Zaprimljen: 15.6.2025.
Odobren za objavu: 13.10.2025.
Pregledni rad

ULOGA KIBERNETIČKE SIGURNOSTI U JAČANJU REGIONALNE GOSPODARSKE OTPORNOSTI: INSTITUCIONALNE I GEOPOLITIČKE PERSPEKTIVE

Sanela Ravlić[1], Ivana Unukić[2]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: sravlic@unisb.hr
[2]Sveučilište J. J. Strossmayera u Osijeku, Ekonomski fakultet u Osijeku, Trg Lj. Gaja 7, 31000 Osijek, Hrvatska, ePošta: ivana.unukic@efos.hr

Sažetak: Ovaj rad istražuje ulogu sigurnosti i kibernetičke sigurnosti unutar šire analize regionalne ekonomije jugoistočne Europe, s fokusom na geopolitičke i društvene izazove koji oblikuju gospodarske procese u Hrvatskoj i susjednim zemljama. U digitaliziranom gospodarstvu, sigurnosna infrastruktura – uključujući zaštitu informacijskih sustava, podataka i komunikacijskih kanala – postaje ključan preduvjet za održivi regionalni razvoj, gospodarsku stabilnost i prekograničnu suradnju.
Kibernetička sigurnost razmatra se ne samo kao tehnički zahtjev, već i kao element koji je duboko povezan s institucionalnim kapacitetima sigurnosnih protokola i razinom međusobnog povjerenja među državama regije. Jezične barijere dodatno otežavaju usklađivanje sigurnosnih mjera i krizne komunikacije, čime se povećava rizik od digitalne fragmentacije prostora koji teži integraciji.
U radu se analizira kako različite razine kibernetičke otpornosti i sigurnosne politike među državama utječu na investicijsku atraktivnost, inovacijsku suradnju i digitalnu transformaciju unutar regije. Rad nudi interdisciplinarni pristup koji spaja ekonomske, sigurnosne, jezične i tehnološke perspektive, s ciljem oblikovanja preporuka za stvaranje otpornije i sigurnije regionalne gospodarske arhitekture.
U ovom radu je primijenjen kvalitativni, komparativni pristup koji uključuje sustavni pregled literature, analizu nacionalnih strategija i institucionalne studije slučaja relevantne za regiju jugoistočne Europe.

Ključne riječi: geopolitička stabilnost, kibernetička sigurnost, regionalni razvoj

1. Uvod

U sve digitaliziranijem svijetu, kibernetička sigurnost postala je temelj ekonomske otpornosti, posebno u regijama obilježenim institucionalnom fragmentacijom i geopolitičkim napetošću. Jugoistočna Europa, koja uključuje Hrvatsku i susjedne zemlje, suočava se s jedinstvenim izazovima u usklađivanju nacionalnih infrastruktura kibernetičke sigurnosti sa širim ciljevima regionalnog razvoja. Iako je Europska unija (EU) uvela sveobuhvatne regulatorne okvire poput Zakona o kibernetičkoj otpornosti (Europska komisija, 2024), njihova provedba ostaje neujednačena u navedenoj regiji.

Kibernetička sigurnost često se shvaća kao isključivo tehničko pitanje, ali njezina uloga u poticanju ekonomske stabilnosti, atraktivnosti ulaganja i inovacijskog potencijala proteže se dalje od samog IT protokola. Prema Sulichu i suradnicima (2021), kibernetička sigurnost mora se shvatiti kao višedimenzionalni izazov koji uključuje institucionalne kapacitete, mehanizme izgradnje povjerenja i adaptivno upravljanje. Cilj ovog

istraživanja jest istražiti kako institucionalne i geopolitičke dimenzije utječu na sposobnost regije da koordinira kibernetičke politike i poboljša prekograničnu gospodarsku suradnju.

Iako su prethodna istraživanja temeljito ispitala politike kibernetičke sigurnosti na razini EU (Bendiek i Bund, 2023), manje je pozornosti posvećeno tome kako ti okviri funkcioniraju u regijama s nižim institucionalnim povjerenjem i izraženim jezičnim barijerama. Ovaj rad rješava taj nedostatak predlažući interdisciplinarnu perspektivu koja kombinira ekonomske, institucionalne i geopolitičke uvide u analizu otpornosti kibernetičke sigurnosti.

