvisnosti, odpornost in upravljanje). Končni nabor virov je bil določen na podlagi načela konceptualne saturacije, saj dodatni viri niso več bistveno prispevali k razširitvi ali spremembi identificiranih konceptov. Število virov odraža interdisciplinarni značaj teme in potrebo po zadostni konceptualni pokritosti treh raziskovalnih tokov (medsektorske odvisnosti, organizacijska odpornost in upravljanje).

Omejitev konceptualnega raziskovalnega pristopa je predvsem odsotnost neposredne empirične validacije modela v realnih organizacijskih okoljih. Model CIRG zato predstavlja teoretično izhodišče za nadaljnje empirične raziskave in razvoj operativnih kazalnikov učinkovitosti organizacijskega odzivanja (Jaakkola, 2020; Osei-Kyei idr., 2023).

Analitična matrika ni služila zgolj klasifikaciji literature, temveč tudi identifikaciji ponavljajočih se organizacijskih funkcij in konceptualnih povezav med raziskovalnimi tokovi, ki so predstavljale osnovo za razvoj strukturnih elementov modela CIRG.

4.3 Merila vključevanja in konceptualne sinteze

V analitično sintezo so bili vključeni viri, ki so obravnavali najmanj eno izmed naslednjih področij: medsektorske odvisnosti in verižne učinke, organizacijsko odpornost, upravljavske mehanizme kriznega odzivanja ali koordinacijo medorganizacijskega delovanja v kompleksnih sociotehničnih sistemih.

Iz analize so bili izključeni izrazito tehnično usmerjeni modeli brez organizacijske ali upravljavske dimenzije. Teoretična saturacija je bila dosežena v fazi, ko dodatni viri niso več prispevali novih organizacijskih funkcij, upravljavskih mehanizmov ali konceptualnih povezav med raziskovalnimi tokovi (Jaakkola, 2020).

4.4 Proces konceptualnega razvoja modela

Proces razvoja modela CIRG je potekal v petih iterativnih fazah: identifikacija treh osrednjih raziskovalnih tokov; identifikacija ponavljajočih se organizacijskih funkcij in konceptov; primerjalna klasifikacija ter združevanje konceptov v funkcionalne kategorije; abstrakcija in oblikovanje štirih glavnih ter dveh prečnih elementov modela; ter integracija elementov v enoten upravljavski okvir z mehanizmom odločitvenih sprožilcev in učno zanko.

Štirje glavni elementi modela CIRG niso bili določeni vnaprej, temveč so nastali kot rezultat primerjalne abstrakcije ponavljajočih se organizacijskih funkcij, identificiranih v analizirani literaturi. Ti funkcionalni sklopi so predstavljali osnovo za oblikovanje strukturne arhitekture modela CIRG. Takšen iterativni pristop sledi metodološkimi priporočilom za razvoj konceptualnih okvirov (Jabareen, 2009; Jaakkola, 2020).

5 PREDLAGANI MODEL CIRG

5.1 Konceptualna izhodišča in razvoj modela

Na podlagi identificirane raziskovalne vrzeli ter izvedene analitične sinteze literature je bil razvit model CIRG. Predlagani model CIRG predstavlja integrativni upravljavski okvir, katerega namen je povezati ključne organizacijske funkcije upravljanja odpornosti v enoten upravljavski model. Pri tem povezuje analizo medsektorskih odvisnosti, krizno odločanje, koordinacijo odziva in upravljanje obnovitvenih procesov v celovit proces upravljanja odpornosti kritične infrastrukture (Linkov idr., 2022; Labaka idr., 2015).

Razviti model CIRG operacionalizira odpornost kot večnivojski proces koordinacije, krizne eskalacije in delitve odgovornosti med deležniki kritične infrastrukture (Rhodes, 1996; Boin idr., 2017). Ključna novost modela je formalizacija prehodov med ravnmi odločanja ter koordinacija odziva med medsebojno odvisnimi akterji.

5.2 Struktura modela CIRG

Predlagani upravljavski model CIRG sestavljajo štirje glavni elementi (zaznava kritičnih odvisnosti, razvoj scenarijev verig vplivov, upravljanje odziva in usklajevanje obnovitvenih procesov) ter dva prečna elementa (odločitveni sprožilci in učna zanka), ki omogočata dinamično delovanje celotnega sistema (Linkov idr., 2022; Rydén Sonesson idr., 2021; Pescaroli in Alexander, 2016). Posamezni elementi modela predstavljajo medsebojno povezane organizacijske funkcije, ki skupaj podpirajo zaznavanje, odločanje, odzivanje in obnovo v različnih fazah razvoja sistemske motnje. Njihova medsebojna povezanost omogoča dinamično prilagajanje organizacijskega odziva ter usklajeno odločanje na operativni, taktični in strateški ravni. Arhitektura modela in medsebojne povezave med njegovimi elementi so prikazane na Sliki 2.



Slika 2
Konceptualna
arhitektura
modela CIRG

Vir: lastni prikaz na podlagi Linkov idr. (2022), Boin idr. (2017), Rydén Sonesson idr. (2021) in Pescaroli in Alexander (2016).

