

STRUCTURAL VULNERABILITY AND INDONESIA'S DIGITAL SOVEREIGNTY AMID TRANSNATIONAL CYBERCRIME: A SYSTEMATIC LITERATURE REVIEW

Pratomo Widodo¹, Puspitasari², Muhamad Sahroni Rofii³, Yudho Giri Sucahyo⁴

¹ Universitas Indonesia, Indonesia

² Universitas Indonesia, Indonesia

³ Universitas Indonesia, Indonesia

⁴ Universitas Indonesia, Indonesia

Corresponding Author:

Pratomo Widodo,
Universitas Indonesia, Indonesia
Jl. Lingkar, Pondok Cina, Kecamatan Beji, Kota Depok, Jawa Barat 16424
Email: pratow37@gmail.com

Article Info

Received: April 10, 2026

Revised: June 11, 2026

Accepted: August 17, 2026

Online Version: October 20, 2026

Abstract

Indonesia faces an exponential surge in cyber threats, evidenced by a 714 percent rise in incidents in 2025 (BSSN) and cases including the Bank Jambi breach, the Brain Cipher ransomware attack on the Temporary National Data Center, and the relocation of regional scam networks from Cambodia, Myanmar, Laos, and Vietnam into Indonesia. This study aims to map the characteristics of these threats and Indonesia's structural vulnerability, evaluate the effectiveness of its cybersecurity oversight and law enforcement policies, and formulate strategies for strengthening digital sovereignty. A systematic literature review following the PRISMA 2020 protocol was employed, searching Scopus, SINTA, Google Scholar, DOAJ, SSRN, and authoritative institutional reports, yielding 50 studies from 370 initially identified records. Results show that structural vulnerability is multidimensional, spanning geographic, demographic, technological, regulatory, and institutional dimensions; policy effectiveness is constrained by institutional fragmentation and weak international legal cooperation; and strengthening digital sovereignty requires integrating structural reform, institutional capacity, regulatory harmonization, and international cooperation. The novelty lies in integrating structural vulnerability, digital sovereignty, and transnational crime theory into one analytical framework for Indonesia, with the implication of guiding future empirical research based on primary stakeholder data.

Keywords: Digital Sovereignty, Structural Vulnerability, Transnational Cybercrime



© 2026 by the author(s)

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).

Journal Homepage

<https://research.adra.ac.id/index.php/Scientechno>

How to cite:

Widodo, P., Puspitasari, Puspitasari., Rofii, S, M & Sucahyo, G, Y. (2026). Structural Vulnerability and Indonesia's Digital Sovereignty Amid Transnational Cybercrime: A Systematic Literature Review. *Scientechno: Journal of Science and Technology*, 5(4), 413–424. <https://doi.org/10.70177/scientechno.v5i4.4493>

Published by:

Yayasan Adra Karima Hubbi

INTRODUCTION

Indonesia's rapid digital transformation has been accompanied by an exponential escalation of cyber threats. Data from BSSN recorded more than 5.5 billion anomalies and cyberattacks throughout 2025, a 714 percent increase over the previous year's baseline, and this trend continued with an additional 1.52 billion incidents between January and April 2026 (BSSN, 2025, 2026). The scale of this threat is no longer incidental but systemic, as reflected in a series of concrete incidents: the breach of Bank Jambi's banking system, which involved the conversion of criminal proceeds into cryptocurrency assets; the Brain Cipher ransomware attack in June 2024, which paralyzed the Temporary National Data Center (PDNS) and affected 239 user institutions; and confirmation from INTERPOL's National Central Bureau (NCB) Indonesia regarding the relocation of international scam operation networks from Cambodia, Myanmar, Laos, and Vietnam into Indonesian territory. This series of incidents places Indonesia in a vulnerable position as a new destination for the relocation of transnational cybercrime operations, a phenomenon that this study understands as a manifestation of structural vulnerability, that is, a systemic condition inherent in a country's geographic, demographic, technological, regulatory, and institutional characteristics, which collectively create conditions conducive to exploitation by criminal actors. In response, the Government of Indonesia is currently drafting the Cyber Security and Resilience Bill (RUU KKS), which on one hand is expected to strengthen national cybersecurity governance, but on the other hand has drawn criticism from civil society groups regarding its potential impact on citizens' digital rights.

