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

Fragmented Cybersecurity Governance in Indonesia: Institutional Overlap and Its Impact on Regulatory Enforcement

Elsa Laila Rohmah [1]

[1] Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, Indonesia

Abstract

Article history:
Received: July 27, 2025
Revised: September 4, 2025
Accepted: October 25, 2025
Published: December 30, 2025

Keywords:
Coordination,
Cybersecurity Governance,
Enforcement,
Governance Fragmentation,
Institutional Overlap,
Regulatory Effectiveness.

Identifier:
Zera Open
Page: 139-159
https://zeraopen.com/journal/jclis

The increasing complexity of digital governance has led to the expansion of cybersecurity regulatory frameworks involving multiple institutions with overlapping mandates. This study examines how institutional fragmentation affects the effectiveness of cybersecurity governance in Indonesia and analyzes the impact of regulatory overlap on enforcement. Using a normative juridical method combined with systematic and sociological approaches, the research evaluates the relationship between institutional structures and regulatory outcomes. The findings indicate that although Indonesia has established a comprehensive legal and institutional framework, governance remains fragmented due to overlapping authority, weak coordination mechanisms, and unclear institutional mandates. This fragmentation leads to inconsistent policy implementation and undermines enforcement effectiveness. The study further demonstrates that enforcement failure is a structural consequence of fragmented governance rather than the absence of legal regulation. It concludes that improving cybersecurity governance requires strengthening institutional coordination, clarifying authority, and developing integrated governance mechanisms to ensure effective and consistent enforcement.

*Corresponding author:
(Elsa Laila Rohmah)

1. Introduction

The rapid expansion of digital governance has significantly increased the complexity of regulatory systems, particularly in areas such as cybersecurity and data protection where multiple institutions are involved. As digital risks evolve, governments are required to develop legal and institutional frameworks capable of coordinating responses across diverse regulatory domains. However, the growth of regulatory frameworks is often accompanied by the proliferation of institutions with overlapping mandates and responsibilities. Kitchin and Moore-Cherry (2021) highlight that fragmented governance structures are a common feature in complex policy environments, particularly where multiple actors operate within interconnected systems. Similarly, Peters et al. (2022) emphasize that modern public administration increasingly involves multi-level and multi-actor governance arrangements that require high levels of coordination. This indicates that governance complexity is not only a matter of regulatory expansion but also of institutional design and interaction.

The emergence of multi-agency governance systems in cybersecurity reflects the need to address diverse and evolving digital threats through specialized institutional roles. Legal and policy frameworks often distribute responsibilities across various agencies to enhance expertise and responsiveness. However, such distribution of authority can create overlapping jurisdictions and regulatory ambiguity when coordination mechanisms are insufficient. Haftel and Lenz (2022) argue that institutional overlap in governance systems can lead to inefficiencies and conflicts in policy implementation. Kreuder-Sonnen and Zürn (2020) further

emphasize that fragmentation often results in interface conflicts, where different institutions pursue competing or unaligned objectives. These dynamics suggest that institutional complexity may undermine rather than strengthen governance effectiveness. Consequently, the presence of multiple regulatory actors must be evaluated in terms of their ability to operate cohesively rather than independently.

Institutional fragmentation becomes particularly problematic when it affects the coordination of policy implementation and regulatory enforcement. Effective governance requires not only the distribution of authority but also the integration of institutional actions through coherent coordination mechanisms. Trein and Maggetti (2020) highlight that fragmented governance systems often struggle to align policy objectives and instruments, resulting in inconsistent implementation. De Wulf et al. (2023) further demonstrate that coordination barriers within fragmented systems reduce the capacity of institutions to deliver coherent policy outcomes. These findings indicate that fragmentation introduces structural constraints that limit the effectiveness of governance systems. As a result, regulatory frameworks may fail to achieve their intended objectives despite being formally well-designed. This suggests that governance effectiveness depends on the degree of institutional integration rather than the mere presence of multiple actors.