Slika 2 prikazuje logiko delovanja modela CIRG od zaznave kritičnih odvisnosti do kriznega odziva in obnove sistema. Poseben pomen imajo odločitvena sprožilca in učna zanka, ki omogočajo dinamično prilagajanje modela.

Za večjo preglednost modela so ključni elementi modela ter njihove funkcije povzeti v tabeli 1. Tabela operacionalizira posamezne komponente modela CIRG in prikazuje njihov pomen v procesu upravljanja odpornosti kritične infrastrukture.

Tabela 1
Organizacijske funkcije in upravljavski pomen elementov modela CIRG

Element modela	Organizacijska funkcija
Vhodni elementi modela	Zagotavljanje vhodnih informacij za zaznavo sistemskih tveganj in odvisnosti
Robustni način delovanja	Upravljanje normalnega delovanja sistema in obvladovanje rutinskih motenj
Odločitveni sprožilci	Formalizacija prehodnih pragov med operativnim in kriznim načinom delovanja
Odločitev o eskalaciji	Aktivacija kriznega upravljanja na podlagi vnaprej določenih meril
Odporni način delovanja	Koordinacija kriznega odziva in prilagodljivega delovanja sistema
Obnova in učenje	Stabilizacija sistema ter institucionalizacija organizacijskega učenja
Izhodi modela	Doseganje organizacijskih in sistemskih učinkov odpornosti
Prečni elementi modela	Povezovanje spremljanja, merjenja in odločanja v vseh fazah modela

Vir: lastni prikaz

5.3 Ključni elementi in mehanizmi modela

Osnova učinkovitega upravljanja odpornosti je pravočasna identifikacija kritičnih funkcij, njihovih medsektorskih odvisnosti ter ranljivosti, ki lahko omogočajo širjenje verižnih učinkov v kritični infrastrukturi (Rinaldi idr., 2001; Pescaroli in Alexander, 2016). Organizacije morajo vzpostaviti mehanizme kontinuiranega spremljanja funkcionalnih, informacijskih, logističnih in organizacijskih povezav med sistemi.

Za zmanjševanje negotovosti v pogojih kompleksnih motenj model CIRG vključuje razvoj scenarijev verig vplivov, ki omogočajo določanje prioritet odziva ter podporo organizacijskemu odločanju. Razvoj scenarijev verig vplivov podpira simulacijo možnih poti širjenja motenj med medsebojno povezanimi sektorji, identifikacijo kritičnih točk sistemske ranljivosti ter organizacijsko odločanje in krizno načrtovanje (Helbing, 2013; Gordan idr., 2024; Pescaroli in Alexander, 2016).

V pogojih širjenja verižnih učinkov postane osrednji izziv pravočasno usklajevanje odziva med deležniki. Upravljanje odziva predstavlja osrednji operativni element modela CIRG, saj omogoča prehod iz rutinskega upravljanja incidentov v odporni način delovanja. Vključuje aktivacijo ustreznih ravni upravljanja, koordinacijo med organizacijami, določanje prioritet odziva ter vzpostavitev skupnega situacijskega pregleda na podlagi usklajenega pretoka informacij, jasne razdelitve pristojnosti in skupnega odločanja v pogojih visoke negotovosti (Boin idr., 2017; Rydén Sonesson idr., 2021).

Četrty element modela vključuje določanje prioritet ponovne vzpostavitve kritičnih storitev, koordinacijo razporejanja virov ter usklajevanje aktivnosti med medsebojno odvisnimi organizacijami in sektorji. V kompleksnih sistemih lahko nepravilno zaporedje obnove posameznih funkcij povzroči dodatne motnje ali ponovno destabilizacijo sistema. Obnovitveni procesi zato ne predstavljajo zgolj tehničnega vračanja sistema v prvotno stanje, temveč tudi proces stabilizacije delovanja, prilagajanja postopkov ter zmanjševanja tveganj za prihodnje incidente. S tem je omogočena dolgoročna krepitev organizacijske odpornosti in izboljševanje usklajevanja med deležniki kritične infrastrukture (Hickford idr., 2019; Duchek, 2020).

CIRG dopolnjujeta dva prečna elementa: odločitveni sprožilci in učna zanka. Skupaj delujeta kot regulativni mehanizem modela in omogočata njegovo dinamično prilagajanje. Odločitveni sprožilci omogočajo strukturiran prehod med operativnim odzivanjem na incident in širšim kriznim upravljanjem. Njihov namen je omogočiti pravočasno organizacijsko eskalacijo ob preseganju zmogljivosti standardnega odziva (Boin idr., 2017). Za operativno uporabnost modela so sprožilci operacionalizirani v petih osnovnih kategorijah:

- časovni (trajanje motnje),
- vplivni (obseg prizadetih funkcij ali deležnikov),
- sistemski (širjenje motnje prek medsektorskih odvisnosti),
- informacijski (izguba situacijskega pregleda) in
- regulatorni sprožilci (aktivacija formalnih obveznosti kriznega odziva).