Academic research on this phenomenon still exhibits a significant gap. The literature on digital sovereignty is generally conceptual-normative in nature and focuses on the context of developed countries or supranational entities, with limited empirical application to the context of a developing archipelagic state such as Indonesia (Fratini et al., 2024; Robles-Carrillo, 2023; Pohle, 2024), while the literature on transnational organized crime in Southeast Asia is generally descriptive-investigative and has not yet been explicitly linked to the digital sovereignty framework as a unified analytical construct (Jeselyn & Goh, 2025; UNODC, 2024). Indonesia-focused literature, for its part, tends to be sectoral, examining regulatory aspects, institutional aspects, or single-incident case studies in isolation, without integrating them into a comprehensive and multidimensional structural vulnerability framework (Aji, 2022; Chotimah, 2019; Firdaus, 2025). Based on this gap, this study aims to: (1) map the characteristics of transnational cybercrime threats and Indonesia's structural vulnerability based on a synthesis of available literature; (2) evaluate the effectiveness of Indonesia's cybersecurity oversight and law enforcement policies based on findings from prior research; and (3) formulate the direction of strategies for strengthening an adaptive and equitable Indonesian digital sovereignty based on a synthesis of the theoretical framework and policy precedents examined in the literature.

Unlike primary research based on in-depth interviews commonly used in qualitative policy studies, this study specifically employs a systematic literature review (SLR) approach to map and synthesize existing knowledge in a systematic and replicable manner, while simultaneously serving as a conceptual foundation for follow-up research based on primary data. This methodological choice rests on the premise that, before primary data are collected from stakeholders, a thorough and systematic mapping of the knowledge already produced by the academic community and authoritative institutions on the three issues above is needed, so

that follow-up research can be designed more purposefully and avoid duplicating what is already well established in the literature.

RESEARCH METHOD

Research Design

This study employs a systematic literature review (SLR) approach, a research method that identifies, appraises, and synthesizes all research evidence relevant to a specific research question in a systematic, transparent, and replicable manner (Snyder, 2019). The reporting procedure for this study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines (Page et al., 2021), which comprise four main stages, namely identification, screening, eligibility assessment, and inclusion.

Data Sources and Search Strategy

The literature search was conducted across reputable academic databases, namely Scopus, SINTA, Google Scholar, DOAJ, and SSRN, and was supplemented by a search of publications from authoritative think tanks and international organizations in the fields of cybersecurity and transnational crime, including the S. Rajaratnam School of International Studies (RSIS), the United Nations Office on Drugs and Crime (UNODC), the Center for Strategic and International Studies (CSIS), the Global Initiative Against Transnational Organized Crime (GI-TOC), the Council of Europe, INTERPOL, the ASEAN Secretariat, and Pacific Forum. Search keywords were organized into six thematic clusters: (1) concepts and models of digital sovereignty; (2) theories of transnational organized crime and cross-border cybercrime; (3) structural vulnerability, digital divides, and asymmetric vulnerability; (4) cybersecurity governance and institutional fragmentation; (5) law enforcement, regulatory harmonization, and international cooperation; and (6) the empirical context of Indonesia and Southeast Asia.

Inclusion and Exclusion Criteria

The inclusion criteria comprised: (a) publications from 2000 to 2026, to capture both classical theoretical foundations and recent developments; (b) written in Indonesian or English; (c) constituting peer-reviewed articles in reputable indexed journals, official reports from authoritative institutions, or academic book chapters; and (d) being directly relevant to the themes of digital sovereignty, structural vulnerability, transnational cybercrime, or the empirical context of Indonesia and Southeast Asia. The exclusion criteria comprised: duplicate records, records whose full text could not be accessed, records deemed thematically irrelevant following title and abstract screening, and records with inadequate methodological rigor or thematic coverage already represented by other, more comprehensive studies.

Study Selection Process

The selection process followed the PRISMA flow diagram presented in Figure 1. Database and other-source searches yielded 370 records (342 from databases, 28 from other sources), which were reduced to 298 records after duplicates were removed. Title and abstract screening excluded 189 irrelevant records, leaving 109 full-text articles assessed for eligibility. Full-text eligibility assessment further excluded 59 records on the grounds of thematic or contextual irrelevance, weak methodological rigor, or thematic overlap with other, more comprehensive studies, leaving 50 studies included in the final synthesis. Of these 50 studies, 10 with the most direct theoretical and empirical relevance to the study's objectives were

synthesized narratively, while the remaining 40 are presented in a summary matrix (Table 1) to enrich and broaden the contextual discussion.

