

Legal politics of cybersecurity governance in Indonesia: Strengthening national cyber resilience in the digital era

Ginting Bryan Suanta S H, Dr. Bambang Slamet Riyadi S H M H, Dr. Riza Zulfikar S H M T, M Kn

Master of Law, Langlang Buana University, Bandung, Indonesia

Abstract

The rapid advancement of information and communication technology has significantly increased Indonesia's dependence on digital infrastructure across government, business, and public services. While digital transformation has improved efficiency and economic growth, it has also heightened the risk of cyber threats, including cyberattacks, data breaches, ransomware, and cyber espionage. These developments require a comprehensive legal framework capable of ensuring cybersecurity while protecting national interests and citizens' digital rights. This article examines the legal politics of cybersecurity governance in Indonesia by analyzing the legal policy underlying cybersecurity regulation, the state's role in developing national cyber resilience, and the challenges encountered in implementing cybersecurity governance. This study employs a normative juridical approach using statutory, conceptual, and literature-based analyses. The findings indicate that Indonesia's cybersecurity legal policy reflects the state's commitment to strengthening national security and supporting digital transformation through various laws, regulations, and institutional arrangements. Nevertheless, the effectiveness of cybersecurity governance remains constrained by regulatory fragmentation, institutional overlap, limited human resource capacity, and the increasing sophistication of cyber threats. Therefore, strengthening legal harmonization, institutional coordination, and cybersecurity awareness is essential to establish an adaptive and resilient national cybersecurity system.

Keywords: Legal politics, cybersecurity governance, national cyber resilience, digital security, Indonesia

Introduction

The rapid advancement of information and communication technology has transformed the way governments, businesses, and society conduct their activities. Digital technologies have become fundamental to public administration, financial services, education, healthcare, and commercial transactions, making cyberspace an essential component of national development. However, this transformation has also increased exposure to cyber threats that may disrupt public services, economic activities, and state security. Consequently, cybersecurity has evolved from a purely technical concern into an important issue of governance and public policy that requires an integrated legal framework^[1].

Indonesia has experienced substantial digital transformation over the past decade through the expansion of electronic government services, digital financial systems, and online public services. While these developments have generated significant economic and administrative benefits, they have also created new vulnerabilities within national digital infrastructure. Cyber incidents involving public institutions have demonstrated that inadequate cybersecurity governance may jeopardize data protection, service continuity, and public trust in government institutions^[2].

As a constitutional state, Indonesia is required to ensure that technological advancement is supported by a legal system capable of protecting national interests and safeguarding the rights of its citizens. The government's commitment to strengthening cybersecurity is reflected in various regulatory instruments governing electronic systems and digital governance. Nevertheless, the existing legal framework remains fragmented because cybersecurity provisions are dispersed across different laws and regulations rather than being comprehensively regulated under a dedicated cybersecurity statute^[3].

From the perspective of legal politics, cybersecurity governance reflects the state's policy direction in responding to technological change and emerging security challenges. The formulation of legal policy determines institutional authority, regulatory priorities, and mechanisms for coordinating cybersecurity responsibilities among government agencies. Therefore, cybersecurity governance should be understood not only as a matter of information technology but also as a strategic legal instrument for strengthening national resilience and supporting sustainable digital transformation^[4].

Based on these considerations, this article examines the legal politics of cybersecurity governance in Indonesia by analyzing the direction of state legal policy, the existing regulatory framework, and the challenges faced in strengthening national cybersecurity governance in the digital era.

Problem Formulation

Based on the background presented above, the problem formulation in this study is as follows:

How does the legal politics of cybersecurity governance in Indonesia shape the development and implementation of cybersecurity regulations in strengthening national cyber resilience during the digital era?

Discussion

1. Legal Politics as the Foundation of Cybersecurity Governance

Legal politics serves as the foundation for the formulation and development of national laws to address emerging societal challenges. In the context of cybersecurity, legal politics reflects the government's strategic direction in establishing legal norms, institutional arrangements, and regulatory mechanisms capable of responding to the

increasing complexity of cyber threats. As digital transformation continues to reshape governance and economic activities, cybersecurity has become an essential component of national legal policy aimed at protecting public interests, maintaining state sovereignty, and ensuring the security of digital infrastructure [5].