In the Indonesian context, cybersecurity governance is characterized by the involvement of multiple institutions with distinct but interconnected roles, including regulatory authorities, enforcement bodies, and technical agencies. Legal instruments such as Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan

Transaksi Elektronik, and institutional arrangements related to the National Cyber and Crypto Agency (BSSN) collectively form the foundation of cybersecurity governance. However, the distribution of responsibilities across these frameworks has created challenges related to coordination and authority clarity. Priyandita (2025) highlights that Indonesia's cybersecurity governance faces limitations in institutional coordination, particularly in responding to complex cyber threats. Similarly, Aji (2025) emphasizes that overlapping institutional roles and unclear authority boundaries hinder effective governance. These conditions suggest that Indonesia's cybersecurity system reflects broader patterns of fragmented governance. Consequently, the effectiveness of cybersecurity regulation cannot be fully understood without examining the structure of institutional relationships.

The implications of institutional fragmentation extend beyond coordination challenges to affect the enforcement of legal frameworks. When responsibilities are distributed across multiple agencies without clear coordination mechanisms, enforcement becomes inconsistent and less effective. Andarge and Lichtenberg (2020) argue that regulatory effectiveness is closely tied to the credibility and consistency of enforcement, which are undermined in fragmented systems. In such conditions, institutions may operate independently or pursue overlapping mandates, reducing accountability and weakening regulatory impact. This creates a situation in which legal frameworks exist but are not effectively enforced in practice. As a result, fragmentation transforms governance systems into loosely connected structures rather than integrated regulatory regimes. This highlights the need to analyze enforcement not only as a legal function but as an outcome of institutional design.

Based on these considerations, this study aims to analyze the impact of institutional fragmentation on the effectiveness of cybersecurity governance in Indonesia and to examine how regulatory overlap and weak coordination undermine enforcement. Using a normative juridical method combined with systematic and sociological approaches, the study evaluates the relationship between institutional structures and regulatory outcomes. The analysis focuses on identifying how fragmented governance systems affect coordination, authority distribution, and enforcement capacity. By shifting the focus from legal provisions to governance structures, this research provides a deeper understanding of the underlying causes of regulatory ineffectiveness. Furthermore, it offers insights into how institutional integration and coordination can enhance the performance of cybersecurity governance. Through this approach, the study contributes to the development of more coherent and effective digital governance systems in Indonesia.

2. Literature Review

Institutional fragmentation has emerged as a central concept in understanding governance challenges within complex policy environments, particularly where multiple actors operate across overlapping jurisdictions. Fragmentation refers to the distribution of authority across institutions that are only loosely coordinated, often resulting in inconsistent policy implementation and reduced effectiveness. Haftel and Lenz (2022) conceptualize institutional overlap as a condition in which multiple governance bodies possess intersecting mandates, creating potential conflicts and inefficiencies. Similarly, Kreuder-Sonnen and Zürn (2020) argue that fragmented

governance systems frequently produce norm collisions and interface conflicts that undermine policy coherence. Kitchin and Moore-Cherry (2021) further demonstrate that fragmented governance structures in data-driven environments lead to coordination challenges and inconsistent regulatory outcomes. These perspectives indicate that fragmentation is not merely an organizational feature but a structural condition that shapes governance effectiveness.

The issue of coordination is closely linked to institutional fragmentation, as effective governance depends on the ability of multiple actors to align their actions and objectives. Coordination mechanisms serve to integrate institutional activities, ensuring that policy implementation is coherent and consistent across different levels and sectors. Trein et al. (2021) emphasize that policy coordination is essential for managing complex governance systems and avoiding conflicting policy outcomes. Hustedt and Radtke (2024) further highlight that coordination plays a critical role in policy implementation by facilitating communication and cooperation among institutions. An et al. (2021) also demonstrate that inter-agency collaboration enhances governance capacity, particularly in addressing cross-sectoral challenges. However, when coordination mechanisms are weak or absent, fragmentation leads to siloed institutional behavior. As a result, governance systems become less capable of producing integrated and effective policy outcomes.

The relationship between institutional fragmentation and enforcement effectiveness is a critical dimension of regulatory governance that has received increasing attention in recent scholarship. Enforcement requires clarity of authority, consistent application of rules, and coordination among responsible institutions.

Andarge and Lichtenberg (2020) argue that regulatory compliance is strongly influenced by the credibility and consistency of enforcement, which are weakened in fragmented systems. Sumkoski et al. (2025) further emphasize that regulatory systems characterized by unclear authority and fragmented governance structures face significant challenges in enforcing legal norms effectively. These findings indicate that enforcement failure is often a structural consequence of institutional fragmentation rather than a result of inadequate legal provisions. When multiple institutions share overlapping responsibilities without clear coordination, enforcement becomes inconsistent and less predictable. Consequently, the effectiveness of legal frameworks is significantly reduced.

To address the challenges associated with fragmentation, the concept of integrated or whole-of-government governance has been developed as a strategic approach to enhance coordination and policy coherence. Integrated governance emphasizes collaboration across institutions, alignment of policy objectives, and the development of mechanisms that facilitate information sharing and joint decision-making. Aoki et al. (2024) define whole-of-government approaches as efforts to overcome institutional silos by promoting coordinated action across public sector entities. Cairney (2025) further highlights that policy coherence and integration are essential for improving governance effectiveness in complex policy environments. These approaches suggest that fragmentation can be mitigated through structural and relational reforms that enhance coordination and collaboration. However, the implementation of integrated governance remains challenging, particularly in contexts where institutional fragmentation is deeply embedded. This indicates that

achieving effective coordination requires both institutional redesign and cultural change within governance systems.

The Indonesian context illustrates how institutional fragmentation and coordination challenges affect cybersecurity governance in practice. The involvement of multiple agencies in cybersecurity regulation and enforcement reflects an attempt to address complex digital risks through specialized institutional roles. However, empirical studies indicate that coordination among these institutions remains limited, resulting in inefficiencies and overlapping responsibilities. Maskun et al. (2022) highlight that fragmented institutional arrangements in Indonesia create barriers to effective policy implementation, particularly in complex regulatory domains. Siti-Nabiha et al. (2023) further demonstrate that fragmentation in public sector governance reduces the effectiveness of policy coordination and performance outcomes. Priyandita (2025) emphasizes that Indonesia's cybersecurity governance faces challenges related to institutional alignment and strategic coordination. These findings indicate that fragmentation is a key factor shaping the effectiveness of cybersecurity governance in Indonesia.

Overall, the literature suggests that institutional fragmentation, coordination failure, and enforcement weakness are interconnected dimensions of governance effectiveness. Fragmentation creates structural barriers that hinder coordination, while weak coordination undermines enforcement capacity and regulatory outcomes. This relationship highlights the importance of analyzing governance systems as integrated structures rather than isolated components. The theoretical and empirical insights reviewed in this section provide a foundation for examining

how institutional fragmentation affects cybersecurity governance in Indonesia. They also support the argument that improving governance effectiveness requires addressing structural issues related to institutional design and coordination mechanisms. Therefore, the study builds on this literature to analyze the impact of fragmentation on enforcement and regulatory effectiveness in Indonesia's cybersecurity governance system.

3. Methods

This study employs a normative juridical research method combined with systematic and sociological approaches to analyze the impact of institutional fragmentation on the effectiveness of cybersecurity governance in Indonesia. The normative juridical approach is used to examine legal frameworks and institutional arrangements governing cybersecurity, including the distribution of authority across multiple agencies and regulatory instruments. This approach enables the identification of formal structures that define institutional roles, responsibilities, and regulatory objectives. However, as governance research emphasizes, the existence of formal institutional arrangements does not necessarily ensure effective coordination or implementation. Trein et al. (2021) highlight that governance effectiveness depends on how institutional relationships are structured and managed within complex policy environments. Therefore, this study extends beyond formal legal analysis to evaluate how fragmentation affects governance performance in practice.

The systematic approach is applied to analyze the relationships between institutions, regulatory frameworks, and coordination mechanisms within

Indonesia's cybersecurity governance system. This involves examining how authority is distributed across agencies, how responsibilities overlap, and how institutional interactions influence policy implementation and enforcement. Hustedt and Radtke (2024) emphasize that coordination is a critical component of policy implementation, particularly in systems involving multiple actors and overlapping mandates. By using a systematic perspective, this study identifies structural inconsistencies and gaps that contribute to fragmentation and weak coordination. This approach allows for the evaluation of whether the governance system operates as an integrated framework or as a collection of disconnected institutional arrangements. Consequently, it provides a basis for understanding how fragmentation affects regulatory coherence and enforcement outcomes.

In addition, a sociological approach is employed to assess how institutional fragmentation influences coordination behavior and enforcement practices in real-world governance contexts. This approach focuses on the interaction between institutions, including patterns of collaboration, communication, and authority negotiation. An et al. (2021) highlight that inter-agency collaboration is essential for addressing complex policy challenges, particularly in environments requiring coordinated responses. Eriksson et al. (2020) further emphasize that collaborative governance depends on shared objectives and coordinated value creation among public institutions. In fragmented systems, however, such collaboration is often limited, leading to siloed behavior and inconsistent enforcement. By incorporating a sociological perspective, this study captures the "governance in action" dimension

of fragmentation and coordination. This enables a more comprehensive analysis of how institutional dynamics shape the effectiveness of cybersecurity governance.

The sources of legal materials used in this study consist of primary and secondary materials selected based on relevance and academic rigor. Primary materials include laws and regulations governing cybersecurity and digital governance in Indonesia, while secondary materials consist of peer-reviewed academic literature on institutional fragmentation, coordination, and enforcement. The analysis is conducted through qualitative legal interpretation, supported by systematic reasoning and sociological insights into institutional behavior. As noted in regulatory governance studies, enforcement effectiveness is closely linked to institutional design and coordination capacity rather than legal provisions alone (Andarge & Lichtenberg, 2020; Sumkoski et al., 2025). This methodological approach enables the study to identify structural weaknesses in governance systems and their implications for enforcement. It also provides a robust analytical framework for addressing the research questions related to fragmentation and regulatory effectiveness.

4. Results

4.1. Institutional Fragmentation and Governance Ineffectiveness

The findings indicate that cybersecurity governance in Indonesia is characterized by institutional fragmentation, where multiple agencies operate with distinct yet overlapping mandates. This fragmentation arises from the distribution of authority across legal and institutional frameworks that are not fully integrated.

Haftel and Lenz (2022) explain that institutional overlap occurs when multiple governance bodies possess intersecting responsibilities, often leading to inefficiencies in implementation. In the Indonesian context, Maskun et al. (2022) highlight that fragmented institutional arrangements create barriers to effective policy implementation, particularly in complex regulatory domains. These conditions suggest that governance structures are designed in a manner that distributes authority without ensuring adequate coordination mechanisms. As a result, the effectiveness of cybersecurity governance is constrained by structural fragmentation rather than the absence of legal frameworks.

A key manifestation of institutional fragmentation is the presence of overlapping authority among agencies responsible for cybersecurity governance. Legal frameworks assign responsibilities to different institutions, including regulatory bodies, enforcement agencies, and technical authorities, often without clearly delineating their roles. Kreuder-Sonnen and Zürn (2020) argue that such overlap generates interface conflicts, where institutions pursue unaligned or competing objectives. Similarly, Aji (2025) highlights that overlapping mandates in Indonesia's cybersecurity governance create ambiguity in authority and hinder effective coordination. This ambiguity leads to uncertainty in decision-making processes and reduces accountability among institutions. As a result, governance becomes fragmented across multiple actors with limited alignment. Consequently, overlapping authority weakens the coherence of regulatory implementation.

Institutional fragmentation also affects the coordination of policy implementation, limiting the ability of governance systems to function cohesively.

Effective governance requires mechanisms that facilitate communication, collaboration, and alignment among institutions. An et al. (2021) emphasize that inter-agency coordination enhances governance capacity by enabling institutions to address complex challenges collectively. However, De Wulf et al. (2023) demonstrate that fragmented governance systems often face significant coordination barriers, resulting in siloed institutional behavior. In Indonesia, the lack of effective coordination mechanisms prevents institutions from aligning their actions and policy objectives. This leads to inconsistencies in policy implementation and reduces the overall effectiveness of governance. Therefore, coordination failure emerges as a direct consequence of institutional fragmentation.

The combined effect of fragmentation and weak coordination results in governance systems that are unable to deliver coherent and effective policy outcomes. Trein and Maggetti (2020) argue that policy integration is essential for aligning objectives and instruments across governance systems, particularly in complex policy environments. Priyandita (2025) further highlights that Indonesia's cybersecurity governance faces challenges related to institutional alignment and strategic coordination. Without effective integration, governance systems operate as disconnected entities rather than cohesive frameworks. This fragmentation leads to inefficiencies, duplication of efforts, and inconsistent policy outcomes. Consequently, the effectiveness of cybersecurity governance is significantly reduced. These findings indicate that institutional fragmentation is a fundamental constraint on governance effectiveness.

4.1. Regulatory Overlap and Enforcement Failure

The findings further indicate that regulatory overlap and institutional fragmentation directly contribute to weaknesses in enforcement within Indonesia's cybersecurity governance system. Enforcement requires clarity of authority and coordination among institutions responsible for implementing legal frameworks. However, when responsibilities are distributed across multiple agencies with overlapping mandates, enforcement becomes inconsistent and less effective. Andarge and Lichtenberg (2020) argue that the credibility and effectiveness of enforcement depend on consistent application of legal norms, which is difficult to achieve in fragmented systems. Sumkoski et al. (2025) further emphasize that unclear authority and fragmented governance structures reduce the capacity of institutions to enforce regulations effectively. These conditions suggest that enforcement failure is a structural outcome of fragmented governance. As a result, legal frameworks are not fully operationalized in practice.

Institutional ambiguity further exacerbates enforcement challenges by creating uncertainty regarding roles and responsibilities among regulatory bodies. Effective enforcement depends on clearly defined institutional mandates that enable agencies to act decisively and consistently. Hustedt and Radtke (2024) highlight that coordination and clarity of roles are essential for effective policy implementation, particularly in multi-actor governance systems. Maskun et al. (2022) similarly emphasize that fragmented institutional arrangements in Indonesia create obstacles to effective enforcement. In such environments, institutions may either duplicate efforts or fail to act due to uncertainty about jurisdiction. This reduces accountability

and weakens the overall enforcement process. Consequently, institutional ambiguity becomes a critical barrier to effective cybersecurity governance.

The lack of coordination among institutions also undermines enforcement by limiting the ability of agencies to share information and align their actions. Enforcement in cybersecurity governance often requires collaboration across agencies, including regulatory bodies, law enforcement, and technical institutions. Eriksson et al. (2020) emphasize that collaborative governance enhances the effectiveness of public sector actions by promoting coordinated value creation. Similarly, An et al. (2021) highlight that inter-agency collaboration is essential for addressing complex governance challenges. However, in fragmented systems, coordination mechanisms are weak or absent, leading to isolated institutional actions. This results in inconsistent enforcement and reduced regulatory impact. Therefore, weak coordination directly contributes to enforcement failure.

The persistence of enforcement weaknesses ultimately leads to broader governance failures, where legal frameworks are unable to achieve their intended objectives. In the absence of effective enforcement, regulatory systems lose their deterrent function and fail to influence behavior. Priyandita (2025) highlights that Indonesia's cybersecurity governance continues to face challenges in achieving effective enforcement due to institutional limitations. Aoki et al. (2024) further emphasize that overcoming such challenges requires integrated governance approaches that enhance coordination across institutions. Without such integration, governance systems remain fragmented and ineffective. This creates a regulatory environment in which cyber risks persist despite the presence of legal frameworks.

Consequently, strengthening enforcement requires addressing the underlying structural issues related to fragmentation and coordination.

5. Discussion

The findings of this study demonstrate that the central challenge of cybersecurity governance in Indonesia is not the absence of legal frameworks, but the fragmented institutional structure through which these frameworks are implemented. While multiple laws and agencies exist to regulate digital activities, their effectiveness is constrained by the lack of integration among governing institutions. This fragmentation creates a governance environment in which authority is distributed without sufficient coordination, leading to inconsistencies in policy implementation. As a result, governance operates through parallel institutional processes rather than a unified system. This structural condition prevents legal frameworks from functioning as coherent regulatory instruments. Consequently, the effectiveness of cybersecurity governance is limited by institutional design rather than normative inadequacy.

The interaction between institutional fragmentation and coordination failure further reveals that governance effectiveness depends on the alignment of institutional roles and responsibilities. When agencies operate within overlapping jurisdictions without clear coordination mechanisms, enforcement becomes inconsistent and less predictable. This weakens the credibility of regulatory systems and reduces their capacity to influence behavior. In such conditions, institutions may either duplicate efforts or fail to act due to uncertainty regarding authority, both of

which undermine enforcement effectiveness. Moreover, the absence of coordinated action prevents the development of shared strategies for addressing complex cybersecurity challenges. This indicates that coordination is not merely a procedural element but a fundamental requirement for effective governance. Therefore, improving enforcement requires restructuring institutional relationships to ensure clarity and alignment.

From a broader governance perspective, the findings highlight the need to shift from fragmented institutional arrangements toward integrated governance models that emphasize coordination and collaboration. Addressing fragmentation requires not only clarifying institutional mandates but also developing mechanisms that facilitate communication, information sharing, and joint decision-making. A more integrated approach would enable institutions to operate as part of a cohesive system rather than as isolated entities. Such transformation is essential for improving the consistency and effectiveness of enforcement in cybersecurity governance. In addition, strengthening coordination can enhance accountability by clearly defining roles and responsibilities across institutions. Without these reforms, governance systems will continue to produce fragmented and suboptimal outcomes. Therefore, the improvement of cybersecurity governance in Indonesia depends on the ability to align institutional structures with regulatory objectives.

6. Conclusion

This study concludes that the effectiveness of cybersecurity governance in Indonesia is fundamentally constrained by institutional fragmentation rather than

the absence of legal frameworks. Although multiple regulations and agencies exist to govern cybersecurity and data protection, their impact is limited by the lack of coordination and integration among institutions. This indicates that governance effectiveness depends not only on the existence of legal instruments but also on how institutional structures are organized and aligned. Fragmented arrangements create inconsistencies in implementation and reduce the overall coherence of regulatory systems. As a result, legal frameworks are unable to function as effective tools for managing digital risks. Therefore, the primary limitation of cybersecurity governance in Indonesia lies in its structural configuration rather than its normative foundation.

The findings further demonstrate that regulatory overlap and unclear institutional mandates significantly undermine enforcement effectiveness. When authority is distributed across multiple agencies without clear boundaries, enforcement becomes inconsistent and less predictable. This weakens the credibility of legal systems and reduces their ability to influence behavior. In such conditions, institutions may either duplicate enforcement efforts or fail to act due to uncertainty regarding jurisdiction. These dynamics create a regulatory environment in which enforcement is fragmented and ineffective. Consequently, strengthening enforcement requires addressing institutional ambiguity and improving coordination among regulatory bodies. Without such reforms, legal frameworks will continue to operate below their intended capacity.

Finally, this study emphasizes that improving cybersecurity governance in Indonesia requires a transition toward more integrated and coordinated institutional arrangements. Strengthening governance effectiveness involves not only refining

legal frameworks but also restructuring institutional relationships to ensure clarity, alignment, and collaboration. Developing mechanisms for coordination, information sharing, and joint decision-making is essential for overcoming fragmentation. In addition, establishing clear lines of authority can enhance accountability and improve the consistency of enforcement. Such reforms would enable governance systems to operate as cohesive and effective regulatory structures. Therefore, the future of cybersecurity governance in Indonesia depends on the ability to transform fragmented institutional arrangements into integrated systems capable of addressing complex digital challenges.

References

Aji, M. P. (2025). Cybersecurity politics in building cyber sovereignty in Indonesia through strengthening the role of the National Cyber and Crypto Agency. *Society, 13*(2), 1056–1071.

An, B. Y., Tang, S. Y., & Leach, W. D. (2021). Managing environmental change through inter-agency collaboration: Protective governance in mandated sustainability planning. *Environmental Science & Policy, 125*, 146–156.

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.

Cairney, P. (2025). Policymaking integration, policy coherence, and whole-of-government approaches: A qualitative systematic review of advice for policymakers. *Open Research Europe, 5*, 75.

De Wulf, N., Voets, J., & Molenveld, A. (2023). Policy coordination and integration in local government: Perspectives on barriers. *Policy & Politics, 51*(3), 530–549.

Eriksson, E., Andersson, T., Hellström, A., Gadolin, C., & Lifvergren, S. (2020). Collaborative public management: Coordinated value propositions among public service organizations. *Public Management Review, 22*(6), 791–812.

Haftel, Y. Z., & Lenz, T. (2022). Measuring institutional overlap in global governance. *The Review of International Organizations, 17*(2), 323–347.

Hustedt, T., & Radtke, I. (2024). Coordination and policy implementation. In *Handbook of Public Policy Implementation* (pp. 429–436). Edward Elgar Publishing.

Kitchin, R., & Moore-Cherry, N. (2021). Fragmented governance, the urban data ecosystem and smart city-regions: The case of Metropolitan Boston. *Regional Studies, 55*(12), 1913–1923.

Kreuder-Sonnen, C., & Zürn, M. (2020). After fragmentation: Norm collisions, interface conflicts, and conflict management. *Global Constitutionalism, 9*(2), 241–267.

Maskun, M., Al Mukarramah, N. H., Bachril, S. N., & Assidiq, H. (2022). Fragmented agencies in public sector: An obstruction to Indonesia's climate policy implementation. In *IOP Conference Series: Earth and Environmental Science* (Vol. 1105, No. 1, p. 012015). IOP Publishing.

Priyandita, G. (2025). Indonesia's cybersecurity resilience. *Asia Policy, 20*(2), 25–34.

Siti-Nabiha, A. K., Djamhuri, A., & Amirya, M. (2023). Does performance management system implementation reduce fragmentation in an Indonesian local government? *Chinese Public Administration Review, 14*(4), 269–281.

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

Trein, P., Biesbroek, R., Bolognesi, T., Cejudo, G. M., Duffy, R., Hustedt, T., & Meyer, I. (2021). Policy coordination and integration: A research agenda. *Public Administration Review, 81*(5), 973–977.

Trein, P., & Maggetti, M. (2020). Patterns of policy integration and administrative coordination reforms: A comparative empirical analysis. *Public Administration Review, 80*(2), 198–208.