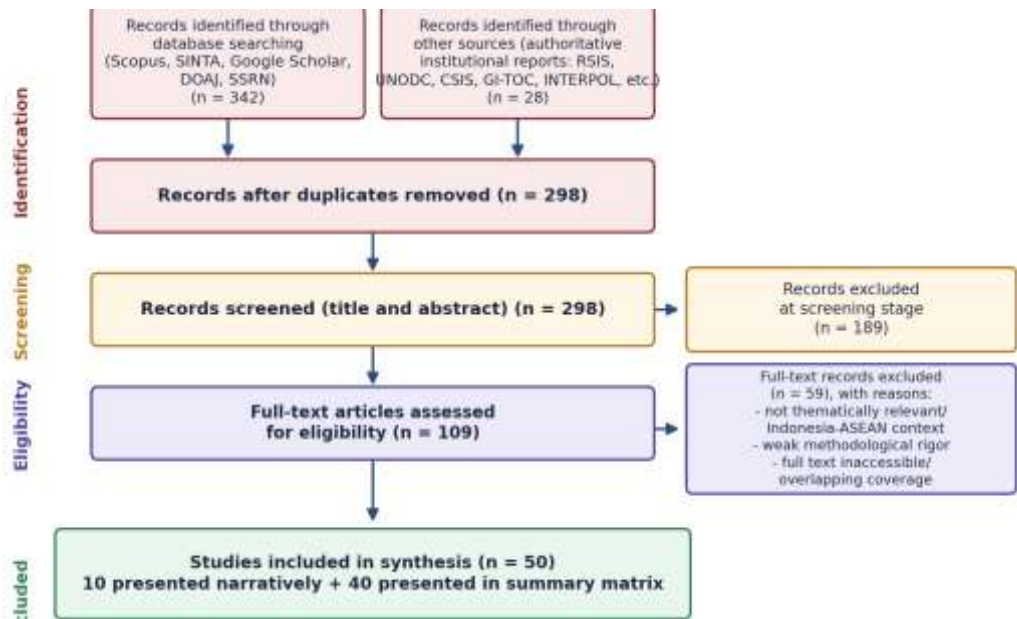


Figure 1. PRISMA Flow Diagram of Study Selection

Figure 1 illustrates the study selection process using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. The process began with the identification of 370 records, consisting of 342 records obtained from database searches, including Scopus, SINTA, Google Scholar, DOAJ, and SSRN, and 28 records identified through other sources, such as institutional repositories and additional academic platforms. After removing duplicate records, 298 records remained for screening based on their titles and abstracts. At this stage, 189 records were excluded because they did not meet the initial relevance criteria. Subsequently, 109 full-text articles were assessed for eligibility. Of these, 59 articles were excluded for several reasons, including insufficient thematic relevance, limited methodological rigor, inaccessible full-text documents, and overlapping coverage. Finally, 50 studies were included in the review synthesis. Of these, 10 studies were presented narratively, while 40 studies were incorporated into the summary matrix. This systematic selection process ensured that the included studies were relevant to the research objectives and met the established eligibility criteria, thereby providing a structured foundation for the subsequent analysis and synthesis of the literature.

Data Extraction and Synthesis

Data were extracted in a structured manner for each included study, covering the author(s) and year of publication, title, the study's original research method, key findings, and their relevance to the focus of this study. Synthesis was conducted thematically, grouping the findings from the 50 studies into five theoretical pillars that form the analytical framework, namely digital sovereignty, structural vulnerability and asymmetric vulnerability, transnational organized crime, cybersecurity securitization, and cybersecurity governance and institutional fragmentation, which were subsequently mapped onto the three research objectives formulated in the introduction. This thematic synthesis approach was chosen because it enables the integration of findings from studies with diverse methodological designs, whether qualitative, quantitative, or legal-normative, into a coherent analytical framework (Snyder, 2019).

