JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(2), 1275-1283
ISSN: 2589-1316

Building Cyber Sovereignty in Indonesia Through Revitalization of the National Cyber and Crypto Agency of the Republic of Indonesia

Muhammad Prakoso Aji [1*], Gumilar Rusliwa Somantri [2], Muhammad Syaroni Rofii [3]

[1] *School Of Strategic and Global Studies, University of Indonesia,* INDONESIA
[2] *School Of Strategic and Global Studies, University of Indonesia,* INDONESIA, *gumilar.r29@ui.ac.id*
[3] *School Of Strategic and Global Studies, University of Indonesia,* INDONESIA, *muhammadsyaroni@ui.ac.id*

*__Corresponding Author:__ muhammad.prakoso21@ui.ac.id

Citation: Aji, M. P., Somantri, G. R. and Rofii, M. S. (2025). Building Cyber Sovereignty in Indonesia Through Revitalization of the National Cyber and Crypto Agency of the Republic of Indonesia, *Journal of Cultural Analysis and Social Change*, 10(2), 1275-1283. https://doi.org/10.64753/jcasc.v10i2.1771

Published: November 14, 2025

ABSTRACT

This study aims to analyze the development of cyber sovereignty in Indonesia through the revitalization of the structure and functions of the National Cyber and Encryption Agency (BSSN). The research employs the theory of cyber sovereignty, complemented by the concepts of cybersecurity, political will, and related theoretical perspectives. A qualitative method with a descriptive-analytical approach is applied. The findings of this study show the necessity of establishing a robust national cybersecurity governance framework that positions BSSN as the principal authority representing the state in safeguarding cyber sovereignty. Furthermore, the study reveals the limited political will of the Indonesian government to build a comprehensive national cybersecurity system. Therefore, stronger political commitment from all stakeholders is crucial to achieving effective cyber sovereignty in Indonesia.

Keywords: Cyber Sovereignty, Cybersecurity, Revitalization, Political Will

INTRODUCTION

This research is significant because the advancement of digital technologies has fundamentally transformed state governance and national security. While cybersecurity was not considered essential in the past, in today's era of global connectivity, a country's capacity to secure its cyberspace has become a crucial indicator of state sovereignty (Gordon, 2024). One of the key emerging concepts is data sovereignty, which refers to the principle that data must be subject to the laws and regulations of the country where it is physically stored (Hummel et al., 2021).

The strategic value of data as a national resource positions cybersecurity as a central pillar in safeguarding sovereignty (von Scherenberg et al., 2024). Accordingly, a state institution with strong authority is required to represent the nation's cyberspace presence, protect strategic data, and ensure the resilience of digital infrastructure. Several studies emphasize that data and information have become valuable commodities, necessitating robust institutional governance protection (Belli et al., 2024; de Jong-Chen, 2015; Pierucci, 2025).

Thus, establishing a principal institution as the backbone of national cybersecurity policy is urgently necessary (AlDaajeh et al., 2022; Parkin et al., 2023). This institution must also possess adequate authority to safeguard national sovereignty in the digital domain (Baldoni & Di Luna, 2025; Pierucci, 2025).

In Indonesia, this necessity was addressed through establishing the Cyber and Encryption Agency (Badan Siber dan Sandi Negara, BSSN) in 2017 as a form of revitalization of the State Intelligence Agency for Cryptography

(Lemsaneg). This institutional reform was formalized through Presidential Regulation No. 53 of 2017 and further strengthened by Presidential Regulation No. 28 of 2021, which reorganized the structure and functions of BSSN (BSSN RI, 2023). The formation of BSSN also integrated several institutions, including the Directorate of Information Security of the Ministry of Communication and Informatics and the Indonesian Response Team on Internet Infrastructure (Id-SIRTII).

Despite its establishment, BSSN's data indicate that the number of cyberattacks in Indonesia has continued to increase annually. This underscores that the national cybersecurity capacity still faces various limitations.