Za njihovo učinkovito uporabo morajo biti sprožilci opredeljeni z merljivimi ali jasno določljivimi pragovi, ki temeljijo na organizacijskih prioritetah, analizi tveganj in scenarijih verig vplivov.

Drugi prečni element (učna zanka) omogoča sistematično izboljševanje modela na podlagi izkušenj iz incidentov in vaj, vključno s preverjanjem ustreznosti zemljevida odvisnosti, scenarijev in upravljavskih mehanizmov. S tem deluje kot mehanizem institucionaliziranega učenja, ki omogoča dolgoročno krepitev organizacijske odpornosti (Duchek, 2020).

Med ključnimi operativnimi mehanizmi modela CIRG imajo posebno vlogo odločitveni sprožilci, saj omogočajo pravočasno organizacijsko eskalacijo in aktivacijo ustreznih ravni upravljanja. Tabela 2 ponazarja način operacionalizacije odločitvenih sprožilcev v okviru modela CIRG.

Vrsta sprožilca	Primer kazalnika	Ilustrativni prag eskalacije	Upravljavski učinek	Organizacijski odziv
Časovni	Izpad kritične storitve	> 30 minut neprekinjene motnje	Prehod iz operativnega v odporni način delovanja	Aktivacija kriznega štaba
Vplivni	Prizadetost uporabnikov ali kritičnih funkcij	> 20 % prizadetih uporabnikov ali kritične funkcije	Aktivacija medorganizacijskega usklajevanja	Aktivacija koordinacije med deležniki

Tabela 2
Ilustrativni primer organizacijskih sprožilcev modela CIRG

Sistemske	Potrjeno širjenje motnje v drug sektor kritične infrastrukture	Medsektorska eskalacija incidenta	Aktivacija večnivojske upravljaljske koordinacije	Aktivacija odpornega načina delovanja
Informacijske	Izguba situacijskega pregleda ali potrjena informacijska nedosegljivost	Kritična degradacija komunikacijskih tokov	Eskalacija strateškega odločanja	Aktivacija strateške ravni upravljanja
Regulatorne	Aktivacija zakonskih ali regulatornih obveznosti kriznega odziva	Formalna razglasitev kriznega stanja ali regulativni prag	Aktivacija institucionalne koordinacije	Vključitev regulatorjev in državnih organov

Vir: lastni prikaz na podlagi Boin idr. (2017), Duchek (2020) in National Institute of Standards and Technology (2024)

Operativna uporaba sprožilcev v modelu CIRG temelji na zaporednem procesu zaznave motnje, preverjanja eskalacijskih pragov, aktivacije ustrezne ravni upravljanja ter koordinacije odziva med deležniki. Po zaznavi motnje operativna raven preveri, ali incident presega vnaprej določene časovne, vplivne ali sistemske pragove. Ob doseženem pragu se aktivira ustrezna raven kriznega upravljanja, ki prevzame koordinacijo odziva in usklajevanje medorganizacijskih aktivnosti.

Pragovi sprožilcev morajo biti prilagojeni značilnostim organizacije, kritičnosti funkcij in stopnji medsektorske povezanosti. Njihovo ustreznost je treba periodično preverjati ter prilagajati na podlagi incidentov, vaj in procesov organizacijskega učenja (National Institute of Standards and Technology, 2024; Duchek, 2020).

Upravljaljska arhitektura modela CIRG temelji na večnivojski organizaciji odziva, ki vključuje operativno, taktično in strateško raven upravljanja. Posamezne ravni se aktivirajo glede na stopnjo sistemske eskalacije ter omogočajo usklajeno koordinacijo odziva in obnove sistema (Boin idr., 2017; Rydén Sonesson idr., 2021). Za večjo konceptualno preglednost so ključne ravni upravljanja, njihove funkcije in aktivacijski sprožilci prikazani v tabeli 3.

Tabela 3
*Večnivojska
upravljaljska ar-
hitektura modela
CIRG*

Raven upravljanja	Primarna odgovornost	Odločitveni fokus	Aktivacijski sprožilci	Ključni deležniki
Operativna	Stabilizacija incidenta	Omejevanje neposredne motnje	Lokalni operativni incident	Operativne enote, varnostno- operativni centri, osebje operativnih tehnologij
Taktična	Medorganizacijska koordinacija	Omejevanje širjenja verižnih učinkov	Medsektorska prizadetost	Nacionalni odzivni centri, regulatorji, partnerji

Strateška	Krizno upravljanje in ponovna vzpostavitev sistema	Zagotavljanje kontinuitete kritičnih funkcij	Sistemska eskalacija	Vodstvo organizacij, država, krizni štabi
-----------	--	--	----------------------	---

Vir: lastni prikaz

Pomemben element učinkovitega delovanja modela CIRG predstavlja tudi vzpostavljanje skupnega situacijskega pregleda (angl. *situational awareness*) med deležniki kritične infrastrukture. V pogojih kompleksnih verižnih učinkov organizacije pogosto delujejo ob nepopolnih informacijah, visoki časovni obremenitvi in interpretativni negotovosti. Učinkovitost organizacijske eskalacije je zato pomembno odvisna od vzpostavitve skupnega razumevanja razvoja motnje, pravočasne izmenjave informacij ter usklajenega interpretiranja tveganj med deležniki (Jovanović idr., 2021b).