RESULTS AND DISCUSSION

Characteristics of Threats and Indonesia's Structural Vulnerability

The literature synthesis shows that Indonesia's structural vulnerability to transnational cybercrime is multidimensional and cannot be explained by a single factor. At the structural-systemic level, quantitative findings by Morić, Urošev, and Kopal (2026), based on global trade network data from 2010 to 2020, show that a country's structural position within the global trade network, that is, its level of accessibility and connectivity, increases the probability of cyberattacks from a range of 7-10 percent to 30-40 percent per year. This finding is relevant to Indonesia's position as the world's largest archipelagic state, with more than 17,000 islands and the fourth-longest coastline in the world, which is structurally difficult to monitor evenly, consistent with the three-layer cyber sovereignty conceptualization, namely physical, logical, and cognitive, proposed by Moreno Junior (2026).

At the cognitive level, the concept of asymmetric vulnerability, that is, the gap between society's capacity to access digital technology and its capacity to understand the accompanying risks, is empirically supported by the study of Khan, Ikram, and Saleem (2023) in Pakistan, which found a significant correlation between socioeconomic disparity and weak cybersecurity behavior, as well as the study of Soroya, Ahmad, Ahmad, and Soroya (2021), which showed internet literacy skill gaps among digital natives in developing countries despite their early exposure to technology. In the Indonesian context, with more than 220 million internet users yet low and uneven levels of cyber literacy, this asymmetric vulnerability becomes one of the key factors amplifying the space for exploitation through targeted social engineering and disinformation (Sarjito, 2024; Gonzaga et al., 2026).

At the technical and institutional level, the systematic literature review by Rambe and Hermawan (2025) of 45 published studies identified six categories of critical weaknesses underlying the Brain Cipher ransomware attack on PDNS, which are interrelated: technical deficiencies, shortages of cybersecurity human resources, governance failures in the form of poor inter-agency coordination, regulatory gaps, procurement irregularities, and low public awareness. This same pattern of multidimensional vulnerability is also confirmed by investigative findings from UNODC (2024), ASEAN-Australia Counter Trafficking (2024), CSIS (2026), and the Global Initiative Against Transnational Organized Crime (2023) regarding the relocation of scam operation networks from Cambodia, Myanmar, Laos, and Vietnam into Indonesia, with quantitative estimates from Jeselyn and Goh (2025) indicating approximately 80,000 Indonesian citizens working illegally in Cambodia and annual losses from online gambling estimated at USD 55.3 billion. Drawing on the theory of transnational organized crime advanced by Galeotti (2001) and Williams (2001), this pattern is consistent with the thesis that non-state criminal actors possess an organizational advantage in networked environments compared to governmental institutions, which tend to be hierarchical, such that cybercrime networks are able to adapt to and exploit domestic structural gaps far more rapidly than the state's institutional response capacity.

Effectiveness of Cybersecurity Oversight and Law Enforcement Policy

The literature synthesis on policy effectiveness reveals a consistent pattern of institutional fragmentation across studies. Chotimah (2019) traces the historical establishment of BSSN as an agency mandated to safeguard cybersecurity and cyber sovereignty while also conducting cyber diplomacy, yet its implementation remains fragmented due to the absence of

a single command structure: the National Police handle cybercrime from a criminal-law perspective, BSSN from a technical perspective, and the Ministry of Communication and Digital Affairs from a platform-regulation perspective, without adequate coordination. This pattern of domestic fragmentation aligns with the findings of Li (2025), who shows that geopolitical and regulatory fragmentation constitutes a major structural barrier to global governance of high-risk technologies, including cybersecurity, as well as Barrinha and Turner (2023), who demonstrate how global actors frame their approaches to multilateral cyber governance differently according to their respective national strategic interests.

At the domestic regulatory level, Firdaus (2025) finds that the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP) have significant limitations in anticipating continuously evolving cybercrime *modus operandi*, while Sulubara, Tasril, and Nurkhalisah's (2025) evaluation of the 2025 RUU KKS finds that although Indonesia already possesses a relevant legal framework, existing regulations remain insufficiently detailed regarding cybercrime terminology and *modus operandi*, such that RUU KKS is regarded as a vital strengthening measure, albeit one that still requires normative caution. At the level of international legal cooperation, Clough (2015) and the Council of Europe Cybercrime Convention Committee (2023) identify that mutual legal assistance (MLA) mechanisms under the Budapest Convention are often slow and inadequate to respond to the speed required for handling electronic evidence, a finding specifically confirmed in the Indonesian context by Galfadillah, Zabril, and Nabila (2026) in their study of MLA implementation in cybercrime cases between Indonesia and the People's Republic of China.