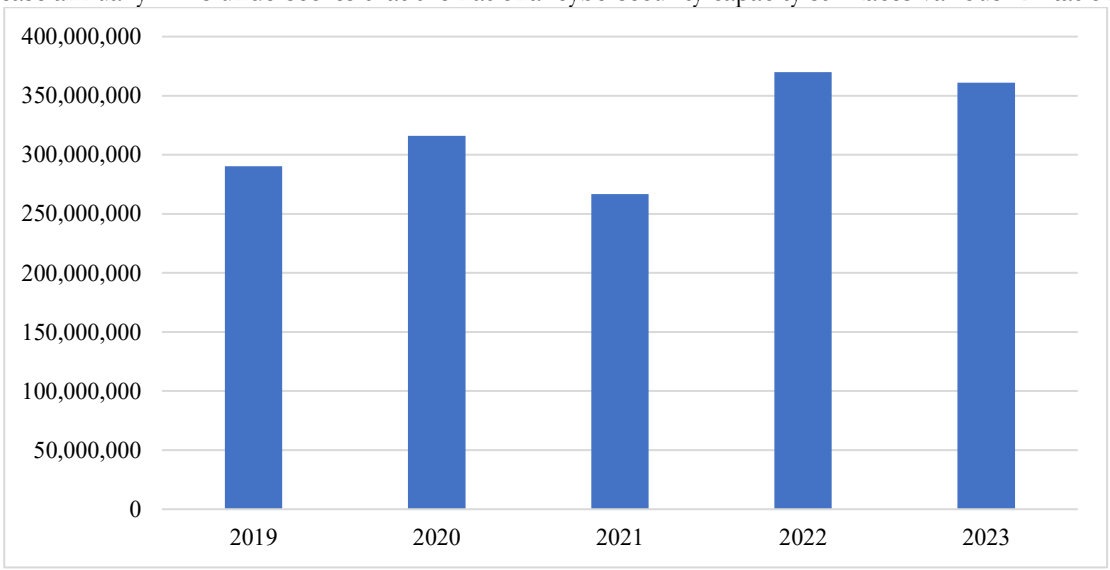

Fig 1. Number of Cyber Attacks in Indonesia, 2019–2023 *(Source: BSSN RI, 2023)*

In addition, the absence of a comprehensive legal framework—particularly the delay in ratifying the Draft Law on Cybersecurity and Resilience—demonstrates that Indonesia's cybersecurity governance is not yet fully prepared to confront the complexity of contemporary cyber threats. Therefore, revitalizing the structure and functions of BSSN is a fundamental step for the agency to effectively assume its role as the leading sector in realizing cyber sovereignty.

From an international perspective, the concept of cyber sovereignty remains contested. China and Russia promote a state-centered governance model, whereas the United States and Western countries continue to defend an open and decentralized model of the internet (Mirza et al., 2021; Qiao-Franco, 2024). This polarization directly impacts Indonesia's strategy in pursuing cyber sovereignty amid global dynamics.

Previous studies have highlighted various aspects of cybersecurity in Indonesia. For instance, research has examined the urgency of strengthening BSSN's institutional capacity (Chotimah, 2019), securitization strategies in addressing cyber threats (Haryanto & Sutra, 2023), and cyber diplomacy as an instrument of digital defense in the global era. At the international level, similar studies have also emphasized the importance of cybersecurity governance and the role of state institutions in safeguarding digital sovereignty.

In Indonesia, existing research on cybersecurity has predominantly focused on regulatory aspects, technical policies, and cyber diplomacy. Still, it has not thoroughly examined the revitalization of BSSN's institutional structure and functions. Yet, BSSN's role as the frontline institution in safeguarding cyber sovereignty is crucial in addressing the increasingly complex dynamics of cyber threats.

From this literature review, two aspects remain largely underexplored. First, studies on BSSN have thus far been limited to examining its role within regulatory and policy frameworks, without addressing the more comprehensive aspect of institutional revitalization. Second, no research has explicitly connected the revitalization of BSSN with the achievement of Indonesia's cyber sovereignty.