2. Metodologija

Istraživanje ovoga rada predlaže kvalitativni, komparativni pristup ispitivanju spremnosti za kibernetičku sigurnost i mehanizama regionalne koordinacije u jugoistočnoj Europi. Prvenstveno, proveden je sustavni pregled literature korištenjem relevantnih akademskih baza podataka poput Scopusa, Web of Science i Science Directa, s naglaskom na recenzirane znanstvene članke objavljene između 2015. i 2024. godine.

Polazeći od ciljeva istraživanja, rad se temelji na sljedećim istraživačkim pitanjima: (1) Kako institucionalni kapaciteti i razina povjerenja među državama regije utječu na učinkovitost koordinacije u području kibernetičke sigurnosti? (2) U kojoj mjeri nacionalne strategije kibernetičke sigurnosti doprinose privlačenju ulaganja i inovacijskom potencijalu regije? (3) Kako jezične i regulatorne barijere oblikuju prekograničnu suradnju u upravljanju kibernetičkom sigurnošću?

Drugo, provedena je analiza politika usporedbom nacionalnih strategija kibernetičke sigurnosti iz Hrvatske i nekoliko susjednih zemalja s direktivama EU-a, poput NIS2 i Zakona o kibernetičkoj otpornosti. Analizirani su ključni dokumenti s obzirom na njihovu usklađenost s regionalnim ciljevima i institucionalnim kapacitetima.

Treće, institucionalne studije slučaja preuzete su iz aktivnosti regionalnih projekata poput CyberSEE projekata Vijeća Europe i EU-a, koji promiču kibernetičku koordinaciju i razmjenu znanja (Vijeće Europe, 2024).

Ograničenja ovog istraživanja uključuju nedostatak empirijskih podataka za sve zemlje u regiji, jezične pristranosti u dostupnosti literature i brzo promjenjivu prirodu zakonodavstva EU u području kibernetičke sigurnosti.

3. Pregled literature

Kibernetička sigurnost je disciplina koja se još uvijek razvija na presjeku informacijske tehnologije, prava, upravljanja i ekonomske politike. Europska komisija (2024) naglašava kako je kibernetička otpornost ključna za zaštitu, ne samo digitalne imovine, već i demokratskih institucija i ekonomske infrastrukture. Međutim, prijelaz s politike i *slova na papiru* na praksu ostaje neravnomjeran među regijama, posebno u jugoistočnoj Europi.

Prema Sulichu i suradnicima (2021), otpornost u kibernetičkoj sigurnosti treba promatrati kao dinamičan sustav sposoban predvidjeti, apsorbirati i prilagoditi se digitalnim prijetnjama. Njihov model, koji se sastoji od otkrivanja, odgovora, prilagodbe i učenja, pruža korisnu analitičku perspektivu, iako zahtijeva regionalnu prilagodbu na temelju institucionalne spremnosti.

Bendiek i Bund (2023) tvrde da je regulatorni pristup EU prvenstveno namijenjen državama članicama s jakim administrativnim kapacitetima, a to može predstavljati izazove za manje razvijena institucionalna okruženja. Ovakva regulatorna neusklađenost

postaje još izraženija pri ispitivanju prekograničnih digitalnih rizika, posebno onih povezanih s kritičnom infrastrukturom i tokovima podataka.

Odebade i Benkhelifa (2023) ističu razlike u nacionalnim strategijama kibernetičke sigurnosti, napominjući da mnoge zemlje usvajaju okvire visoke razine bez specificiranja metrika provedbe. U regijama s ograničenim fiskalnim i ljudskim kapitalom, ovi nedostaci mogu rezultirati *papirnatom usklađenošću*, odnosno formalnim usvajanjem politika bez odgovarajućih operativnih kapaciteta.

Khan i suradnici (2024) u *Cybersecurity as a geopolitical tool* analiziraju kako države upotrebljavaju kibernetičke napade i digitalnu sabotažu kao instrument geopolitičke strategije – što može pogoršati nesigurnost i nestabilnost, osobito u geopolitički napetim regijama poput Zapadnog Balkana.

Još jedna zanemarena dimenzija je jezična interoperabilnost, koju Diplomacy.edu i DCAF (2016) identificiraju kao ključnu prepreku u regionalnoj suradnji. Dostupnost obuke za kibernetičku sigurnost i tehničkih standarda na materinskim jezicima je ograničena, što često dovodi do isključenja manjih gospodarstava ili država izvan EU iz ključnih inicijativa.