From the perspective of policy construction, the Copenhagen School securitization framework, as adapted by Hansen and Nissenbaum (2009) for the cyber domain, comprising three modalities, namely hypersecuritization, everyday security practices, and technification, provides an important analytical lens for understanding how the urgency of RUU KKS is constructed as a national security issue. Nevertheless, Thumfart (2023), through Just Securitization Theory, emphasizes that the legitimacy of state cybersecurity securitization measures must be tested against the principle of subsidiarity, namely proportionality and necessity, an evaluative framework that is particularly relevant given the concerns raised by Neumann (2026) and Sherman (2021) regarding the expansion of military actors' roles in the cyber domain, which risks distributing security authority disproportionately without commensurate accountability.

Strategies for Strengthening Indonesia's Digital Sovereignty

The literature synthesis on digital sovereignty shows that the concept is plural and context-dependent rather than singular. Robles-Carrillo (2023) affirms that digital sovereignty is an autonomous category distinct from traditional sovereignty, rather than merely its 'online version,' such that its function shifts toward an independent framework for responding to contemporary technological challenges and geopolitical competition. Fratini, Hine, Novelli, Roberts, and Floridi (2024), through a systematic review of 271 scholarly articles, identify four digital sovereignty models developing in parallel, namely rights-based, market-oriented, centralization, and state-based models, with the important finding that no single model perfectly combines comprehensive regulation with responsiveness to technological change. This finding provides an evaluative framework for positioning the direction of Indonesia's digital sovereignty policy, including RUU KKS, among these four models, while also

cautioning against leaning entirely toward the centralization or state-based model without an anchor in citizens' digital rights (Pohle, 2024; Krishnamurthy, 2025).

At the regional level, the ASEAN Cybersecurity Cooperation Strategy 2021-2025 (ASEAN Secretariat, 2022) and the Cyber ASEAN initiative by Pacific Forum and DFAT (2024) offer capacity-building cooperation frameworks that can serve as a comparative reference for strengthening Indonesia's cybersecurity institutions, in line with the recommendations of Jeselyn and Goh (2025) regarding strengthened ASEAN law enforcement coordination and harmonized anti-trafficking legislation to address cross-border cybercrime. Taken together, this literature synthesis affirms that an effective and sustainable strategy for strengthening Indonesia's digital sovereignty requires the simultaneous integration of four elements: structural reform across the five dimensions of vulnerability (geographic, demographic, technological, regulatory, and institutional); strengthening institutional capacity and human resources to address the fragmentation identified above; harmonizing domestic regulation with international standards such as the Budapest Convention; and enhanced international cooperation, while maintaining a balance between state security interests and the protection of citizens' digital rights, as cautioned by McCusker (2006) regarding the risk of threat inflation and by Thumfart (2023) regarding the principle of proportionality in securitization.

Table 1. Summary Matrix of Selected Studies by Thematic Pillar

Author(s) (Year)	Theme	Original Study Method	Key Findings
Fratini et al. (2024)	Digital sovereignty	Systematic review of 271 articles	Four digital sovereignty models (rights-based, market- oriented, centralization, state- based); no single model is optimal
Robles- Carrillo (2023)	Digital sovereignty	Conceptual analysis	Digital sovereignty is an autonomous category, not an online version of classical sovereignty
Moreno Junior (2026)	Digital sovereignty	Theoretical- methodological model (set theory)	Cyber sovereignty operates across three layers: physical, logical, cognitive
Morić, Urošev, & Kopal (2026)	Structural vulnerability	Quantitative, network analysis 2010- 2020	Structural position in the global trade network raises cyberattack risk from 7-10% to 30-40%
Khan, Ikram, & Saleem (2023)	Structural vulnerability (asymmetric vulnerability)	Survey of 758 students (Pakistan)	Socioeconomic disparity correlates with weak cybersecurity behavior
Rambe & Hermawan (2025)	Structural vulnerability (PDNS case)	Systematic Literature Review, 45	Six critical weakness categories in the Brain Cipher incident: technical, human