To address this research gap, this study seeks to answer the central question: how can cyber sovereignty in Indonesia be developed through revitalizing the structure and functions of BSSN? This research is expected to contribute theoretically to the cyber sovereignty discourse while offering practical policy recommendations to strengthen national cybersecurity governance.

LITERATUR REVIEW

Cyber Sovereignty

According to Fischer (2012), cybersecurity encompasses a range of practices, measures, and strategies to protect cyberspace and user and corporate assets from threats that may compromise data and information confidentiality, integrity, or availability. Based on the Global Cybersecurity Index (GCI) 2020, Indonesia ranked 24th with a score of 94.88, while Singapore and Malaysia occupied the 4th (98.52) and 5th (98.06) positions, respectively. According to a report by A.T. Kearney, specialized sectors dedicated to cybersecurity in Indonesia remain very limited and, in fact, cannot be fully established (Badan Keahlian DPR RI, 2021). On the other hand, Indonesia's national strategy, awareness-raising efforts, capacity-building initiatives, and regulations related to cybersecurity are still at an early stage of development (Puskaji Anggaran DPR-RI, 2021).

The role and functions of BSSN are highly strategic in the context of its revitalization to realize cyber sovereignty. Revitalizing BSSN's roles and functions is intended to establish a more capable national cybersecurity system. The transformation of Lemsaneg into BSSN strengthened the agency, which previously focused solely on cryptography, by expanding its mandate to take control of national cybersecurity. To analyze this, the author employs Yeli's (2017) Theory of Cyber Sovereignty, which explains that cyber sovereignty can be understood through three perspectives. Within this framework, traditional sovereignty—by nature exclusive—cannot be fully applied to cyberspace. This is because globalization requires acceptance, or at least consideration, of the proportional transfer of authority. In other words, states can no longer maintain absolute cyber sovereignty without interacting with different state and non-state actors. Each state, therefore, must carefully determine which elements of sovereignty must be retained absolutely and which can be transferred or shared, along with the extent of such boundaries.

Academic and practical debates on cyber sovereignty have largely focused on whether sovereignty in the digital realm should be viewed as an extension of traditional sovereignty or positioned within a new framework more adaptive to globalization dynamics. Furthermore, Yeli (2017) emphasizes that cyberspace has emerged as the fifth domain of conflict, following land, sea, air, and space. Consequently, traditional approaches that emphasize the exclusivity of sovereignty are no longer sufficient, as the borderless, interconnected nature of cyberspace—coupled with the involvement of multiple actors—demands a more flexible, collaborative approach based on the proportional distribution of authority. Therefore, analyzing cyber sovereignty through the Three Perspectives framework is crucial to distinguish between the traditional and contemporary approaches that emphasize adaptation and the transfer of authority within reasonable limits. The three perspectives in the Theory of Cyber Sovereignty are illustrated in the following figure:

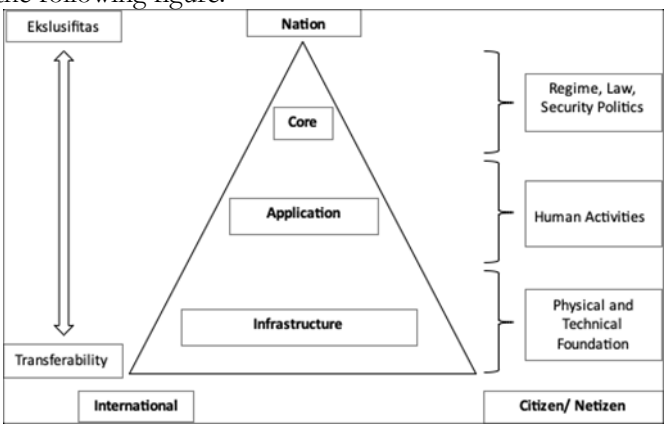

Fig 2. Three Perspectives within the Theory of Cyber Sovereignty *(Source: Yeli, 2017)*