5.4 Empirična validacija in nadaljnji razvoj modela

Za zmanjšanje abstraktnosti modela prispevek predlaga okvirno operacionalizacijo ključnih komponent s kazalniki, ki lahko služijo kot podlaga za prihodnjo empirično validacijo. Predlagani kazalniki se nanašajo na stopnjo identifikacije kritičnih odvisnosti, razvitost scenarijev verižnih učinkov, časovno učinkovitost prehoda med robustnim in odpornim načinom delovanja, kakovost koordinacije med deležniki in sposobnost sistematičnega učenja po incidentih. Predlagani okvir omogoča prihodnjo primerjalno analizo organizacijske odpornosti med različnimi sektorji kritične infrastrukture. Tabela 4 predstavlja primere okvirnih kazalnikov, ki podpirajo nadaljnjo operacionalizacijo modela CIRG.

Element modela	Primer kazalnika	Možen način merjenja	Namen kazalnika
Eskalacija odziva	Čas aktivacije kriznega upravljanja	Minute od zaznave incidenta do aktivacije kriznega štaba	Merjenje hitrosti organizacijske eskalacije
Koordinacija odziva	Čas deljenja ključnih informacij med deležniki	Čas med zaznavo incidenta in distribucijo ključnih informacij	Ocena učinkovitosti koordinacije in komunikacije
Obnova sistema	Čas ponovne vzpostavitve kritičnih funkcij	RTO oz. čas stabilizacije sistema	Ocena učinkovitosti obnovitvenih procesov
Organizacijsko učenje	Stopnja implementacije ukrepov po incidentu	Delež realiziranih korektivnih ukrepov	Merjenje učinkovitosti učne zanke
Medorganizacijsko sodelovanje	Število skupnih vaj in koordinacijskih aktivnosti	Letno število izvedenih vaj ali usklajevanj	Krepitev medorganizacijske koordinacije
Situacijski pregled	Stopnja skupnega situacijskega razumevanja med deležniki	Delež usklajenih operativnih ocen med organizacijami	Ocena kakovosti skupnega situacijskega pregleda

Tabela 4
Primeri okvirnih kazalnikov modela CIRG

Učinkovitost sprožilcev	Delež pravilno aktiviranih eskalacijskih sprožilcev	Razmerje med upravičenimi in neupravičenimi eskalacijami	Ocena ustreznosti pragov sprožilcev
Kakovost odločanja	Čas sprejetja ključnih kriznih odločitev	Čas od zaznave incidenta do potrditve ključnih odločitev	Merjenje učinkovitosti kriznega odločanja
Medsektorska koordinacija	Stopnja sodelovanja med sektorji kritične infrastrukture	Število koordiniranih aktivnosti ali delež vključenih deležnikov	Ocena učinkovitosti medorganizacijskega usklajevanja

Vir: lastni prikaz na podlagi Boin idr. (2017), Osei-Kyei idr. (2023), Rydén Sonesson idr. (2021), Endsley (1995), Comfort (2007), Ansell idr. (2010) in Duchek (2020).

5.5 Primer uporabe modela CIRG

V primeru kibernetskega napada na sistem za nadzor, upravljanje in zajem podatkov SCADA (angl. *Supervisory Control and Data Acquisition*) (Upadhyay in Sampalli, 2020) energetskega operaterja, ki povzroči izpad oskrbe s pitno vodo, model CIRG omogoča strukturirano organizacijsko eskalacijo odziva. V robustnem načinu delovanja operater najprej aktivira rezervne generatorje in standardne protokole incidenta. Po 35 minutah neprekinjene motnje se aktivira časovni sprožilec, hkrati pa se zaradi potrjenega širjenja motnje na vodovodni sektor aktivira tudi sistemski sprožilec. Na tej podlagi vodja incidenta sproži prehod v odporni način delovanja ter eskalira odziv na taktično raven upravljanja.

Sledi medorganizacijska koordinacija med energetske, vodovodnim, zdravstvenim sektorjem ter civilno zaščito, določijo se prioritete ponovne vzpostavitve kritičnih funkcij (najprej bolnišnice in črpališča, nato gospodinjstva), hkrati pa se vzpostavi skupni krizni štab. V fazi stabilizacije sistema se aktivira tudi učna zanka, namenjena posodobitvi zemljevida medsektorskih odvisnosti ter prilagoditvi pragov sprožilcev na podlagi pridobljenih izkušenj. Takšen strukturiran prehod med organizacijskimi ravni omogoča učinkovitejše omejevanje širjenja verižnih učinkov in skrajševanje trajanja systemske motnje (Boin idr., 2017; Rydén Sonesson idr., 2021; National Institute of Standards and Technology, 2024).

Uporabnost modela CIRG je mogoče ponazoriti tudi na primeru kibernetskega napada na ukrajinsko elektroenergetsko infrastrukturo leta 2015, ki velja za enega prvih potrjenih kibernetskih napadov z neposrednimi fizičnimi posledicami za kritično infrastrukturo. Incident je razkril izrazite medsektorske odvisnosti med energetske, komunikacijskimi sistemi in kriznim upravljanjem ter pokazal, kako se lahko motnje širijo med kritičnimi sektorji. Z vidika modela CIRG bi formalizirani organizacijski sprožilci lahko omogočili hitrejšo eskalacijo odziva, zgodnejše usklajevanje med deležniki ter pravočasno vključitev regulatorjev, nacionalnih odzivnih centrov in drugih akterjev kritične infrastrukture. Primer hkrati potrjuje pomen usklajevanja obnovitvenih procesov in organizacijskega učenja, saj so ukrajinski operaterji po napadu bistveno okrepili postopke kriznega upravljanja, segmentacijo omrežij in koordinacijske mehanizme med organizacijami (Lee idr., 2016).

6 RAZPRAVA

Obstoječi modeli odpornosti kritične infrastrukture pogosto predpostavljajo, da organizacije analitično zaznano tveganje uspešno pretvorijo v pravočasno ukrepanje. V praksi pa številni incidenti kažejo, da fragmentacija pristojnosti, nejasne delitve odgovornosti in odsotnost formaliziranih eskalacijskih mehanizmov pogosto upočasnijo aktivacijo širšega kriznega odziva (Boin idr., 2017; Rydén Sonesson idr., 2021). Model CIRG skuša to omejitev nasloviti z vključitvijo formaliziranih sprožilcev in večnivojske koordinacije, vendar je njihova učinkovitost v praksi odvisna od organizacijske pripravljenosti ter kakovosti medinstitucionalnega sodelovanja.

Ključna dodana vrednost modela CIRG je vključitev upravljske dimenzije organizacijske odpornosti v obravnavo kritične infrastrukture. Za razliko od obstoječih pristopov, ki se osredotočajo predvsem na analizo medsektorskih odvisnosti, širjenja motenj ali posamezne vidike kriznega upravljanja (Gordan idr., 2024; Marquez-Tejon idr., 2023), CIRG te elemente povezuje v enoten konceptualni okvir, ki podpira organizacijsko odločanje, koordinacijo odziva in upravljanje obnovitvenih procesov v pogojih kompleksnih verižnih učinkov. Njegova posebnost je vključitev formaliziranih odločitvenih sprožilcev in večnivojske upravljske arhitekture, ki omogočata bolj strukturirano organizacijsko eskalacijo ter usklajevanje odziva med različnimi ravni upravljanja (Boin idr., 2017; Rydén Sonesson idr., 2021).

Razviti model deluje kot integriran sistem, ki analitično razumevanje sistemskih tveganj pretvarja v konkretno ukrepanje na strateški, taktični in operativni ravni (Marquez-Tejon idr., 2023). Implementacija modela CIRG zahteva vzpostavitev formaliziranega procesa upravljanja medsektorskih odvisnosti, določitev odgovornih nosilcev eskalacije ter opredelitev eskalacijskih pragov. Scenarije verig vplivov je smiselno vključiti v krizno načrtovanje in zagotavljanje stalnega delovanja. Organizacije morajo redno preverjati sprožilce, izvajati medorganizacijske vaje ter vzpostaviti učinkovito deljenje informacij, pri čemer uspešna implementacija predpostavlja zadostne organizacijske zmogljivosti in podporo vodstva (Boin idr., 2017; Rydén Sonesson idr., 2021).

Z vidika teorije odpornosti predlagani model povezuje literaturo o medsektorskih odvisnostih, organizacijski odpornosti in kriznem upravljanju v enoten konceptualni okvir. Odpornost pri tem ni obravnavana zgolj kot lastnost sistema, temveč kot proces koordinacije, eskalacije odločanja in institucionalnega učenja v pogojih sistemske negotovosti.

Model CIRG ima kljub integrativni zasnovi več omejitev. Gre za konceptualni model brez neposredne empirične validacije, njegova implementacija pa je lahko otežena v organizacijah z nižjo stopnjo organizacijske zrelosti, omejenimi zmogljivostmi ter razdrobljenostjo regulativnega okvira. Poseben izziv predstavlja standardizacija sprožilcev med različnimi sektorji. Pretirana formalizacija sprožilcev in koordinacijskih postopkov lahko v pogojih kompleksnih kriznih situacij zmanjša organizacijsko fleksibilnost. Učinkovitost modela je zato pomembno odvisna od sposobnosti organizacij, da vzpostavijo ravnotežje med formaliziranimi postopki in prilagodljivim kriznim odločanjem (Boin idr., 2017). Poseben izziv predstavlja tudi možnost lažno pozitivnih sprožilcev (angl. *false*

positives), pri katerih prezgodnja eskalacija v odporni način delovanja povzroči nepotrebno obremenitev organizacije, povečano porabo virov ter utrujenost ključnih deležnikov (Ansell idr., 2010).