			studies	resources, regulatory, public awareness	governance, procurement, Non-state criminal actors
Galeotti (2001)	Transnational organized crime	Conceptual analysis		outperform institutions in networked environments	hierarchical in
Jeselyn & Goh (2025)	Transnational organized crime	RSIS Commentary, policy analysis		~80,000 Indonesian citizens working illegally in Cambodia; ~USD 55.3 billion in online gambling losses	
UNODC (2024)	Transnational organized crime	Investigative report		Southeast Asia's cyberfraud industry is worth billions of dollars and continues to expand	
Chotimah (2019)	Governance/institutional fragmentation	Qualitative, literature study		BSSN holds a dual mandate but implementation remains fragmented without unified command	
Clough (2015)	Governance/international legal cooperation	Comparative doctrinal legal analysis		The Budapest Convention facilitates harmonization but is hindered by differing domestic legal systems	
Hansen & Nissenbaum (2009)	Securitization	Discourse analysis (Estonia 2007 case study)		Three modalities of cyber threat construction: hypersecuritization, everyday practice, technification	
Thumfart (2023)	Securitization (normative)	Normative theoretical analysis		The legitimacy of cyber securitization must be tested against the subsidiarity principle (proportionality)	

Note: The table above presents 15 of the 50 studies included in the synthesis, selected to represent the five thematic pillars. The complete matrix of 50 studies is available from the corresponding author upon request.

CONCLUSION

The systematic review of 50 literature studies yields three main conclusions. First, Indonesia's structural vulnerability to transnational cybercrime is multidimensional, spanning geographic, demographic, technological, regulatory, and institutional dimensions that interact cumulatively rather than in isolation, as confirmed both by quantitative evidence regarding Indonesia's structural position within global networks and by qualitative findings regarding technical and institutional vulnerabilities in concrete incidents such as the Brain Cipher attack on PDNS. Second, the effectiveness of Indonesia's cybersecurity oversight and law

enforcement policy is significantly constrained by institutional fragmentation lacking a single command structure, by limitations in domestic regulation in anticipating continuously evolving criminal modus operandi, and by weak international legal cooperation mechanisms. Third, an effective and sustainable strategy for strengthening Indonesia's digital sovereignty requires an approach that simultaneously integrates structural reform, strengthening of institutional capacity and human resources, harmonization of domestic regulation with international standards, and international cooperation, while maintaining a balance between state security interests and the protection of citizens' digital rights.

This study has methodological limitations that must be transparently disclosed. As a systematic literature review, the findings presented are derived from a synthesis of secondary data and have not been verified through the collection of primary data from stakeholders directly involved in handling cybercrime and formulating Indonesia's cybersecurity policy. Follow-up research employing a qualitative approach based on in-depth interviews with key stakeholders, such as BSSN officials, investigators from the Cyber Crime Directorate of the National Police Criminal Investigation Agency, policymakers at the Ministry of Communication and Digital Affairs and Commission I of the House of Representatives, academics, and representatives of the private sector and civil society, is therefore essential to verify and deepen the findings of this literature synthesis empirically, while also testing the propositions generated against the evolving realities of Indonesia's cybersecurity policy and law enforcement practice.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

In the course of preparing this work, the author employed Google Assisted assistance for language refinement, academic paraphrasing, and plagiarism detection to ensure that the content was original and free from duplication. Following the use of this tool, the author conducted a thorough review and revision of the material, thereby accepting full responsibility for the accuracy, integrity, and authenticity of the publication.

AUTHOR CONTRIBUTIONS

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.

Author 2: Conceptualization; Data curation; In-vestigation.

Author 3: Data curation; Investigation.

Author 4: Formal analysis; Methodology; Writing - original draft.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

- Aji, M. P. (2022). Sistem keamanan siber dan kedaulatan data di Indonesia dalam perspektif ekonomi politik (Studi kasus perlindungan data pribadi). *Jurnal Politica: Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*.
- Al Ghiffari, A. (2025). Kejahatan siber dan tantangan penegakan hukum di Indonesia. *Jurnal Penelitian Ilmiah Multidisipliner*, 2(2).

- Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis risiko keamanan siber dalam transformasi digital pelayanan publik di Indonesia. *Jurnal Kajian Strategik Ketahanan Nasional*, 6(2). <https://doi.org/10.7454/jkskn.v6i2.10082>
- ASEAN Secretariat. (2022). *ASEAN cybersecurity cooperation strategy 2021–2025*. ASEAN.
- ASEAN–Australia Counter Trafficking. (2024). *Compound crime: Cyber scam operations in Southeast Asia*. ASEAN-ACT Programme.
- Badan Siber dan Sandi Negara. (2025). *Lanskap keamanan siber Indonesia 2025*. BSSN.
- Badan Siber dan Sandi Negara. (2026). *Ringkasan tren insiden siber Januari-April 2026*. BSSN.
- Barrinha, A., & Turner, R. (2023). Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India. *Contemporary Security Policy*. <https://doi.org/10.1080/13523260.2023.2266906>
- Castells, M. (2000). *The rise of the network society* (2nd ed.). Blackwell Publishers.
- Castle, A. (1997). *Transnational organized crime and international security* (Working Paper No. 19). Institute of International Relations, University of British Columbia.
- Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, 5(1). <https://doi.org/10.1093/cybsec/tyz001>
- Center for Strategic and International Studies. (2026). *Cyber scamming goes global: Unveiling Southeast Asia's high-tech fraud factories*. CSIS.
- Chotimah, H. C. (2019). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara. *Jurnal Politika: Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*.
- Clough, J. (2015). A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation. *Monash University Law Review*, 40(3), 698–736.
- Council of Europe, Cybercrime Convention Committee (T-CY). (2023). *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*. Council of Europe.
- Firdaus, R. A. (2025). Efektivitas ketentuan pidana UU ITE dan peran preventif UU PDP dalam kerangka hukum kejahatan siber Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(1), 79–104. <https://doi.org/10.14421/cf582q68>
- Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society*, 3. <https://doi.org/10.1007/s44206-024-00146-7>
- Galeotti, M. (2001). Underworld and upperworld: Transnational organized crime and global society. In D. Josselin & W. Wallace (Eds.), *Non-state actors in world politics* (pp. 203–217). Palgrave Macmillan.
- Galfadillah, K. M., Zabril, A., & Nabila, G. (2026). Implementasi mutual legal assistance (MLA) pada alat bukti elektronik yang telah dilakukan forensik digital dalam cyber crime antara Indonesia–RRT. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 5(1). <https://doi.org/10.31004/riggs.v5i1.7927>
- Global Initiative Against Transnational Organized Crime. (2023). *Compound crime: Cyber scam operations in Southeast Asia*. GI-TOC.
- Gonzaga, K., Serra, S., Gomes, M., & Malta, S. (2026). AI-powered social engineering: Emerging attack vectors, vulnerabilities, and multi-layered defense strategies. *Computers*, 15(2), 128. <https://doi.org/10.3390/computers15020128>
- Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175.
- Hwang, J. (2025). Digital sovereignty in an era of cyber threats and global connectivity. *International Journal of Multidisciplinary Research Updates*, 9(2), 012–023.
- INTERPOL. (2021). *ASEAN cyberthreat assessment 2021*. INTERPOL.

- Jabir, R., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. *AI*, 6(8), 174. <https://doi.org/10.3390/ai6080174>
- Jeselyn, & Goh, D. L. (2025). *Transnational crime in Cambodia and Indonesia: Strengthening regional and national responses* (RSIS Commentary CO25134). S. Rajaratnam School of International Studies.
- Khan, N. F., Ikram, N., & Saleem, S. (2023). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Security Journal*, 37(2), 214–244. <https://doi.org/10.1057/s41284-023-00375-4>
- Krishnamurthy, V. (2025). Anchoring digital sovereignty. *Chicago Journal of International Law*, 25(2).
- Li, J. (2025). Governing high-risk technologies in a fragmented world: Geopolitical tensions, regulatory gaps, and institutional barriers to global cooperation. *Fudan Journal of the Humanities and Social Sciences*, 19(1), 113–137. <https://doi.org/10.1007/s40647-025-00445-4>
- McCusker, R. (2006). Transnational organised cyber crime: Distinguishing threat from reality. *Crime, Law and Social Change*, 46, 257–273.
- Meiryani. (2023). Exploration of potential money laundering crimes with virtual currency facilities in Indonesia. *Journal of Money Laundering Control*, 27(6), 985–994. <https://doi.org/10.1108/JMLC-01-2023-0010>
- Moreno Junior, W. (2026). Cyber sovereignty and state power in the 21st century: A theoretical-methodological proposal for understanding sovereignty in cyberspace. *International Journal of Scientific Research and Management*, 14(5), 153–164.
- Morić, Z., Urošev, S., & Kopal, R. (2026). Network position in global trade systems and cyberattack risk: Evidence from country-level trade networks, 2010–2020. *Systems*, 14(4), 367. <https://doi.org/10.3390/systems14040367>
- Nelson, F. M., Prosperiani, M. D., Ramadhan, C. R., & Andini, P. P. (2024). Cracking the code: Investigating the hunt for crypto assets in money laundering cases in Indonesia. *Journal of Indonesian Legal Studies*, 9(1), 89–130. <https://doi.org/10.15294/jils.vol9i1.4534>
- Neumann, I. (2026). It is complicated: Cyber into the civil–military relationship. *Journal of Cybersecurity*, 12(1).
- Nyonyoh, R. (2025). Ransomware and the vulnerability of critical infrastructure: A national security and economic analysis. *Asian Journal of Economics, Business and Accounting*, 25(4). <https://doi.org/10.9734/ajeba/2025/v25i41759>
- Pacific Forum, & Department of Foreign Affairs and Trade Australia. (2024). *Cyber ASEAN: Advancing cyber resiliency and capacity in Southeast Asia*. Pacific Forum.
- 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., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Pohle, J. (2024). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*.
- Putri, T., Amiludin, A., Ahmad, D. N., & Hidayatulloh. (2023). Inadequate cryptocurrency and money laundering regulations in Indonesia (Comparative law of US and Germany). *Yustisia*, 12(2), 129–152. <https://doi.org/10.20961/yustisia.v12i2.71835>
- Rambe, R., & Hermawan, F. F. (2025). [Tinjauan literatur sistematis serangan ransomware terhadap Pusat Data Nasional Sementara Indonesia]. *Indonesian Journal on Computing*, 10(1), 1–11.

