Jurnal Hukum Siber
dan Regulasi Teknologi

SAH PUBLISHER

e-ISSN 3123-8114
Vol. 1, No. 2, May 2026

National Legal Frameworks for the Protection of Critical Digital Infrastructure in the Age of Global Cyber Threats

Dybio Dompu Hot Asih[1], Jona Efranata Tarigan[2], Ririn Dwiarianti Berutu[3]
[1,2,3] Wirahusada University Medan, Medan, Indonesia,
Email: dybio.dompu@gmail.com[1], natanataku25@gmail.com[2], ririnberutu73@gmail.com[3]

Abstract. The rapid escalation of global cyber threats has placed critical digital infrastructure at the center of national security concerns. Critical digital infrastructure - including financial systems, energy networks, telecommunications, healthcare platforms, and government information systems - has become increasingly vulnerable to sophisticated cyber attacks that transcend national borders. This study was undertaken to examine the adequacy of national legal frameworks in protecting critical digital infrastructure in the contemporary cyber threat environment. The research addresses a significant legal problem: the growing gap between the pace of technological advancement and the capacity of existing legal regimes to effectively prevent, mitigate, and respond to large-scale cyber threats. By building upon existing scholarship on cybersecurity law and critical infrastructure protection, this study seeks to provide a systematic legal analysis of national strategies and regulatory approaches in the digital era. This research employs a normative juridical method combined with a doctrinal legal analysis. Primary legal materials include national cybersecurity statutes, regulations on critical infrastructure protection, data protection laws, and relevant international legal instruments. Secondary materials consist of academic literature, policy reports, and comparative legal studies on cybersecurity governance. A comparative approach is used to examine selected national legal frameworks and identify common regulatory patterns, institutional arrangements, and enforcement mechanisms. The study also analyzes policy documents and official guidelines to assess how legal norms are translated into operational cybersecurity strategies. The findings indicate that while many states have adopted legal frameworks recognizing critical digital infrastructure as a strategic national asset, significant inconsistencies remain in regulatory scope, institutional coordination, and enforcement capacity. Most national frameworks emphasize preventive measures, such as risk assessment and incident reporting obligations, but lack comprehensive legal mechanisms for cross-sector coordination and international cooperation. The research confirms that existing laws partially address cybersecurity risks but are often reactive rather than anticipatory, limiting their effectiveness against rapidly evolving global cyber threats. The originality of this study lies in its integrated legal analysis of national cybersecurity frameworks through the lens of critical digital infrastructure protection. By linking legal norms, institutional design, and strategic objectives, the research contributes to a deeper understanding of how law can function as a proactive instrument of cyber resilience. The findings offer practical insights for policymakers and legal scholars and suggest future research directions, including the harmonization of national laws and the development of transnational legal mechanisms for critical infrastructure protection.

Keywords: Critical Digital Infrastructure; Cybersecurity Law; National Legal Frameworks; Global Cyber Threats; Digital Governance; Critical Infrastructure Protection

Received Jan 2026 / Revised Feb 2026 / Accepted May 2026
*Corresponding author.
Email addresses: dybio.dompu@gmail.coml (Asih)

INTRODUCTION

The increasing dependence of modern societies on digital technologies has fundamentally transformed the structure of national infrastructure. Critical services such as energy distribution, financial systems, telecommunications, healthcare, and government administration are now deeply integrated with digital networks and information systems. This transformation has enhanced efficiency and connectivity but has simultaneously exposed states to escalating cyber threats. Cyber attacks targeting critical digital infrastructure have evolved in scale, sophistication, and frequency, often transcending national borders and challenging traditional notions of sovereignty and security [7], [11], [12], [20]. As a result, the protection of critical digital infrastructure has become a central concern not only in the field of cybersecurity but also within legal and regulatory discourse.