Nadalje, Kalisz (2023) naglašava ulogu javno-privatnih partnerstava (JPP) u izgradnji kibernetičke otpornosti. Njegovo istraživanje sugerira da lokalni ekosustavi u kojima surađuju poduzeća, akademska zajednica i vlade mogu značajno poboljšati izgradnju operativnih kapaciteta. Međutim, takvi su modeli još uvijek nerazvijeni u jugoistočnoj Europi, gdje je povjerenje u javne institucije često nisko.

Konačno, OECD (2022) izvještava da mala i srednja poduzeća (MSP) ostaju vrlo ranjiva zbog ograničene svijesti i nedovoljnih ulaganja u kibernetičku sigurnost. Navedeno je posebno problematično s obzirom na to da MSP-ovi čine gospodarsku okosnicu mnogih zemalja jugoistočne Europe, a što ih čini i metama i slabim karikama u lancu kibernetičke obrane.

4. Rezultati i rasprava

Nalazi ovog istraživanja ističu složen odnos između kibernetičke sigurnosti i regionalne ekonomske otpornosti, posebno u jugoistočnoj Europi. U zemljama poput Hrvatske, Slovenije i Srbije, strategije kibernetičke sigurnosti postoje na papiru, ali praktična provedba znatno varira zbog institucionalnih ograničenja, nedostatka povjerenja u institucije i ekonomskih asimetrija.

Kako tvrde Sulich i sur. (2021), kibernetičku sigurnost ne može se promatrati isključivo kroz prizmu nacionalne obrane, već ona mora biti ugrađena u ekonomsku politiku kao sistemski faktor rizika. To se posebno odnosi na posttranzicijska gospodarstva, gdje je digitalna infrastruktura često nedovoljno financirana, a institucije se suočavaju s izazovima u međusektorskoj koordinaciji.

Kritična ranjivost je niska uključenost MSP-ova u nacionalne inicijative za kibernetičku sigurnost. Prema OECD-u (2022), malim i srednjim poduzećima u jugoistočnoj Europi često nedostaju resursi i svijest za provedbu čak i osnovnih protokola kibernetičke sigurnosti. Navedeni nedostatak pripremljenosti izlaže cijele lance opskrbe riziku, posebno u prekograničnoj trgovini i digitalnim uslugama. Nedostatak ciljane podrške za MSP u nacionalnim strategijama (primjerice, financiranje obuke, pojednostavljeni mehanizmi usklađenosti) odražava jaz između namjere politike i ekonomske strukture (OECD, 2022, 2023).

Nadalje, JPP koja su se pokazala učinkovitima u provedbi politike

kibernetičke sigurnosti u zapadnoj Europi još uvijek su nerazvijena u regiji. Kalisz (2023) naglašava da su povjerenje, pravna jasnoća i uzajamna korist preduvjeti za uspješna JPP-a. Međutim, na Zapadnom Balkanu, povijesno nepovjerenje između privatnih aktera i vlada često potkopava tu suradnju; što dovodi do fragmentiranih napora i dupliciranih sustava, a ne do koherentnih, isplativih obrana.

Druga dimenzija zabrinutosti je nedostatak operativne interoperabilnosti između nacionalnih institucija, posebno timova za odgovor na računalne hitne slučajeve (CERT), što ometa koordinirane odgovore na kibernetičke incidente. Čak i kada zemlje dijele geopolitičke interese, razlike u regulatornim okvirima, tehničkim kapacitetima i jeziku ometaju suradnju u stvarnom vremenu (Diplomacy.edu i DCAF, 2016). Ove se prepreke pojačavaju tijekom kriza, a gdje su učinkovita komunikacija i povjerenje u zajedničke protokole ključni.

Što se tiče institucionalne spremnosti, Slovenija se ističe integriranim pristupom koji povezuje akademska istraživanja, industrijske partnere i javne institucije u jedinstveni okvir kibernetičke sigurnosti (Sulich i sur., 2021). Hrvatska je ostvarila napredak kroz Strategiju kibernetičke sigurnosti 2022. – 2026., no njezina provedba ostaje fragmentirana, posebice u pogledu međuagencijske koordinacije i angažmana dionika.

Kibernetička sigurnost također utječe na investicijsku klimu u regiji. Kao što su primijetili Osula i Rõigas (2017), investitori sve više procjenjuju kibernetičko upravljanje zemlje kao dio svoje analize rizika. Zemlje s transparentnim politikama, učinkovitom provedbom i međunarodnom suradnjom doživljavaju se kao sigurnija okruženja za digitalna ulaganja i inovacije. Suprotno tome, nedosljedni ili nerazvijeni okviri izazivaju zabrinutost zbog zaštite podataka, kontinuiteta poslovanja i pravnih sredstava.