- Robles-Carrillo, M. (2023). Sovereignty vs. digital sovereignty. *Journal of Digital Technologies and Law*, 1(3), 673–690. <https://doi.org/10.21202/jdtl.2023.29>
- Santisteban Santisteban, A., Ocares Cunyarachi, L., & Andrade-Arenas, L. (2020). Analysis of national cybersecurity strategies. *International Journal of Advanced Computer Science and Applications*, 11(12).
- Sarjito, A. (2024). Hoaks, disinformasi, dan ketahanan nasional: Ancaman teknologi informasi dalam masyarakat digital Indonesia. *Journal of Governance and Local Politics*, 6(2).
- Sarjito, A., & Lelyana, N. (2025). Disinformation's influence on public perception and defense policy implementation in Indonesia. *Multidisciplinary Science Journal*, 7(8), e2025362. <https://doi.org/10.31893/multiscience.2025362>
- Sherman, J. (2021). Digital authoritarianism and implications for US national security. *The Cyber Defense Review*, 6(1).
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Soroya, S. H., Ahmad, A. S., Ahmad, S., & Soroya, M. S. (2021). Mapping internet literacy skills of digital natives: A developing country perspective. *PLOS ONE*, 16(4). <https://doi.org/10.1371/journal.pone.0249495>
- Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). [Perlindungan data pribadi di era metaverse]. *Jurnal Masalah-Masalah Hukum*, 52(1).
- Sulubara, S. M., Fauzi, H., Muslim, B., Putra, M. F. F., & Musmulyadi. (2025). Judi online sebagai cybercrime serta tantangan penegakan hukum. *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora*, 4(2), 539–552. <https://doi.org/10.55606/jurrish.v4i2.4990>
- Sulubara, S. M., Tasril, V., & Nurkhalisah. (2025). Legal protection of cybercrime crimes from ransomware attacks and evaluation of the Cyber Security and Resilience Bill 2025 in Indonesia's defense. *DE LEGA LATA: Jurnal Ilmu Hukum*, 10(2), 287–297. <https://doi.org/10.30596/dll.v10i2.25786>
- Thumfart, J. (2023). The (il)legitimacy of cybersecurity: An application of just securitization theory to cybersecurity based on the principle of subsidiarity. *Applied Cybersecurity & Internet Governance*.
- UNODC. (2024). *Billion-dollar cyberfraud industry expands in Southeast Asia as criminals adopt new technologies*. United Nations Office on Drugs and Crime, Regional Office for Southeast Asia and the Pacific.
- Williams, P. (2001). Transnational criminal networks. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 61–97). RAND Corporation.

Copyright Holder :

© Pratomo Widodo et al. (2026).

First Publication Right :

© Sciencetechno: Journal of Science and Technology

This article is under:

