Journal of Cyber Law and Information Security
Volume 4, Number 2, 2025

Towards Integrated Cybersecurity Governance in Indonesia: Addressing Fragmentation, Enforcement Gaps, and Institutional Constraints

Alfarel Endito Putra [1]

[1] Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia

Abstract

Article history:
Received: September 21, 2025
Revised: October 04, 2025
Accepted: November 22, 2025
Published: December 30, 2025

Keywords:
Collaborative Governance, Cybersecurity Governance, Enforcement Capacity, Governance Integration, Institutional Coordination, Regulatory Effectiveness.

Identifier:
Zera Open
Page: 179-197
https://zeraopen.com/journal/jclis

Cybersecurity governance in Indonesia faces systemic challenges arising from institutional fragmentation, weak enforcement capacity, and limited coordination mechanisms. While existing legal frameworks provide a formal basis for regulating digital activities, their effectiveness remains constrained by the lack of integration among institutional actors and processes. This study examines the structural barriers to integrated cybersecurity governance and proposes an integrated governance model to enhance regulatory effectiveness. Using a normative juridical method combined with systematic and sociological approaches, the research analyzes the interaction between institutional structure, enforcement capacity, and coordination mechanisms. The findings indicate that fragmentation and capacity limitations lead to inconsistent policy implementation and weak enforcement outcomes. To address these challenges, the study proposes an integrated governance model that aligns institutional roles, strengthens coordination mechanisms, and embeds enforcement capacity within governance design. The study concludes that integrated governance is essential for improving cybersecurity regulation and ensuring effective and coherent digital governance in Indonesia.

*Corresponding author:
(Alfarel Endito Putra)

1. Introduction

The rapid expansion of digital technologies has significantly increased the complexity of governance systems, particularly in areas such as cybersecurity where multiple institutions and regulatory instruments intersect. As digital risks become more multidimensional, governance frameworks must address not only legal regulation but also institutional coordination and enforcement capability. However, in many regulatory environments, the proliferation of laws and agencies has led to fragmented governance structures that struggle to operate cohesively. Haapasaari et al. (2021) highlight that integrated governance is essential for managing complex policy problems that span multiple domains and actors. Similarly, Peters (2022) emphasizes that institutional design plays a critical role in shaping the effectiveness of policy implementation in complex governance systems. These perspectives indicate that governance effectiveness is increasingly dependent on the ability to integrate diverse institutional components into a coherent system.

A central challenge in contemporary governance is the persistence of fragmentation, where institutions operate within siloed structures with limited coordination. Fragmentation reduces the ability of governance systems to align policy objectives, share information, and implement regulations consistently. Vantaggiato et al. (2021) demonstrate that cross-departmental interaction is often constrained by institutional barriers that limit coordination and collaboration. Klijn et al. (2025) further argue that governance networks require structured coordination mechanisms to function effectively in multi-actor environments. In the absence of such mechanisms, institutions tend to operate independently, leading to

inefficiencies and policy inconsistencies. This suggests that fragmentation is not merely an organizational issue but a structural limitation that undermines governance effectiveness. Consequently, addressing fragmentation requires a shift toward more integrated governance approaches.

In addition to fragmentation, enforcement capacity represents a critical factor influencing the effectiveness of cybersecurity governance. Even when legal frameworks are comprehensive, their impact depends on the ability of institutions to enforce them consistently and effectively. Chowdhury (2022) emphasizes that state capacity is a key determinant of regulatory performance, particularly in complex policy environments. Geddes (2023) further highlights that institutional capacity constraints often limit the ability of governments to implement policies effectively. Weak enforcement capacity reduces the credibility of legal frameworks and undermines their deterrent effect. As a result, regulatory systems fail to achieve their intended objectives despite formal legal provisions. This indicates that enforcement capacity must be considered alongside institutional structure in assessing governance effectiveness.