According to Hao Yeli (2017), the key to understanding cyber sovereignty lies in examining the division of sovereignty using a layered approach, which clearly identifies which elements must remain exclusive and which can be transferred or shared. At the lowest level—the physical layer—cyber sovereignty is represented by the fundamental infrastructure of cyberspace. Key aspects at this layer include efforts to achieve global standardization and to build extensive interconnectivity. In this context, countries worldwide must be collectively willing to transfer part of their authority for standardization and global interconnection. States with advanced cyber capabilities bear both a moral and strategic responsibility to take the initiative in expanding the application of these standards, while simultaneously bridging the digital divide by distributing technological achievements to developing countries. The next level—the application layer—represents various digital platforms and Internet operators that operate in the real world. This layer plays a critical role because the application space has integrated multiple aspects of life,

including technology, culture, economy, trade, and everyday social interactions. At this layer, cyber sovereignty cannot be applied rigidly. Instead, the degree of sovereignty must be adapted to each country's local context and conditions. The main objective is to achieve a dynamic balance emphasizing multilateral governance, stakeholder participation, and a trade-off between individual freedom and social order. Thus, cyber sovereignty can be mapped more proportionally through this layered approach. On the one hand, there are global elements that require cross-national collaboration. On the other hand, local dimensions must still be regulated according to national needs and interests.

At the top or core layer, cyber sovereignty encompasses fundamental inviolable aspects of regime, law, political security, and ideology. These elements serve as the foundation of governance and embody the state's core interests. Differences in national conditions, religious backgrounds, and cultural diversity across countries underscore that diversity is an existential norm of humanity that a single culture cannot dominate. Therefore, differences and diversity must be deeply understood, respected, and tolerated, even when they conflict with a country's social system or ideology. Meanwhile, cyber sovereignty can still be transferred to some extent at the middle and lower levels of the three-layer structure. This creates broader opportunities for diverse stakeholders to participate in cybersecurity governance, leading to the emergence of a multistakeholder governance model. However, the government remains the principal factor in determining policy directions at the top level. Consistent with the consensus affirmed by the Group of Governmental Experts (GGE), it is emphasized that "the right to make public policy on the Internet is part of state sovereignty, and each state naturally possesses judicial authority over information conveyed through its domestic information infrastructure." Accordingly, respect for a state's freedom to determine its development path and cyberspace management model is a prerequisite for governmental responsibility and international cooperation. A comprehensive understanding of these three layers further clarifies the distinction between multilateral governance based on state sovereignty and multistakeholder governance involving non-state actors. These two models are not inherently contradictory; they apply to different domains and levels within cyberspace. Regarding ideology, policy, law, institutional security, and governance, the state plays a central role through effective multilateral governance while accommodating multistakeholder governance in other layers (Hao Yeli, 2017).

Based on this theory, it can be analyzed that the highest layer pertains to the norms, principles, and values that shape the governance framework of cyberspace. At this level, cyber sovereignty addresses fundamental issues such as legal sovereignty, national security, human rights protection, and digital ideology and culture sovereignty. States at this layer must carefully determine which values and norms should be preserved as part of their national identity and sovereignty, and to what extent these values can be negotiated or adapted in global interactions. Thus, the normative layer emphasizes that, although cyberspace requires global interconnectedness, states retain the right to uphold fundamental principles that constitute the foundation of their existence. Overall, the Three Perspectives framework demonstrates that cyber sovereignty is not merely an extension of traditional sovereignty but a new form of sovereignty that requires exclusive protection and international cooperation. States are expected to selectively define the scope of non-transferable sovereignty while remaining open to global collaboration to maintain stability, security, and justice in cyberspace.

RESEARCH METHOD

The methodology employed in this study is qualitative, using a descriptive-analytical approach. According to Lune and Berg (2017), a qualitative researcher seeks to explore and understand the meanings of phenomena by engaging directly or indirectly with the research subject.