Poleg operativnih omejitev odpira model tudi več širših organizacijskih in upravljavskih dilem. Dodatno tveganje predstavlja pojav t. i. »*trigger fatigue*«, pri katerem prepogosta aktivacija kriznih mehanizmov postopno zmanjšuje odzivnost organizacij in povzroča utrujenost ključnih deležnikov. Učinkovitost modela je zato odvisna tudi od organizacijske kulture, stopnje medorganizacijskega zaupanja ter sposobnosti politične in institucionalne koordinacije med deležniki sistema. V okoljih z izrazito razpršenimi pristojnostmi ali nizko stopnjo sodelovanja med deležniki lahko implementacija modela ostane omejena kljub formalno vzpostavljenim upravljavskim mehanizmom (Comfort, 2007; Ansell idr., 2010).

Nadaljnji razvoj modela zahteva empirično validacijo v različnih sektorjih kritične infrastrukture ter razvoj merljivih kazalnikov učinkovitosti organizacijskega odzivanja. Prihodnja empirična validacija modela CIRG bi lahko temeljila na večmetodnem raziskovalnem pristopu. Model bi bilo mogoče preverjati v okviru študij primerov incidentov v kritični infrastrukturi, ekspertnih intervjujev, Delphi analiz, simulacijskih vaj ter primerjalne analize organizacijskih odzivov v različnih sektorjih kritične infrastrukture. Posebej pomembna bi bila analiza učinkovitosti odločitvenih sprožilcev, časa eskalacije odziva ter kakovosti medorganizacijske koordinacije. Takšen pristop bi omogočil preverjanje predpostavk modela, razvoj operativnih kazalnikov ter oceno njegove uporabnosti v različnih organizacijskih in regulatornih okoljih (Jaakkola, 2020; Osei-Kyei idr., 2023).

7 ZAKLJUČEK

Prispevek obravnava vrzel med analitičnim razumevanjem medsektorskih odvisnosti ter sposobnostjo organizacij, da zaznana tveganja pravočasno pretvorijo v učinkovito krizno ukrepanje, koordinacijo odziva in obnovo sistema. Na podlagi strukturirane konceptualne sinteze literature je bil razvit model CIRG, ki odpornost obravnava kot večnivojski proces kriznega usklajevanja in prilagodljivega odzivanja v pogojih kompleksnih sistemskih motenj.

Osrednji prispevek modela CIRG je povezovanje analitične zaznave sistemskih tveganj z mehanizmi kriznega odločanja, koordinacije odziva in ponovne vzpostavitve sistema. Model pri tem presega pretežno tehnično obravnavo verižnih učinkov, saj vključuje tudi organizacijske, koordinacijske in odločitvene razsežnosti kriznega odzivanja. Posebna izvirnost modela je v formalizaciji odločitvenih sprožilcev kot mehanizma prehoda med robustnim in odpornim načinom delovanja. Tak pristop omogoča bolj strukturirano in pravočasno aktivacijo kriznega upravljanja v pogojih širjenja sistemskih motenj. Prispevek ima tudi praktično uporabnost za organizacije kritične infrastrukture, saj model CIRG podpira sistematično obravnavo medsektorskih odvisnosti ter strukturirano načrtovanje, koordinacijo in upravljanje kriznega odziva. Model lahko služi kot konceptualna podlaga za razvoj organizacijskih upravljavskih okvirov, načrtovanje kriznega upravljanja, izvajanje vaj ter izboljševanje medorganizacijske

koordinacije v pogojih kompleksnih kriznih situacij. Takšna ilustrativna aplikacija nakazuje, da CIRG ni uporaben zgolj kot konceptualni upravljavski okvir, temveč tudi kot potencialno operativno orodje za strukturiranje organizacijskega odziva v pogojih kompleksnih verižnih učinkov (Boin idr., 2017; Rydén Sonesson idr., 2021).

Pomemben del koncepta CIRG predstavlja tudi institucionalna raven države, ki povezuje organizacijsko upravljanje kritičnih subjektov z nacionalnim regulativnim in varnostnim okvirom. Državne institucije v tem okviru določajo pristojnosti in obveznosti ter zagotavljajo regulativne in institucionalne pogoje za zaščito in odpornost kritične infrastrukture, vključno z ukrepi na področju obrambe, informacijske in kibernetske varnosti ter zasebnega varovanja. V slovenskem okolju se te pristojnosti izvajajo skozi več medsebojno povezanih predpisov, zlasti Zakon o kritični infrastrukturi (ZKI-1), Zakon o obrambi (ZObr), Zakon o informacijski varnosti (ZInfV-1) in Zakon o zasebnem varovanju (ZZasV-1). Ti predpisi urejajo različna področja varnosti, zaščite in odpornosti ter skupaj tvorijo širši institucionalni in regulativni okvir, v katerem se izvajajo ukrepi za zagotavljanje neprekinjenega delovanja kritične infrastrukture. Model CIRG zato državnih institucij ne obravnava kot zunanje akterje, temveč kot del večnivojske upravljalvske strukture, ki je vključena v regulativni kontekst in določanje pogojev za ukrepanje ter koordinacijo na taktični in strateški ravni (Zakon o kritični infrastrukturi (ZKI-1), 2024; Zakon o obrambi (ZObr), 2004; Zakon o informacijski varnosti (ZInfV-1), 2025; Zakon o zasebnem varovanju (ZZasV-1), 2011).