The complexity of cybersecurity governance further amplifies the challenges associated with fragmentation and enforcement capacity. Cybersecurity requires coordinated action across multiple institutions, including regulatory agencies, law enforcement bodies, and technical organizations. Savaş and Karataş (2022) highlight that cybersecurity governance involves a network of actors that must operate in a coordinated manner to address evolving digital threats. Del-Real and Díaz-Fernández (2022) further demonstrate that cybersecurity governance often involves

overlapping institutional arrangements that complicate coordination and resource allocation. These conditions create a governance environment in which responsibilities are dispersed and enforcement is inconsistent. As a result, cybersecurity governance systems struggle to respond effectively to emerging risks. This underscores the need for integrated approaches that align institutional roles and capabilities.

Despite the recognition of these challenges, existing research has largely focused on individual aspects of governance, such as legal effectiveness, institutional fragmentation, or enforcement capacity, without fully addressing their interconnection. This creates a gap in understanding how these factors interact to shape overall governance performance. Aoki et al. (2024) emphasize that whole-of-government approaches are necessary to overcome institutional silos and improve policy coherence. Andarge and Lichtenberg (2020) further highlight that effective enforcement depends on consistent and coordinated institutional action. These insights suggest that fragmentation, enforcement, and capacity are interdependent elements of governance systems. However, there remains a lack of integrated frameworks that address these dimensions collectively. Therefore, a comprehensive approach is required to understand and improve cybersecurity governance.

Based on these considerations, this study aims to analyze the structural barriers that hinder the development of integrated cybersecurity governance in Indonesia and to propose an integrated governance model that enhances enforcement effectiveness and regulatory performance. Using a normative juridical method combined with systematic and sociological approaches, the study evaluates

the relationship between institutional structure, enforcement capacity, and governance outcomes. The analysis focuses on identifying how fragmentation, coordination failure, and capacity limitations interact within Indonesia's cybersecurity governance system. By synthesizing these dimensions, the study provides a framework for understanding the systemic nature of governance challenges. Furthermore, it offers a model for integrating institutional arrangements, coordination mechanisms, and enforcement processes. Through this approach, the study contributes to the development of more coherent and effective cybersecurity governance systems in Indonesia.

2. Literature Review

Integrated governance has emerged as a critical framework for addressing complex policy challenges that involve multiple actors, institutions, and regulatory domains. It emphasizes the coordination and alignment of institutional actions to achieve coherent policy outcomes. Haapasaari et al. (2021) define integrated governance as an approach that seeks to manage multidimensional problems through coordinated institutional arrangements and shared objectives. Similarly, Aoki et al. (2024) highlight that whole-of-government approaches aim to overcome institutional silos by promoting collaboration and integration across public sector entities. These frameworks recognize that fragmentation undermines governance effectiveness by limiting coordination and coherence. As a result, integrated governance is increasingly viewed as a necessary condition for effective policy

implementation. This suggests that governance systems must evolve toward more coordinated and collaborative structures.

The role of coordination and collaborative governance is central to the functioning of integrated governance systems. Effective coordination enables institutions to align their actions, share information, and jointly address complex policy challenges. Voets et al. (2021) emphasize that collaborative governance involves structured interaction among public sector actors to achieve shared policy goals. Klijn et al. (2025) further argue that governance networks provide a framework for managing interdependencies among institutions in multi-actor environments. Vantaggiato et al. (2021) demonstrate that overcoming institutional silos requires deliberate efforts to enhance cross-departmental interaction and coordination. However, coordination is often hindered by institutional barriers, including differences in organizational culture and competing objectives. These challenges indicate that coordination mechanisms must be carefully designed to ensure effective collaboration.

Governance models and policy design play a crucial role in shaping how integrated governance systems operate in practice. Governance models provide the structural framework through which institutions interact and implement policies. Pierre (2022) emphasizes that policy design must account for institutional complexity and interdependence to ensure effective governance outcomes. Peters (2022) further highlight that institutional theory provides insights into how governance structures influence policy implementation. Asaduzzaman and Virtanen (2023) argue that governance models must incorporate both structural and relational

dimensions to address complex policy challenges. These perspectives indicate that effective governance requires not only coordination but also well-designed institutional frameworks. Consequently, governance models must be tailored to support integration and collaboration.