Na kraju, pitanje jezične fragmentacije dodatno pogoršava regionalnu kibernetičku ranjivost. Različiti jezici, terminologija i administrativne tradicije predstavljaju prepreke standardiziranoj kriznoj komunikaciji i usklađenom regulatornom usklađivanju (Diplomacy.edu i DCAF, 2016). Navedeno može odgoditi ili iskriviti komunikaciju tijekom kibernetičkog incidenta, što zauzvrat utječe na ekonomsku stabilnost.

Ova istraživanja i njihovi zaključci sugeriraju da se kibernetička sigurnost više ne bi trebala tretirati kao sekundarno pitanje, već kao strateški prioritet za regionalnu otpornost. Integrirani pristup; onaj koji uključuje mala i srednja poduzeća, promiče javno-privatno povjerenje i potiče prekograničnu suradnju, mogao bi uvelike ojačati i ekonomsku i institucionalnu snagu u jugoistočnoj Europi.

Odgovori na postavljena istraživačka pitanja proizašli su iz analize literature i institucionalnih dokumenata. Prvo, institucionalni kapaciteti i razina međusobnog povjerenja uvelike određuju učinkovitost koordinacije kibernetičkih politika: zemlje s jačim administrativnim okvirima i razvijenim modelima javno-privatne suradnje (poput Slovenije) pokazuju bolju implementaciju sigurnosnih protokola. Drugo, nacionalne strategije koje sadrže konkretne mehanizme potpore malim i srednjim poduzećima te koje promiču transparentnu komunikaciju o rizicima kibernetičke sigurnosti pozitivno utječu na percepciju investicijskog rizika, čime postaju konkurentnije na regionalnoj razini. Treće, jezične razlike, regulatorne neusklađenosti i tehnička neujednačenost među državama značajno otežavaju uspostavu učinkovitih prekograničnih mehanizama suradnje, što se posebice očituje u

nedostatku interoperabilnosti CERT timova i slaboj operativnoj integraciji u kriznim situacijama.

4. Zaključak

Ovaj rad istražio je ulogu kibernetičke sigurnosti u jačanju regionalne ekonomske otpornosti kroz interdisciplinarnu prizmu koja kombinira ekonomske, institucionalne i geopolitičke perspektive. Zaključci pokazuju kako kibernetička sigurnost nije samo tehničko ili obrambeno pitanje, već i strukturna komponenta održivog razvoja u jugoistočnoj Europi. Slaba institucionalna koordinacija, niska uključenost MSP-a i ograničeno prekogranično povjerenje ključne su ranjivosti koje smanjuju spremnost regije za kibernetičke prijetnje.

Analiza istraživačkih pitanja pokazuje da institucionalna spremnost i razina povjerenja među dionicima predstavljaju temeljne preduvjete za uspješnu koordinaciju kibernetičke sigurnosti u regiji. Strategije koje uključuju konkretne mjere za MSP-ove, kao i transnacionalnu usklađenost s EU direktivama, djeluju kao čimbenici jačanja regionalne privlačnosti za ulagače. Međutim, složenost jezičnih i regulatornih barijera zahtijeva dodatne napore u izgradnji operativnih mehanizama suradnje, osobito u kriznim okolnostima kada brzina i jasnoća komunikacije postaju ključne. Stoga, daljnji razvoj regionalne otpornosti mora se temeljiti na jačanju institucionalne interoperabilnosti i uspostavi zajedničkih protokola djelovanja.

Da bi kibernetička sigurnost postala pravi pokretač regionalnog gospodarskog razvoja, mora biti ugrađena u šire strategije digitalne transformacije, privlačenja ulaganja i inovacijske politike. Jačanje javno-privatnog povjerenja, usklađivanje koordinacije CERT-a i izgradnja uključivih institucionalnih okvira nužni su koraci prema otpornijoj regionalnoj ekonomskoj arhitekturi.

Izvorni doprinos ovog istraživanja leži u naglasku na ekonomskim implikacijama kibernetičke sigurnosti kao faktora regionalnog razvoja, jer naglašava hitnost usklađivanja upravljanja kibernetičkom sigurnošću s izgradnjom institucionalnih kapaciteta i geopolitičkom suradnjom, posebno u digitalno povezanim, ali politički fragmentiranim regijama.