The data for this study were obtained from both primary and secondary sources. Primary data were collected through observations and interviews with various key informants from BSSN RI, the Ministry of Education and Culture of Indonesia (Kemendikbud RI), Commission I of the Indonesian House of Representatives (DPR-RI), civil society organizations such as Safe Net which monitors data policy issues in Indonesia, private sector providers of social media applications, as well as several institutions that have experienced data breaches, such as BPJS Kesehatan, and experts in cybersecurity and defense.

Secondary data were collected from books, relevant journal articles, various media sources, both online and print, and other information sources used to support the primary data previously obtained. A literature review was conducted to allow the researcher to analyze the collected data comprehensively.

The data analysis in this study employed the model proposed by Bogdan and Biklen, which emphasizes qualitative data analysis through stages of data organization, categorization, and interpretation. This model was applied to maintain research focus and ensure that the analysis remains within the research problem's context, as Yusuf (2017) explained.

RESULT AND DISCUSSION

Referring to the implementation of the three perspectives in the Theory of Cyber Sovereignty, this analysis focuses on how the context of cyber sovereignty in Indonesia is still in formation and refinement. Given the current cybersecurity capacity in Indonesia, the author situates the country at the second level, namely the application layer. This is because, in the current context of cyber sovereignty in Indonesia, societal activities have increasingly shifted from the physical space to cyberspace. These activities encompass various actions in political, economic, socio-cultural, and other domains. In recent years, a wide range of applications have been developed to facilitate the public's conducting activities in cyberspace. Applications such as Instagram, TikTok, Gojek, Grab, Tokopedia, Shopee, and others have become essential tools for Indonesian society to engage in activities and meet their needs. Regarding the first layer of the pyramid, which is related to infrastructure, it is evident that Indonesia has already built and continues to develop various infrastructures necessary for the growth of the internet and cyberspace. This indicates that, in terms of infrastructure, Indonesia possesses a sufficiently developed foundation to advance its cyber sovereignty.

In contrast, at the top layer of the pyramid—the core—cybersecurity in Indonesia still lacks the necessary regulatory framework. This is primarily due to the pending ratification of the Draft Law on Cybersecurity and Resilience, which constitutes the central component of national cybersecurity policy. In cybersecurity politics, sectoral egos among ministries and agencies involved in cybersecurity have further hindered cross-sectoral coordination. Each government institution continues to prioritize its own interests. BSSN, which to date operates only under a Presidential Regulation, faces challenges in coordinating with other government institutions that are backed by stronger legal frameworks, such as the Ministry of Communication and Informatics (Kemkominfo), Ministry of Defense (Kemhan), Ministry of Foreign Affairs (Kemlu), the Indonesian National Armed Forces (TNI), and the National Police (Polri), all of which have statutory authority. Therefore, to realize cyber sovereignty, the top layer of the pyramid—the core—requires urgent institutional reform. Political support is essential to achieve this. The Draft Law on Cybersecurity and Resilience, which positions BSSN as the primary driver of national cybersecurity policy, must be ratified immediately.

The role of BSSN has become increasingly strategic given the rapid and pervasive development of technology, which is now inseparable from everyday societal life. This positions BSSN as a key government agency capable of realizing cyber sovereignty. A secure cyberspace, protected from cyberattacks, is clearly a priority for Indonesia's government and the people. Establishing cyber sovereignty is feasible only if all stakeholders recognize its importance. Although BSSN is a relatively newly established government institution, it is expected to impact the nation's cyber sovereignty significantly.

Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure and Presidential Regulation No. 47 of 2023 on the National Cybersecurity Strategy and Cyber Crisis Management constitute the two main regulations currently serving as the foundation for implementing cybersecurity policies in Indonesia. These regulations emphasize the protection of Vital Information Infrastructure (VII) and formulate a national strategy to address cybersecurity challenges. Under these regulations, the government is responsible for safeguarding all aspects of cyberspace, including information assets, from various forms of cyber threats and attacks, whether technological or social (BSSN RI, 2024). The regulations encompass vulnerability management, risk mitigation, and developing cyber crisis response systems that could potentially threaten the nation's strategic infrastructure. The government demonstrates a strong commitment to protecting critical infrastructure from increasingly complex cyber threats through these policies.