The integration of enforcement and institutional capacity within governance systems is essential for ensuring that regulatory frameworks achieve their intended objectives. Enforcement capacity determines whether legal norms can be translated into actual behavior, while institutional capacity influences the ability of governance systems to operate effectively. Andarge and Lichtenberg (2020) highlight that enforcement effectiveness depends on the consistency and credibility of institutional actions. Sumkoski et al. (2025) further emphasize that weak regulatory management reduces the ability of institutions to enforce legal norms effectively. These findings suggest that enforcement and capacity are interconnected components of governance systems. When either element is weak, regulatory effectiveness is compromised. Therefore, integrated governance must incorporate both enforcement mechanisms and institutional capacity to function effectively.

The specific context of cybersecurity governance introduces additional complexity, as it requires coordination among multiple institutions with diverse roles and capabilities. Cybersecurity governance involves regulatory, enforcement, and technical dimensions that must be aligned to address evolving digital threats. Yusif and Hafeez-Baig (2021) propose a conceptual model for cybersecurity governance that emphasizes the integration of institutional roles and processes. Del-Real and Díaz-Fernández (2022) further demonstrate that cybersecurity governance often

involves overlapping institutional arrangements that complicate coordination. Teichmann and Sergi (2025) highlight that hybrid governance approaches are increasingly used to address the complexity of cybersecurity regulation. These perspectives indicate that cybersecurity governance requires integrated approaches that combine legal, institutional, and operational dimensions. As a result, developing integrated governance models is essential for improving cybersecurity outcomes.

Overall, the literature suggests that integrated governance, coordination mechanisms, governance models, and enforcement capacity are interdependent elements that determine the effectiveness of regulatory systems. Fragmentation undermines coordination, while weak enforcement and limited capacity reduce the ability of governance systems to achieve policy objectives. This relationship highlights the need for comprehensive frameworks that address these dimensions collectively. The insights reviewed in this section provide a foundation for analyzing how integrated governance can improve cybersecurity governance in Indonesia. They also support the argument that effective governance requires alignment between institutional structures, coordination mechanisms, and enforcement processes. Therefore, this study builds on these perspectives to develop an integrated governance model tailored to the Indonesian context.

3. Methods

This study employs a normative juridical research method combined with systematic and sociological approaches to analyze the development of an integrated cybersecurity governance model in Indonesia. The normative juridical approach is

used to examine legal frameworks and institutional arrangements governing cybersecurity, including the allocation of authority, regulatory coordination, and enforcement responsibilities across agencies. This enables the identification of how governance structures are formally designed and how integration is addressed within existing legal instruments. However, as policy design scholarship emphasizes, the effectiveness of governance systems depends not only on formal structures but also on how institutions interact in practice. Peters (2022) highlights that institutional design shapes policy outcomes by influencing coordination and implementation processes. Therefore, this study extends beyond doctrinal analysis to evaluate how governance integration can be achieved within existing institutional frameworks.

The systematic approach is applied to analyze the relationships between fragmentation, enforcement capacity, and coordination mechanisms within Indonesia's cybersecurity governance system. This involves examining how institutional structures interact, where coordination failures occur, and how these factors influence governance outcomes. Chowdhury (2022) emphasizes that variations in state capacity significantly affect the performance of governance systems, particularly in complex regulatory environments. In addition, a sociological approach is used to assess how institutions collaborate and coordinate in practice, focusing on patterns of interaction and information sharing. Voets et al. (2021) highlight that collaborative governance requires structured interaction among institutions to achieve shared objectives. By integrating these approaches, the study captures both the formal design and practical operation of governance systems. This

provides a comprehensive basis for developing an integrated governance model that addresses structural and operational challenges in cybersecurity governance.