Kljub integrativni zasnovi ima model tudi več omejitev. Prispevek predstavlja konceptualni okvir brez neposredne empirične validacije, zato ostajajo odprta vprašanja operativne izvedljivosti modela v različnih sektorjih kritične infrastrukture. Dodatne izzive predstavljajo razpršenost regulativnih pristojnosti, različne organizacijske zmogljivosti ter možnost pretirane formalizacije sprožilcev in koordinacijskih postopkov. Vsi ti elementi lahko v pogojih visoke negotovosti zmanjšajo organizacijsko prilagodljivost in fleksibilnost kriznega odločanja (Comfort, 2007).

Prispevek hkrati kaže, da učinkovito upravljanje odpornosti kritične infrastrukture ni odvisno zgolj od poznavanja medsektorskih odvisnosti ali razvoja tehničnih rešitev, temveč tudi od sposobnosti organizacij, da zaznana tveganja pravočasno pretvorijo v usklajeno odločanje, koordiniran odziv in prilagodljivo upravljanje. V tem pogledu model CIRG predstavlja povezavo med analitičnim razumevanjem sistemskih tveganj in organizacijskimi mehanizmi kriznega upravljanja ter prispeva k celovitejšemu razumevanju upravljanja odpornosti kritične infrastrukture.

Nadaljnji razvoj modela CIRG zahteva predvsem empirično validacijo v različnih sektorjih kritične infrastrukture, razvoj operativnih kazalnikov upravljalvske učinkovitosti ter analizo učinkovitosti odločitvenih sprožilcev v realnih ali simuliranih kriznih situacijah. Posebej pomembno ostaja vprašanje ravnotežja med formaliziranimi postopki in prilagodljivim odločanjem v pogojih kompleksnih verižnih učinkov (Osei-Kyei idr., 2023).

LITERATURA

- Ansell, C., Boin, A. in Keller, A. (2010). Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*, 18(4), 195–207. <https://doi.org/10.1111/j.1468-5973.2010.00620.x>
- Boin, A., Hart, P., Stern, E. in Sundelius, B. (2017). *The politics of crisis management: Public leadership under pressure*. Cambridge University Press.
- Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, 67(s1), 189–197. <https://doi.org/10.1111/j.1540-6210.2007.00827.x>
- 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>
- Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13(1), 215–246. <https://doi.org/10.1007/s40685-019-0085-7>
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32–64. <https://doi.org/10.1518/001872095779049543>
- 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/eng>
- 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*, L 333, 80–152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
- Folke, C., Hahn, T., Olsson, P. in Norberg, J. (2005). Adaptive governance of social-ecological systems. *Annual Review of Environment and Resources*, 30, 441–473. <https://doi.org/10.1146/annurev.energy.30.050504.144511>
- Gerbec, M., Čaleta, D., Modic, J., Giunta, G. in Durante, N. G. (2025). Cross-CI assessment of risks and cascading effects in ATLANTIS project. *Applied Sciences*, 15(19), Article 10374. <https://doi.org/10.3390/app151910374>
- Giunta, G., Stira, C., Modic, J., Čaleta, D., Semertzidis, T., Zahariadis, T. in Skianis, C. (2025). Improved resilience of critical infrastructures against large-scale transnational and systemic risks. V I. Gkotsis, D. Kavallieros, N. Stoianov, S. Vrochidis, D. Diagourtas, B. Akhgar (ur.), *Paradigms on technology development for security practitioners* (str. 169–182). Springer. https://doi.org/10.1007/978-3-031-62083-6_14
- Gordan, M., Kountche, D. A., McCrum, D., Schauer, S., König, S., Delannoy, S., Connolly, L., Iacob, M., Durante, N. G., Shekhawat, Y., Carrasco, C., Katsoulakos, T. in Carroll, P. (2024). Protecting critical infrastructure against cascading effects: The PRECINCT approach. *Resilient Cities and Structures*, 3(3), 1–19. <https://doi.org/10.1016/j.rcns.2024.04.001>