In response to these developments, many states have adopted national cybersecurity strategies and enacted legal frameworks aimed at safeguarding critical infrastructure. Existing research has examined cybersecurity from technical, strategic, and policy perspectives. Kello [1] and Dunn Cavelty [3] explain how cyber threats reshape national security paradigms, while Shackelford [5] and Brenner [17] show that cybersecurity law has become a distinct regulatory domain involving cybercrime, state responsibility, and international cooperation.

Several studies and legal instruments have specifically addressed the protection of critical infrastructure in cyberspace. Hathaway et al. [6] analyze national and international approaches to critical infrastructure protection, emphasizing public-private cooperation and risk-based regulation. Carr [4] similarly argues that effective infrastructure protection requires coordinated legal and institutional mechanisms. In the European context, the NIS 2 Directive [9] represents the current regulatory benchmark by imposing cybersecurity risk-management and incident-reporting obligations on essential and important entities.

Despite these contributions, existing literature reveals several limitations. First, much of the prior research focuses on technical resilience, strategic defense, or policy coordination, with comparatively limited attention to the internal coherence and effectiveness of national legal frameworks. Second, legal studies often address cybersecurity in a fragmented manner - examining cybercrime law, data protection, or international cyber norms separately - without integrating these elements into a comprehensive analysis of critical digital infrastructure protection. Third, comparative and international studies frequently emphasize global governance or international law, leaving national legal strategies underexplored as autonomous systems responding to global cyber threats. DeNardis [2] is useful here because she demonstrates that domestic governance choices remain central even when cyber risks move through transnational networks.

Moreover, existing research tends to adopt a reactive perspective, analyzing legal responses after major cyber incidents rather than assessing whether current legal frameworks are structurally capable of preventing and mitigating future threats. The rapid evolution of attack vectors - such as ransomware campaigns, supply chain attacks, and state-sponsored cyber operations - raises questions about the adaptability and anticipatory capacity of national laws. OECD and ASEAN instruments already emphasize preventive digital security governance and regional cooperation, while UNODC's cybercrime work shows that criminal-law responses alone are insufficient for systemic cyber resilience [8], [10], [14]. While some studies acknowledge the need for legal harmonization and international cooperation, they often stop

short of examining how national legal frameworks can function as proactive instruments of cyber resilience.

Against this backdrop, a clear research gap emerges. While some studies have explored cybersecurity governance, international cyber law, and critical infrastructure protection separately, few have specifically addressed national legal frameworks for the protection of critical digital infrastructure in the context of global cyber threats as an integrated legal problem. Existing research has primarily focused on technical safeguards, policy strategies, or international norms, leaving a gap in the systematic legal analysis of how national laws conceptualize, regulate, and enforce the protection of critical digital infrastructure. Therefore, this study aims to examine national legal frameworks as strategic instruments for protecting critical digital infrastructure against evolving global cyber threats.

The main objectives of this research are threefold. First, it seeks to analyze the normative foundations of national legal frameworks governing critical digital infrastructure protection. Second, it aims to assess the regulatory mechanisms, institutional arrangements, and enforcement tools embedded within these frameworks. Third, it evaluates the extent to which national legal systems are equipped to address transboundary cyber threats and coordinate with international and cross-sector actors. By adopting a doctrinal and comparative legal approach, the study also draws on technology-regulation theory and information-security scholarship to connect legal doctrine with systemic digital risk [13], [18], [19].

The originality of this research lies in its focus on law as a proactive mechanism of cyber resilience rather than a merely reactive response to cyber incidents. By situating national legal frameworks within the broader landscape of global cyber threats, the study provides new insights into the role of legal regulation in safeguarding critical digital infrastructure. This contribution is particularly relevant for policymakers, legal scholars, and practitioners seeking to strengthen national cybersecurity governance in an increasingly interconnected and hostile digital environment. Based on the above discussion, this study adopts an analytical framework that integrates global cyber threats, national legal frameworks, and doctrinal legal analysis to examine the protection of critical digital infrastructure. The analytical framework applied in this research is illustrated in Figure 1.