4. Results

4.1. Structural Barriers to Integrated Cybersecurity Governance

The findings indicate that the development of integrated cybersecurity governance in Indonesia is constrained by persistent institutional fragmentation and limited coordination mechanisms. Governance structures involve multiple institutions with distinct mandates that are not fully aligned, resulting in siloed policy implementation. Vantaggiato et al. (2021) demonstrate that cross-departmental interaction is often hindered by institutional barriers that limit coordination and information sharing. Similarly, Klijn et al. (2025) highlight that governance networks require structured coordination mechanisms to manage interdependencies among actors effectively. In the absence of such mechanisms, institutions operate independently, leading to fragmented governance outcomes. This indicates that structural fragmentation remains a primary barrier to integration. Consequently, achieving integrated governance requires addressing these coordination deficiencies.

Institutional silos further exacerbate governance fragmentation by limiting collaboration and preventing the alignment of policy objectives across agencies. Haapasaari et al. (2021) emphasize that integrated governance requires coordinated institutional arrangements to address multidimensional policy challenges. However, Voets et al. (2021) highlight that collaborative governance is often constrained by organizational boundaries and differences in institutional priorities. In Indonesia,

these conditions manifest in limited inter-agency collaboration and weak mechanisms for joint decision-making. This reduces the ability of institutions to develop cohesive strategies for cybersecurity governance. As a result, governance systems remain fragmented and unable to respond effectively to complex digital risks. Therefore, overcoming institutional silos is essential for achieving integration.

In addition to fragmentation, limited enforcement capacity further constrains the development of integrated governance systems. Effective integration requires institutions to possess the capacity to implement coordinated policies and enforce regulations consistently. Geddes (2023) emphasizes that institutional capacity is a key determinant of governance performance, particularly in complex policy environments. Chowdhury (2022) similarly highlights that variations in state capacity affect the ability of governments to implement integrated policy approaches. In Indonesia, capacity limitations are reflected in insufficient resources, lack of technical expertise, and weak organizational structures. These constraints reduce the ability of institutions to coordinate enforcement actions and implement integrated strategies. Consequently, capacity limitations reinforce fragmentation and hinder governance integration.

The interaction between fragmentation and enforcement challenges creates a systemic governance gap in which legal frameworks are not effectively operationalized. Andarge and Lichtenberg (2020) highlight that enforcement effectiveness depends on consistent and coordinated institutional action. Sumkoski et al. (2025) further emphasize that weak regulatory management reduces the ability of governance systems to enforce legal norms effectively. In Indonesia, fragmented

institutional arrangements and limited capacity result in inconsistent enforcement and weak regulatory outcomes. This creates a gap between legal provisions and their practical implementation. As a result, cybersecurity governance remains ineffective despite the presence of formal regulatory frameworks. These findings indicate that structural barriers must be addressed to enable integration.

4.1. Integrated Governance Model for Cybersecurity

The findings support the development of an integrated governance model that aligns institutional structures, coordination mechanisms, and enforcement processes to improve cybersecurity governance. Integrated governance requires the establishment of mechanisms that facilitate coordination, information sharing, and joint decision-making among institutions. Aoki et al. (2024) highlight that whole-of-government approaches are essential for overcoming institutional silos and enhancing policy coherence. Pierre (2022) further emphasizes that effective governance models must account for institutional complexity and interdependence. In the Indonesian context, this implies the need for frameworks that integrate regulatory, enforcement, and technical functions. Such integration would enable institutions to operate as part of a cohesive governance system. Therefore, the development of an integrated governance model is essential for improving regulatory effectiveness.

A key component of the integrated governance model is the establishment of structured coordination mechanisms that enable institutions to align their actions and share information effectively. Klijn et al. (2025) highlight that governance networks provide a framework for managing interdependencies among actors in

complex policy environments. Voets et al. (2021) further emphasize that collaborative governance requires formalized interaction and clearly defined roles among participating institutions. In practice, this involves creating coordination platforms, joint task forces, and shared information systems that facilitate cooperation. These mechanisms reduce fragmentation and improve the consistency of policy implementation. As a result, coordination becomes a central element of integrated governance. This highlights the importance of institutional alignment in achieving effective governance outcomes.