The emergence of cybersecurity as a legal policy issue is closely associated with the growing dependence on digital systems across both public and private sectors. Cyber incidents affecting government institutions, financial services, healthcare systems, and other critical infrastructures have demonstrated that cyber threats may generate consequences extending beyond technical failures to include economic disruption, national security risks, and violations of citizens' rights. Therefore, the state is required to formulate legal policies that provide certainty regarding institutional responsibilities, preventive measures, and enforcement mechanisms for addressing cyber incidents [6].

Indonesia's cybersecurity governance has gradually developed through several sectoral regulations governing electronic information, digital transactions, state intelligence, national defense, and electronic system administration. Although these regulations collectively contribute to cybersecurity governance, they remain fragmented and often create overlapping institutional authority. This condition indicates that Indonesia's legal politics is still evolving toward a more integrated cybersecurity regulatory framework capable of accommodating technological developments and contemporary security challenges [3].

From the perspective of legal development, cybersecurity governance should not merely focus on responding to cybercrime after incidents occur. Instead, legal politics should prioritize preventive governance through institutional coordination, risk management, protection of critical information infrastructure, and continuous regulatory adaptation to technological innovation. Such an approach enables the legal system to function proactively while supporting sustainable digital transformation and strengthening national cyber resilience [4].

Therefore, the legal politics of cybersecurity governance demonstrates that cybersecurity regulation is no longer limited to protecting information systems but has become an integral component of Indonesia's national legal development strategy. Effective legal policies are expected to provide legal certainty, strengthen institutional coordination, and enhance the country's capacity to respond to increasingly sophisticated cyber threats in the digital era.

2. Cybersecurity as a State Responsibility in Protecting National Interests

Cybersecurity has become an inseparable element of national security in the digital era. The extensive use of digital technologies in public administration, defense, financial systems, transportation, healthcare, and communication has increased the dependence of modern states on cyberspace. Consequently, cyberattacks are no longer viewed merely as criminal activities targeting information systems but are increasingly recognized as threats capable of disrupting national stability, economic resilience, and the continuity of essential public services. This development has expanded the state's responsibility to ensure the security and resilience of its national cyber ecosystem [7].

From the perspective of public law, the state has a constitutional obligation to protect its citizens and safeguard national interests against both conventional and non-conventional threats. Cyber threats differ from traditional security threats because they can transcend territorial boundaries, be conducted anonymously, and evolve rapidly alongside technological innovation. Therefore, governments are required to formulate comprehensive legal frameworks that define institutional responsibilities, strengthen inter-agency coordination, and establish effective mechanisms for preventing, detecting, and responding to cyber incidents [8].

In Indonesia, the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara BSSN) plays a strategic role in the national cybersecurity architecture by coordinating cybersecurity governance among government institutions and supporting the protection of critical information infrastructure. Beyond its technical functions, BSSN is expected to strengthen institutional collaboration, improve cyber resilience, and facilitate the development of integrated cybersecurity policies. However, the effectiveness of cybersecurity governance continues to depend on effective coordination among ministries, law enforcement agencies, the private sector, and other stakeholders, as cybersecurity requires a collaborative governance approach rather than relying solely on a single institution [9].

Furthermore, cybersecurity governance should also ensure that national security measures remain consistent with democratic principles and the protection of fundamental rights. Legal policies designed to strengthen cybersecurity should not result in excessive restrictions on privacy, freedom of expression, or access to information. Instead, cybersecurity regulation should maintain an appropriate balance between national security objectives and the protection of constitutional rights, thereby ensuring that legal certainty and human rights are upheld simultaneously within Indonesia's digital governance framework [10].

Based on these considerations, cybersecurity should be understood as a shared responsibility that extends beyond technical protection of digital infrastructure. The state's legal and institutional responsibilities must be supported by effective governance, regulatory coherence, and respect for constitutional values. Such an approach reflects the legal politics of cybersecurity governance that seeks to strengthen national resilience while preserving democratic governance and the rule of law.

3. Challenges and Future Direction of Cybersecurity Governance in Indonesia

Despite the continuous development of cybersecurity regulations, Indonesia still faces several challenges in establishing an effective cybersecurity governance framework. One of the primary challenges is the fragmentation of legal provisions governing cybersecurity across multiple laws and regulations. The absence of a comprehensive cybersecurity law has resulted in overlapping institutional responsibilities and varying interpretations regarding the authority of government agencies in preventing and responding to cyber incidents. Such conditions may reduce regulatory effectiveness and complicate coordination during cybersecurity emergencies [3].