- Helbing, D. (2013). Globally networked risks and how to respond. *Nature*, 497(7447), 51–59. <https://doi.org/10.1038/nature12047>
- Hickford, A. J., Blainey, S. P., Ortega Hortelano, A. in Pant, R. (2018). Resilience engineering: Theory and practice in interdependent infrastructure systems. *Environment Systems and Decisions*, 38, 278–291. <https://doi.org/10.1007/s10669-018-9707-4>
- Hosseini, S., Barker, K. in Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145, 47–61. <https://doi.org/10.1016/j.res.2015.08.006>
- Hollnagel, E. (2015). *From Safety-I to Safety-II: A white paper*. The Resilient Health Care Net. <https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-white-papr.pdf>
- Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, 8(4), 49–62. <https://doi.org/10.1177/160940690900800406>
- Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10, 18–26. <https://doi.org/10.1007/s13162-020-00161-0>
- Jovanović, A., Jelić, M., Klimek, P., Chakravarty, S., Čaleta, D., Gerbec, M. in Nguyen, M. T. (2021a). Modelling interdependencies within and among critical infrastructures/entities exposed to cyber-physical threats. V J. Soldatos, I. Praça in A. Jovanović (ur.), *Cyber-physical threat intelligence for critical infrastructures security: Securing critical infrastructures in air transport, water, gas, healthcare, finance and industry* (str. 53–85). Emerald Publishing Limited. <https://doi.org/10.1561/9781680838237.ch3>
- Jovanović, A. S., Chakravarty, S. in Jelić, M. (2021b). Resilience and situational awareness in critical infrastructure protection: An indicator-based approach. V V. Rosato in A. Di Pietro (ur.), *Issues on Risk Analysis for Critical Infrastructure Protection* (str. 1–27). IntechOpen. <https://doi.org/10.5772/intechopen.97810>
- Labaka, L., Hernantes, J. in Sarriegi, J. M. (2015). Resilience framework for critical infrastructures: An empirical study in a nuclear plant. *Reliability Engineering & System Safety*, 141, 92–105. <https://doi.org/10.1016/j.res.2015.03.009>
- Lee, R. M., Assante, M. J. in Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid*. Electricity Information Sharing and Analysis Center (E-ISAC) and SANS Institute. <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>
- Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A. in Panda, A. (2022). Resilience stress testing for critical infrastructure. *International Journal of Disaster Risk Reduction*, 82, Article 103323. <https://doi.org/10.1016/j.ijdrr.2022.103323>
- Madni, A. M. in Jackson, S. (2009). Towards a conceptual framework for resilience engineering. *IEEE Systems Journal*, 3(2), 181–191. <https://doi.org/10.1109/JSYST.2009.2017397>
- Marquez-Tejon, J., Jiménez Partearroyo, M. in Benito-Osorio, D. (2023). Integrated security management model: A proposal applied to organisational resilience. *Security Journal*, 37, 375–398. <https://doi.org/10.1057/s41284-023-00381-6>

- Meuleman, L. (2010). The cultural dimension of metagovernance: Why governance doctrines may fail. *Public Organization Review*, 10, 49–70. <https://doi.org/10.1007/s11115-009-0088-5>
- Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A. in Barabadi, A. (2021). The resilience of critical infrastructure systems: A systematic literature review. *Energies*, 14(6), Article 1571. <https://doi.org/10.3390/en14061571>
- Myers, C. G. in Sutcliffe, K. M. (2022). High reliability organising in healthcare: Still a long way left to go. *BMJ Quality & Safety*, 31(12), 845–848. <https://doi.org/10.1136/bmjqs-2021-014141>
- National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. <https://doi.org/10.6028/nist.cswp.29>
- Osei-Kyei, R., Almeida, L. M., Ampratwum, G. in Tam, V. (2023). Systematic review of critical infrastructure resilience indicators. *Construction Innovation*, 23(5), 1210–1231. <https://doi.org/10.1108/CI-03-2021-0047>
- 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, n71. <https://doi.org/10.1136/bmj.n71>
- Pescaroli, G. in Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards*, 82, 175–192. <https://doi.org/10.1007/s11069-016-2186-3>
- Rinaldi, S. M., Peerenboom, J. P. in Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6), 11–25. <https://doi.org/10.1109/37.969131>
- Rhodes, R. A. W. (1996). The new governance: Governing without government. *Political Studies*, 44(4), 652–667. <https://doi.org/10.1111/j.1467-9248.1996.tb01747.x>
- 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>
- Smith, R. L. Q. in Shashkina, O. (2023). A way forward to integrating cascading risk into local resilience strategies in Central Asia. *Progress in Disaster Science*, 17, Article 100273. <https://doi.org/10.1016/j.pdisas.2022.100273>
- Stouffer, K. A., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., in Thompson, M. (2023). *Guide to operational technology (OT) security (NIST SP 800-82 Rev. 3)*. National Institute of Standards and Technology. <https://doi.org/10.6028/nist.sp.800-82r3>
- Upadhyay, D. in Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, 89, Article 101666. <https://doi.org/10.1016/j.cose.2019.101666>
- Zakon o kritični infrastrukturi (ZKI-1). (2024). *Uradni list RS*, (102/24).

Zakon o obrambi (ZObr). (2004). *Uradni list RS*, (103/04, 95/15, 139/20, 112/25).

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

Zakon o zasebnem varovanju (ZZasV-1). (2011). *Uradni list RS*, (17/11).

O avtorjih:

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

Dr. Miha Dvojmoč, izredni profesor, Univerza v Mariboru Fakulteta za varnostne vede. E-pošta: miha.dvojmoc@um.si