The integration of cybersecurity governance also requires aligning institutional roles and regulatory frameworks to ensure coherence across different policy domains. Yusif and Hafeez-Baig (2021) propose that effective cybersecurity governance models must integrate institutional responsibilities and processes to address complex threats. Del-Real and Díaz-Fernández (2022) further demonstrate that overlapping institutional arrangements can be managed through structured coordination and resource sharing. In Indonesia, this implies the need to harmonize legal frameworks and clarify institutional mandates to reduce ambiguity. Such alignment would enhance the ability of institutions to coordinate their actions and implement policies consistently. Consequently, regulatory coherence becomes a key outcome of integrated governance. This indicates that institutional alignment is essential for effective cybersecurity governance.

Finally, the integrated governance model must incorporate hybrid governance approaches that combine regulatory frameworks, enforcement mechanisms, and institutional capacity to address cybersecurity challenges effectively. Teichmann and

Sergi (2025) highlight that hybrid governance enables the integration of multiple regulatory instruments and actors within a unified framework. Savaş and Karataş (2022) further emphasize that cybersecurity governance requires the coordination of legal, technical, and organizational components. By integrating these elements, governance systems can respond more effectively to evolving digital threats. This approach enhances both the flexibility and effectiveness of regulatory systems. As a result, integrated governance provides a comprehensive solution to the challenges identified in previous sections. These findings demonstrate that improving cybersecurity governance requires a systemic approach that aligns institutional structures, coordination mechanisms, and enforcement processes.

5. Discussion

The findings of this study demonstrate that the challenges of cybersecurity governance in Indonesia are systemic and cannot be addressed through isolated reforms in legal frameworks, institutional structure, or enforcement capacity alone. Previous analyses have shown that legal effectiveness is limited, institutional arrangements are fragmented, and enforcement capacity is constrained, but these issues are deeply interconnected rather than independent. Fragmentation reduces coordination, weak coordination undermines enforcement, and limited enforcement capacity further weakens governance outcomes. As a result, cybersecurity governance operates as a disjointed system in which legal provisions, institutional roles, and enforcement mechanisms fail to align. This systemic misalignment explains why existing regulatory frameworks are unable to effectively address digital

risks. Consequently, governance reform must move beyond sectoral improvements toward comprehensive system integration.

The proposed integrated governance model highlights that effective cybersecurity governance requires alignment across institutional structures, coordination mechanisms, and enforcement processes. Integration enables institutions to operate within a unified framework where responsibilities are clearly defined, information is shared, and actions are coordinated. This reduces duplication, enhances accountability, and improves the consistency of regulatory implementation. Moreover, integrating enforcement capacity into governance design ensures that legal frameworks are supported by operational capability. Without such integration, even well-designed legal systems will continue to produce suboptimal outcomes. Therefore, governance effectiveness depends on the ability to synchronize institutional functions rather than merely expanding regulatory frameworks.

From a broader perspective, the transition toward integrated cybersecurity governance represents a shift from fragmented and reactive systems to coordinated and proactive governance models. This transformation requires not only structural reforms but also changes in institutional behavior, including increased collaboration and shared responsibility among agencies. Developing coordination platforms, enhancing information-sharing mechanisms, and clarifying institutional mandates are essential steps in this process. In addition, strengthening enforcement capacity must be integrated into governance design to ensure that regulatory systems can respond effectively to evolving challenges. Without these changes, governance

systems will remain constrained by structural inefficiencies and limited operational capability. Therefore, the future of cybersecurity governance in Indonesia depends on the successful implementation of integrated governance principles.

6. Conclusion

This study concludes that the effectiveness of cybersecurity governance in Indonesia is constrained by a combination of institutional fragmentation, weak enforcement capacity, and limited coordination mechanisms, which collectively prevent regulatory frameworks from functioning as an integrated system. While legal instruments provide a formal basis for regulating digital activities, their impact is diminished by structural and operational limitations within governance systems. This indicates that the core problem is not the absence of regulation, but the lack of integration among institutional components responsible for implementation and enforcement. As a result, governance systems operate in a fragmented and inconsistent manner, reducing their ability to address complex cybersecurity challenges. Therefore, improving cybersecurity governance requires a systemic approach that addresses the interconnection between institutional structure, coordination, and enforcement capacity.