Buduća istraživanja trebala bi dodatno istražiti operativne stvarnosti kibernetičke sigurnosti u jugoistočnoj Europi putem empirijskih metoda, uključujući ankete i intervjue s institucionalnim akterima i MSP-ovima. Poseban naglasak trebalo bi staviti na procjenu učinkovitosti javno-privatnih partnerstava, jezičnih barijera u prekograničnoj koordinaciji i uloge kibernetičkog upravljanja u privlačenju stranih ulaganja. Razvoj regionalnog indeksa otpornosti na kibernetičku sigurnost i analiza uspješnih studija slučaja (poput slovenskog integrativnog modela) mogli bi pružiti prenosive strategije za jačanje institucionalne i ekonomske otpornosti u cijeloj regiji.

5. Literatura

Bendiek, A., & Bund, J. (2023). Shifting paradigms in Europe's approach to cyber defence: ambitions to disrupt malicious cyber activity need to protect norms as well as networks.

Diplomacy.edu & DCAF (2016). Cybersecurity in the Western Balkans: Policy gaps and cooperation. Geneva Centre for the Democratic Control of Armed Forces. https://www.diplomacy.edu/resource/cybersecurity-western-balkans-policy-gaps-cooperation/

Europska komisija (2024). Regulation (EU) 2024/2847 on Cyber Resilience Act. Official Journal of the European Union.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847

Kalisz, A. (2023). Public-Private Partnerships on Cybersecurity and International Law: Finding Multilateral Solutions. In Symposium on'Public and Private Governance of Cybersecurity: Challenges and Potential'. Cambridge University Press.

Khan, A. W., Saeed, S., & Kakar, M. S. (2024). CYBERSECURITY AS A GEOPOLITICAL TOOL: THE GROWING INFLUENCE OF DIGITAL WARFARE IN STATECRAFT. International Research Journal of Social Sciences and Humanities, 3(2), 345-357.

OECD (2022). OECD Policy Framework on Digital Security, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en

OECD (2023).NEW PERSPECTIVES ON MEASURING CYBERSECURITY. OECD DIGITAL ECONOMY PAPERS. Dostupno na: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/new-perspectives-on-measuring-cybersecurity_6069c1b9/b1e31997-en.pdf (pristupljeno: 4.6.2025.)

Odebade, A. T., & Benkhelifa, E. (2023). A comparative study of national cyber security strategies of ten nations. arXiv preprint arXiv:2303.13938.

Osula, A. M., & Rõigas, H. (2017). International Cyber Norms: Legal, Policy & Industry Perspectives. NATO Cooperative Cyber Defence Centre of Excellence.

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski , J., Zema, T. (2021). Cybersecurity and Sustainable Development.Procedia Computer Science. https://doi.org/10.1016/j.procs.2021.08.003

Vijeće Europe (2024). CyberSEE: Enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye – Project Summary and Activity Report. Council of Europe. Dostupno na: https://www.coe.int/en/web/cybercrime/cybersee (pristupljeno: 5.6.2025.)

THE ROLE OF CYBERSECURITY IN STRENGTHENING REGIONAL ECONOMIC RESILIENCE: INSTITUTIONAL AND GEOPOLITICAL PERSPECTIVES

Abstract: This paper explores the role of security and cybersecurity within a broader analysis of the regional economy of Southeast Europe, with a focus on the geopolitical and societal challenges that shape economic processes in Croatia and neighboring countries. In an increasingly digitalized economy, security infrastructure—including the protection of information systems, data, and communication channels—has become a key prerequisite for sustainable regional development, economic stability, and cross-border cooperation.

Cybersecurity is examined not only as a technical requirement, but also as an element closely linked to institutional capacities, security protocols, and the level of mutual trust among countries in the region. Language barriers further complicate the harmonization of security measures and crisis communication, increasing the risk of digital fragmentation within a space striving for integration.

The paper analyzes how varying levels of cyber resilience and security policies among countries affect investment attractiveness, innovation collaboration, and digital transformation across the region. An interdisciplinary approach is applied, combining economic, security, linguistic, and technological perspectives, with the aim of formulating recommendations for building a more resilient and secure regional economic architecture.

In this paper, a qualitative, comparative approach is applied, which includes a systematic literature review, analysis of national strategies and institutional case studies relevant to the region of Southeast Europe.

Keywords: cybersecurity, regional development, geopolitical stability