Another significant challenge concerns institutional and technical capacity. As cyber threats continue to evolve in complexity, effective cybersecurity governance requires

competent human resources, adequate technological infrastructure, and strong collaboration among government institutions, the private sector, and academic communities. However, differences in institutional readiness and cybersecurity awareness remain obstacles to developing a resilient national cybersecurity ecosystem. These conditions indicate that cybersecurity governance should be strengthened not only through legal reform but also through institutional capacity building and continuous investment in cyber resilience ^[6].

To address these challenges, Indonesia's future legal policy should emphasize regulatory harmonization and stronger institutional coordination. The development of a comprehensive cybersecurity legal framework would provide greater legal certainty while clarifying the roles and responsibilities of relevant institutions. In addition, strengthening international cooperation, improving cybersecurity capacity, and promoting public awareness are essential components of national cyber resilience, particularly as cyber threats increasingly transcend national borders ^[11].

From the perspective of legal politics, cybersecurity governance should remain adaptive to technological developments without compromising the principles of the rule of law and the protection of constitutional rights. A coherent legal framework, supported by effective institutional cooperation and sustainable policy development, will enable Indonesia to enhance its cybersecurity governance while fostering public trust and supporting long-term digital transformation.

Closing

Conclusion

Cybersecurity governance has become an essential component of Indonesia's legal policy in responding to the growing challenges of digital transformation. From the perspective of legal politics, the development of cybersecurity regulation reflects the state's commitment to protecting national interests, ensuring legal certainty, and strengthening national cyber resilience. The existing legal framework, supported by sectoral regulations and institutional arrangements, demonstrates the government's efforts to establish cybersecurity governance despite the absence of a comprehensive cybersecurity law.

Nevertheless, the implementation of cybersecurity governance continues to face several challenges, including fragmented regulations, overlapping institutional authority, limited cybersecurity capacity, and the increasingly sophisticated nature of cyber threats. Therefore, Indonesia's future legal policy should focus on developing an integrated and adaptive cybersecurity governance framework that promotes effective institutional coordination, regulatory harmonization, and sustainable protection of national digital infrastructure. Such an approach is expected to strengthen public trust, support digital transformation, and enhance Indonesia's resilience in addressing future cybersecurity challenges.

Suggestions

Based on the findings of this study, several recommendations are proposed:

1. The Government of Indonesia should strengthen cybersecurity governance by establishing a comprehensive legal framework that clearly regulates

institutional authority, coordination mechanisms, and the protection of critical information infrastructure to improve legal certainty and the effectiveness of cybersecurity implementation.

2. Future studies are encouraged to examine cybersecurity governance from empirical and comparative perspectives by evaluating the implementation of cybersecurity policies in Indonesia and comparing them with regulatory practices adopted by other countries to provide broader recommendations for legal reform.

References

1. Isfihani AE, Izomiddin, Antasari RR, Is MS. Political Law of Electronic System Implementation in Indonesia. Nurani J. Kaji. Syari'ah dan Masy., 2024, 24(1). doi: 10.19109/nurani.v24i1.22672.
2. Wahyudi E, Suhardi M. Cybersecurity Governance in Electronic-Based Government Systems: An Analysis of the Government's Legal Responsibility for Public Data Breaches. J. Kecerdasan Buatan dan Teknol. Inf., 2024, 4(3). doi: 10.69916/jkbt.v4i3.462.
3. Manullang SO. The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws. Society, 2022;10(2):489–502. doi: 10.33019/society.v10i2.482.
4. Aji MP. Cybersecurity Politics in Building Cyber Sovereignty in Indonesia Through Strengthening the Role of the National Cyber and Crypto Agency. Society, 2025, 13(2). doi: 10.33019/society.v13i2.960.
5. Wahab HNA, Kamaruddin NA. Cybersecurity Governance: A Systematic Literature Review. Int. J. Inf. Manag. Data Insights, 2023, 3(2).
6. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. Publications Office of the European Union, Luxembourg, 2024.
7. International Telecommunication Union. Global Cybersecurity Index 2024. Geneva, Switzerland, 2024.
8. United Nations. United Nations Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021--2025: Final Report. New York, NY, 2025.
9. Rosdiana H, Reja R, Setiawan BH. Peran Badan Siber dan Sandi Negara (BSSN) dalam Arsitektur Keamanan Siber Indonesia. J. Ris. Rumpun Ilmu Sos. Polit. dan Hum., 2025, 5(1). doi: 10.55606/jurish.v5i1.8471.
10. Klimburg A. The Darkening Web: The War for Cyberspace. New York, NY: Penguin Press, 2017.
11. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD, 2024.