The findings further demonstrate that integrated governance provides a viable framework for overcoming these challenges by aligning institutional roles, coordination mechanisms, and enforcement processes within a unified system. Integration enhances the ability of institutions to share information, coordinate actions, and implement policies consistently, thereby improving governance

effectiveness. It also ensures that enforcement capacity is embedded within governance design, allowing legal frameworks to be operationalized more effectively. By reducing fragmentation and strengthening coordination, integrated governance can transform regulatory systems into cohesive and responsive structures. This highlights the importance of moving beyond isolated reforms toward comprehensive governance redesign. Consequently, integration becomes a key determinant of effective cybersecurity governance.

Finally, this study emphasizes that the future of cybersecurity governance in Indonesia depends on the successful implementation of integrated governance principles that prioritize coordination, institutional alignment, and enforcement capability. Achieving this requires not only legal and institutional reforms but also sustained efforts to build capacity, improve collaboration, and develop mechanisms for joint decision-making. Such reforms would enable governance systems to respond more effectively to evolving digital risks and ensure the consistent application of regulatory frameworks. In addition, the development of integrated governance models can serve as a foundation for broader digital governance reforms. Therefore, the transition toward integrated cybersecurity governance is essential for enhancing regulatory performance and ensuring long-term resilience in Indonesia's digital ecosystem.

References

Andarge, T., & Lichtenberg, E. (2020). Regulatory compliance under enforcement gaps. *Journal of Regulatory Economics, 57*(3), 181–202.

Aoki, N., Tay, M., & Rawat, S. (2024). Whole-of-government and joined-up government: A systematic literature review. *Public Administration, 102*(2), 733–752.

Asaduzzaman, M., & Virtanen, P. (2023). Governance theories and models. In *Global Encyclopedia of Public Administration, Public Policy, and Governance* (pp. 5947–5958). Springer.

Chowdhury, A. (2022). Regulation and state capacity. *Rationality and Society, 34*(4), 446–468.

Del-Real, C., & Díaz-Fernández, A. M. (2022). Understanding the plural landscape of cybersecurity governance in Spain: A matter of capital exchange. *International Cybersecurity Law Review, 3*(2), 313–343.

Geddes, B. (2023). *Politician's dilemma: Building state capacity in Latin America*. University of California Press.

Haapasaari, P., Ignatius, S., Pihlajamäki, M., Bryhn, A., Sarkki, S., Tuomisto, J., et al. (2021). Integrated governance for managing multidimensional problems: Potentials, challenges, and arrangements. *Marine Policy, 123*, 104276.

Klijn, E. H., Koppenjan, J., Spekkink, W., & Warsen, R. (2025). *Governance networks in the public sector*. Routledge.

Peters, B. G. (2022). Institutions, institutional theory and policy design. In *Research Handbook of Policy Design* (pp. 54–71). Edward Elgar Publishing.

Pierre, J. (2022). Governance models and policy design. In *Research Handbook of Policy Design* (pp. 296–309). Edward Elgar Publishing.

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), 7–34.

Sumkoski, G., Kocherbaeva, A., & Alapaeva, A. (2025). Regulatory management: Weaknesses and potential for improvement. *Upravlencheskie Nauki, 15*(4), 78–93.

Teichmann, F., & Sergi, B. S. (2025). The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem. *Computer Law & Security Review, 59*, 106209.

Vantaggiato, F. P., Kassim, H., & Connolly, S. (2021). Breaking out of silos: Explaining cross-departmental interactions in two European bureaucracies. *Journal of European Public Policy, 28*(9), 1432–1452.

Voets, J. J., Brandsen, T., Verschuere, B., & Koliba, C. (2021). Collaborative governance.

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research, 16*(4), 490–513.