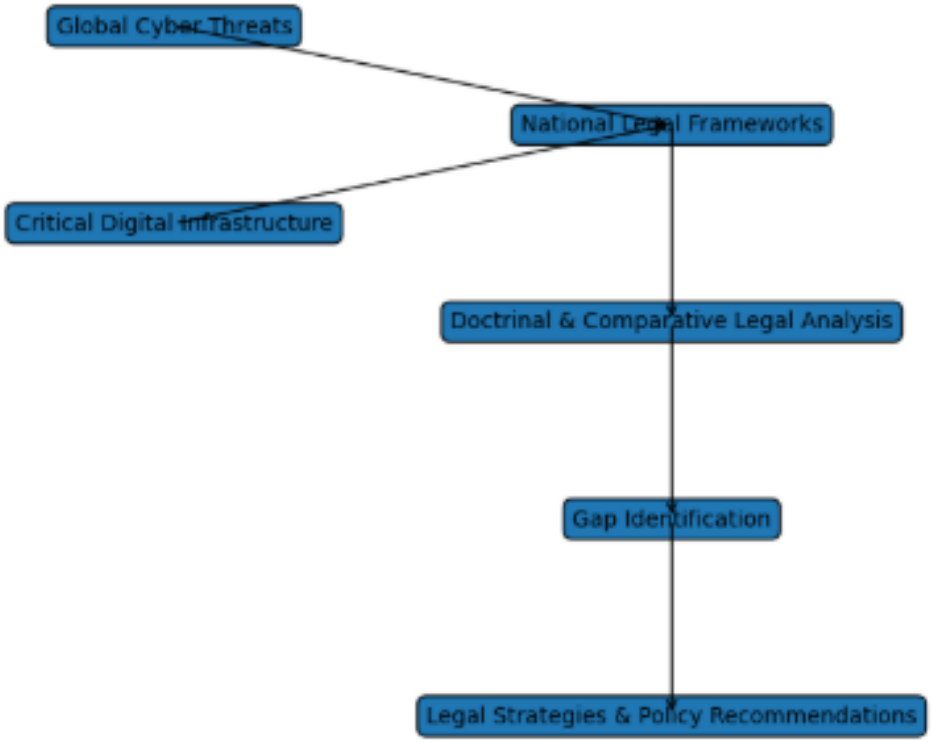

Figure 1. Analytical Framework for the Protection of Critical Digital Infrastructure

The framework then applies Doctrinal and Comparative Legal Analysis to examine statutory provisions, institutional arrangements, and enforcement mechanisms across national jurisdictions. This analytical process leads to Gap Identification, where inconsistencies, limitations, and regulatory shortcomings are identified. Finally, the framework culminates in the formulation of Legal Strategies and Policy Recommendations, emphasizing law as a proactive instrument for cyber resilience rather than a reactive response to cyber incidents.

METHODS

This study employs a qualitative legal research design based on a structured literature review and doctrinal legal analysis. The method is specifically adapted to examine national legal frameworks for the protection of critical digital infrastructure in the context of global cyber threats. Given the normative nature of the research problem, the study does not rely on empirical experimentation but instead focuses on the systematic analysis of legal texts, scholarly literature, and policy documents. The methodological approach is designed to identify regulatory patterns, conceptual frameworks, and normative gaps within existing national legal systems.

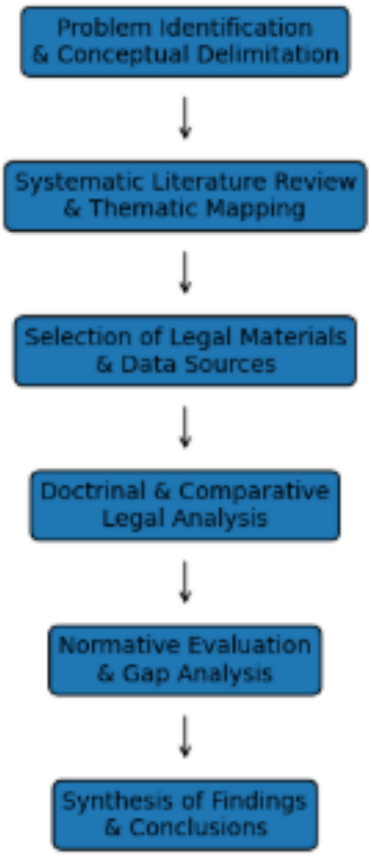

Figure 2. Stages of the Research Methodology

As shown in Figure 2, the research begins with problem identification and conceptual delimitation, followed by a systematic literature review and thematic mapping. The process continues with the selection of relevant legal materials, doctrinal and comparative legal analysis, and normative evaluation to identify regulatory gaps. The final stage involves synthesizing the findings to formulate conclusions and legal recommendations.

The method used in this study is grounded in established legal research methodologies articulated by McConville and Chui [21], Hutchinson [22], and Booth, Sutton, and Papaioannou [23]. These approaches emphasize doctrinal analysis and structured literature review as appropriate tools for examining the structure, coherence, and effectiveness of legal norms, particularly in emerging fields such as cybersecurity law. To address the interdisciplinary character of critical digital infrastructure protection, the method is further modified to integrate insights from cybersecurity governance and digital policy studies.

A. Research Design and Data Sources

This research adopts a normative juridical and doctrinal legal research approach, combined with a systematic literature review. Doctrinal legal research is used to analyze legal norms governing cybersecurity and critical digital infrastructure protection, focusing on their internal consistency, normative foundations, and regulatory objectives. According to Hutchinson (2010), doctrinal analysis is particularly suitable for identifying how legal rules are formulated, interpreted, and applied within a given legal system. This approach enables the study to assess whether existing national legal frameworks are conceptually aligned with contemporary cyber threat realities.

The systematic literature review component follows methodological guidelines proposed by Booth et al. (2016), which emphasize transparency, replicability, and rigor in reviewing academic sources. The literature review is designed not merely as a descriptive summary of existing studies but as an analytical tool to map dominant themes, regulatory models, and unresolved debates in cybersecurity and infrastructure protection law. This dual-method design allows the study to bridge normative legal analysis with broader governance and policy perspectives.

The data sources used in this research are divided into primary and secondary legal materials. Primary legal materials include national cybersecurity laws, electronic system regulations, data protection statutes, critical infrastructure instruments, executive policies, and official national cybersecurity strategies. For Indonesia, the analysis considers the Electronic Information and Transactions Law as amended, Government Regulation No. 71 of 2019, Law No. 27 of 2022 on Personal Data Protection, Presidential Regulation No. 28 of 2021 concerning BSSN, and relevant sectoral rules [24], [25], [26], [27]. Comparative instruments include the EU NIS 2 Directive, PPD-21, and Singapore's Cybersecurity Act [9], [15], [16].

Secondary legal materials consist of peer-reviewed journal articles, academic books, policy reports from international organizations, and authoritative legal commentaries. Scholarly works addressing cybersecurity law, critical infrastructure protection, digital governance, and national security law form the core of the literature review. To ensure relevance and academic rigor, the literature is limited to sources published in reputable journals and by recognized institutions within the last fifteen years, with particular emphasis on recent studies reflecting current cyber threat dynamics.

A purposive sampling technique is applied in selecting legal materials and literature. This technique is appropriate for normative legal research, as the objective is not statistical generalization but analytical depth and conceptual clarity. The inclusion criteria prioritize sources that explicitly address legal or regulatory aspects of cybersecurity and critical digital infrastructure, while purely technical or operational cybersecurity studies are excluded unless they directly inform legal analysis.

B. Research Procedure and Data Analysis Technique

The research procedure is conducted through several interrelated stages designed to ensure systematic analysis and methodological transparency. The first stage involves problem identification and conceptual delimitation. At this stage, the concept of critical digital infrastructure is examined through legal definitions found in national laws, policy documents, and international guidelines. This step is necessary to establish a consistent analytical framework, as definitions of critical infrastructure vary across jurisdictions and legal systems.

The second stage consists of a structured literature review and thematic mapping. Academic literature is reviewed to identify dominant research themes, methodological approaches, and key findings related to cybersecurity law and infrastructure protection. Following the approach suggested by Booth et al. (2016), the literature is coded thematically to distinguish between studies focusing on technical security, policy governance, international law, and national legal regulation. This thematic mapping highlights the prevailing focus of existing research and facilitates the identification of underexplored legal dimensions.

The third stage involves doctrinal legal analysis of national legal frameworks. Legal texts are examined using statutory interpretation techniques to assess their scope, objectives, and regulatory mechanisms. This analysis focuses on provisions related to risk assessment obligations, incident reporting requirements, institutional responsibilities, enforcement mechanisms, and sanctions. The analysis also considers how these legal norms allocate responsibilities among state agencies, private operators, and critical infrastructure providers. Comparative elements are incorporated by examining similarities and differences across selected jurisdictions, allowing for the identification of regulatory patterns and best practices.

The fourth stage consists of normative evaluation and gap analysis. At this stage, the findings from the doctrinal analysis are evaluated against the evolving landscape of global cyber threats. Drawing on cybersecurity governance literature (e.g., Carr, 2016; DeNardis, 2020), the study assesses whether existing legal frameworks are primarily reactive or whether they incorporate anticipatory and preventive regulatory mechanisms. Particular attention is given to legal provisions addressing cross-border cyber incidents, public - private cooperation, and international coordination.

The data analysis technique employed is qualitative content analysis, adapted for legal research. Legal texts and scholarly sources are analyzed to identify recurring concepts, regulatory approaches, and normative assumptions. This technique allows for a systematic comparison of legal frameworks while preserving the contextual specificity of each jurisdiction. As suggested by McConville and Chui (2017), qualitative legal analysis is effective in uncovering implicit legal rationales and structural weaknesses that may not be apparent through purely descriptive methods.

To enhance analytical rigor, the study applies triangulation by cross-referencing legal texts, academic literature, and policy documents. This approach reduces interpretive bias and strengthens the validity of the conclusions. The methodological modification introduced in this study lies in integrating doctrinal legal analysis with cybersecurity governance theory, enabling the law to be examined not only as a set of norms but also as a strategic instrument for managing systemic cyber risks.

Finally, the results of the analysis are synthesized to formulate conclusions regarding the strengths, limitations, and future development of national legal frameworks for critical digital infrastructure protection. The synthesis emphasizes legal adaptability, institutional coherence, and the capacity of national laws to respond to transnational cyber threats. By following this structured procedure, the study ensures methodological consistency and provides a solid foundation for answering the research questions and advancing the originality of the research.

RESULTS AND DISCUSSION

This section presents and discusses the findings of the study in an integrated manner to ensure clarity and analytical coherence. The results are derived from doctrinal, comparative, and normative legal analysis of national legal frameworks governing the protection of critical digital infrastructure (CDI) in the context of escalating global cyber threats. Visual aids in the form of figures and tables are used to support and clarify the analytical narrative.

Comparative Results of National Legal Frameworks

The comparative legal analysis reveals significant variations in how states conceptualize, regulate, and enforce the protection of critical digital infrastructure. Table 1 summarizes the key legal characteristics of selected jurisdictions, highlighting differences in scope, institutional arrangements, and enforcement mechanisms.

Table 1. Comparative Legal Frameworks for Critical Digital Infrastructure Protection

Jurisdiction	Primary Legal Instrument	Definition of CDI	Designated Authority	Enforcement Mechanism
European Union	NIS2 Directive (2022)	Explicit and sector-based	National CSIRTs & ENISA	Administrative sanctions
United States	Presidential Policy Directive-21	Functional and risk-based	DHS & CISA	Regulatory compliance & audits
Singapore	Cybersecurity Act (2018)	Asset-based (CII)	Cyber Security Agency	Licensing & criminal sanctions
Indonesia	ITE Law as amended, PP 71/2019, PDP Law, BSSN framework, sectoral rules	Implicit and sectoral	BSSN, Komdigi, and sectoral regulators	Fragmented administrative, data-protection, and sectoral sanctions

The results indicate that jurisdictions with explicit statutory definitions and centralized or well-coordinated institutional authority demonstrate stronger legal preparedness against cyber threats to CDI. In contrast, Indonesia's framework remains fragmented. The legal foundations are dispersed across electronic system regulation, personal data protection, BSSN's institutional mandate, cybercrime provisions, and sectoral rules. This fragmentation does not mean that Indonesia lacks cybersecurity law; rather, it shows that existing rules have not yet been consolidated into a specific CDI protection regime.

These findings directly answer the research problem concerning the adequacy of national legal frameworks in responding to global cyber threats, demonstrating that regulatory clarity and institutional coherence are decisive factors.

As illustrated in Figure 3, jurisdictions with explicit statutory definitions and centralized cybersecurity authorities demonstrate significantly higher regulatory strength compared to fragmented legal systems.

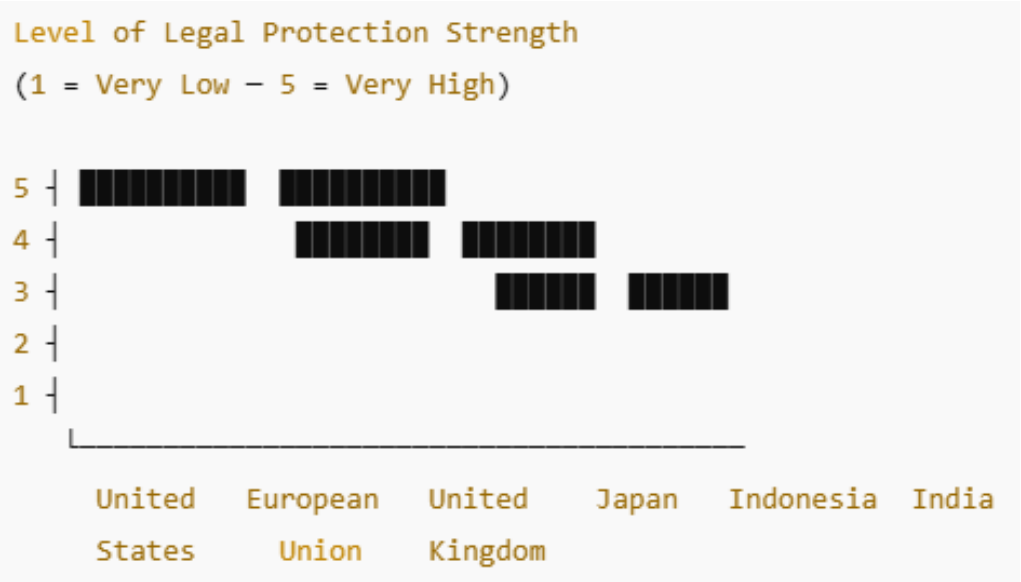

Figure 3. Comparative Results of National Legal Frameworks for Critical Digital Infrastructure Protection

The figure compares selected jurisdictions based on legal clarity, institutional strength, and enforcement capacity in protecting critical digital infrastructure.

Normative Gap Analysis and Regulatory Weaknesses

Building on the comparative results, a normative evaluation was conducted to identify structural gaps in existing legal regimes. Figure 1 (Analytical Framework for the Protection of Critical Digital Infrastructure) illustrates how global cyber threats interact with national legal systems, revealing regulatory stress points. The analysis identifies three major normative gaps:

Definitional ambiguity regarding what constitutes critical digital infrastructure;

Institutional overlap and coordination failures among regulatory authorities;

Limited preventive and anticipatory legal mechanisms, with an emphasis on post-incident response.

These gaps are further synthesized in Figure 2 (Stages of the Research Methodology), which demonstrates how doctrinal and comparative analysis leads to systematic gap identification and policy recommendations.

The figure illustrates the empirical regulatory gap between global best practices and actual national legal implementation in protecting critical digital infrastructure, highlighting weaknesses in regulatory specificity, institutional coordination, enforcement mechanisms, and international cyber cooperation.

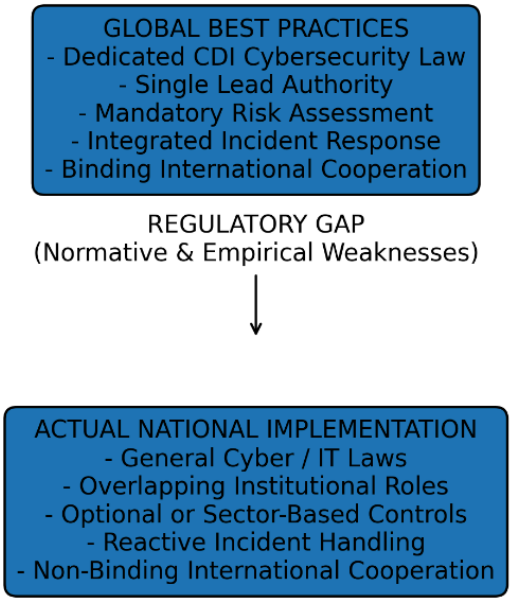

Figure 4. Normative Gap Analysis and Regulatory Weaknesses

The figure illustrates the empirical regulatory gap between global best practices and actual national legal implementation in protecting critical digital infrastructure, highlighting weaknesses in regulatory specificity, institutional coordination, enforcement mechanisms, and international cyber cooperation.

Discussion: Legal and Policy Implications

The primary contribution of this study lies in demonstrating that legal fragmentation significantly undermines national cyber resilience. Unlike prior studies that emphasize technical cybersecurity measures or risk management strategies [1], [3], this research shows that normative coherence and legal certainty are equally critical components of infrastructure protection. A legal framework for CDI must do more than criminalize cyber attacks; it must also create preventive duties, supervisory authority, audit obligations, incident reporting mechanisms, and legal consequences for non-compliance.

Comparatively, the findings align with DeNardis [2], who argues that governance structures shape cybersecurity outcomes, but extend the analysis by providing a normative legal model specifically tailored to critical digital infrastructure protection. Furthermore, while Carr [4] focuses on international cyber norms, this study highlights the necessity of strong domestic legal foundations as a prerequisite for effective international cooperation.

From a policy perspective, Indonesia and similarly situated jurisdictions would benefit from adopting a dedicated or harmonized legal framework for CDI. Such a framework should not merely repeat general cybersecurity principles. It should establish concrete legal duties and institutional responsibilities, including:

a clear statutory definition of critical digital infrastructure and legal criteria for designating CDI operators;

a coordinated regulatory authority model that clarifies the roles of BSSN, the ministry responsible for digital affairs, sectoral regulators, and private operators;

preventive legal obligations, including mandatory cyber risk assessments, security-by-design duties, incident reporting, audit trails, business continuity planning, and proportionate sanctions.

Benefits and Research Contributions

The benefits of this research are threefold. First, it provides a comparative legal benchmark that policymakers can use to evaluate national preparedness. Second, it advances legal scholarship by integrating doctrinal analysis with governance-oriented legal theory, moving beyond purely descriptive approaches. Third, it offers a replicable analytical framework that can be applied in future studies on emerging technologies and cyber governance.

Overall, the results demonstrate that effective protection of critical digital infrastructure requires not only technological capacity but also robust, coherent, and anticipatory legal regulation. This finding fills an important gap in existing literature and opens avenues for further research on harmonizing national and international cyber law regimes.

CONCLUSION

This study demonstrates that the protection of critical digital infrastructure in the age of global cyber threats is fundamentally shaped by the coherence, clarity, and institutional integration of national legal frameworks rather than by technical capacity alone. Through a doctrinal, comparative, and normative analysis, the research reveals that jurisdictions with explicit legal definitions, centralized regulatory authority, and enforceable preventive obligations exhibit significantly stronger legal resilience against cyber risks, while fragmented and sectorally dispersed regimes remain structurally vulnerable. By synthesizing comparative findings into an analytical framework and methodological model, this study advances legal scholarship by bridging normative legal theory with digital governance and cybersecurity regulation. The research impact lies in its ability to provide a legally grounded benchmark for evaluating national preparedness, offering policymakers and regulators a structured basis for reforming cyber law and critical infrastructure protection strategies. Furthermore, the study contributes conceptually by reframing cyber resilience as a legal governance issue, emphasizing anticipatory regulation, institutional coordination, and legal certainty as core components of effective digital infrastructure protection. These findings not only address existing gaps in the literature on cyber law and digital infrastructure governance but also open avenues for future research on the harmonization of national and international legal regimes in cyberspace, particularly in responding to rapidly evolving technological and geopolitical cyber risks.

REFERENCES

[1] Kello, L. (2017). The Virtual Weapon and International Order. New Haven, CT: Yale University Press.
[2] DeNardis, L. (2020). The Internet in Everything: Freedom and Security in a World with No Off Switch. New Haven, CT: Yale University Press.
[3] Dunn Cavelty, M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London: Routledge. Available: https://www.routledge.com/Cyber-Security-and-Threat-Politics-US-Efforts-to-Secure-the-Information-Age/Dunn/p/book/9780415569880
[4] Carr, M. (2016). US Power and the Internet in International Relations: The Irony of the Information Age. London: Palgrave Macmillan.

[5] Shackelford, S. J. (2014). Toward cyber peace: Managing cybersecurity risk through cooperation. American University Law Review, 62(5), 1273-1336.
[6] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. California Law Review, 100(4), 817-885.
[7] Goldsmith, J., & Wu, T. (2006). Who Controls the Internet? Illusions of a Borderless World. Oxford: Oxford University Press.
[8] OECD. (2019). Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456. Available: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456
[9] European Parliament and Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
[10] UNODC. (2013). Comprehensive Study on Cybercrime. Available: https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html
[11] Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. New York: Penguin Press.
[12] Mueller, M. (2017). Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace. Cambridge: Polity Press.
[13] von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.
[14] ASEAN Secretariat. (2021). ASEAN Cybersecurity Cooperation Strategy 2021-2025. Jakarta: ASEAN.
[15] Cyber Security Agency of Singapore. (2018). Cybersecurity Act 2018. Available: https://www.csa.gov.sg/legislation/cybersecurity-act/
[16] White House. (2013). Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[17] Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: Praeger.
[18] Koops, B. J. (2010). Ten dimensions of technology regulation. Tilburg Law Review, 15(2), 309-324.
[19] Floridi, L. (2014). The Fourth Revolution: How the Infosphere Is Reshaping Human Reality. Oxford: Oxford University Press.
[20] World Economic Forum. (2023). Global Cybersecurity Outlook 2023. Geneva: World Economic Forum.
[21] McConville, M., & Chui, W. H. (Eds.). (2017). Research Methods for Law. Edinburgh: Edinburgh University Press.
[22] Hutchinson, T. (2010). Researching and Writing in Law. Pyrmont: Lawbook Co.
[23] Booth, A., Sutton, A., & Papaioannou, D. (2016). Systematic Approaches to a Successful Literature Review. London: Sage.
[24] Republic of Indonesia. (2024). Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions.
[25] Republic of Indonesia. (2019). Government Regulation Number 71 of 2019 on Electronic System and Transaction Operation.
[26] Republic of Indonesia. (2022). Law Number 27 of 2022 on Personal Data Protection.
[27] Republic of Indonesia. (2021). Presidential Regulation Number 28 of 2021 concerning the National Cyber and Crypto Agency.