Within the framework of Cyber Sovereignty Theory, strengthening the infrastructure perspective is essential. The revitalization of BSSN through the enhancement of its cybersecurity infrastructure is closely linked to the budget allocated to the sector. According to A.T. Kearney, as cited in the Budget Research Center of the Indonesian House of Representatives (Puskaji Anggaran DPR-RI, 2021), Indonesia's cybersecurity budget in 2017 amounted to only USD 1.829 million, or approximately 0.02% of its Gross Domestic Product (GDP). This figure remains considerably low compared to other ASEAN countries such as Singapore, Malaysia, Thailand, Vietnam, and the Philippines, and is still below both the ASEAN and global averages. This reality reflects the government's limited budgetary allocation for cybersecurity. Therefore, increased financial support and the accelerated formulation of cybersecurity-related regulations are urgently required. In this regard, the comparison of cybersecurity budget allocations across several countries can be observed as follows:

Table 1. Comparison of Cybersecurity Budgets in 2021

No.	Country	Year	Budget Amount (in US Dollars)
1	United States	2021	$18.78 Billion
2	Israel	2021	$1.5 Billion
3	France	2021	$1.2 Billion
4	Australia	2021	$425.5 Million
5	Canada	2021	$80 Million
6	Iran	2021	$71.4 Million
7	Indonesia	2021	$50.2 Million

Source: (Sagar, 2021)

Regarding the application perspective, which focuses on human activities, analyzing the key actors involved in Indonesia's cybersecurity governance is essential. From the actors' standpoint, cybersecurity governance in Indonesia encompasses three major domains: the government, the private sector, and civil society. Within the government, multiple agencies are directly or indirectly linked through their core duties and functions related to cybersecurity. The private sector, on the other hand, includes diverse stakeholders with vested interests in managing and securing the digital space. Civil society organizations also play an important role in monitoring, advocating, and safeguarding digital rights. The involvement of these three domains illustrates the multi-actor nature of cybersecurity governance in Indonesia. The following table provides a more detailed overview:

Table 2. Actors in the Governance of Cybersecurity in Indonesia

Government	Private Sector	Civil Society
Coordinating Ministry for Political, Legal, and Security Affairs	Telkom Indonesia	Academia
National Cyber and Crypto Agency	Google	Non-Governmental Organizations (NGOs)
Ministry of Communication and Information Technology	Indonesian Internet Service Providers Association (APJII)	Technology Communities
Indonesian National Police	Indonesian E-Commerce Association (idEA)	
State Intelligence Agency		
Indonesian National Armed Forces		

Source: (Sumartias, 2018)

The implementation of cybersecurity governance in Indonesia is currently not yet nationally coordinated and remains largely sectoral, depending on the interests and capacities of each institution, particularly within the government sector. The involvement of multiple agencies and ministries simultaneously handling cybersecurity issues illustrates this field's overlapping nature of governance. Although these institutions adopt different approaches, government actors still rely on their own mechanisms to address cyber threats. Law enforcement agencies generally concentrate on cybercrime, whereas military-related institutions tend to focus on cyber espionage and cyber terrorism.

Bridging the gap in human resource capacity in technology is essential (Sumartias, 2018). According to APJII (the Indonesian Internet Service Providers Association), the cybersecurity workforce in Indonesia remains dominated by foreign professionals due to the relatively low expertise of local talent. Although Indonesia currently has approximately five hundred internationally certified professionals in cybersecurity programs such as ISO27001, CEH, CISA, CISM, and CISSP, this number is insufficient for a country that ranks among the largest internet users in the world while also being highly vulnerable to cyberattacks. Information technology can be easily intercepted or hacked by foreign hackers and crackers, creating particular risks for intelligence information transmitted through cyberspace. In relation to the evaluation of regulations and political will, it is therefore

important to consider the following table on the Regulatory Framework for Cybersecurity Governance in Indonesia, as processed and presented by the author:

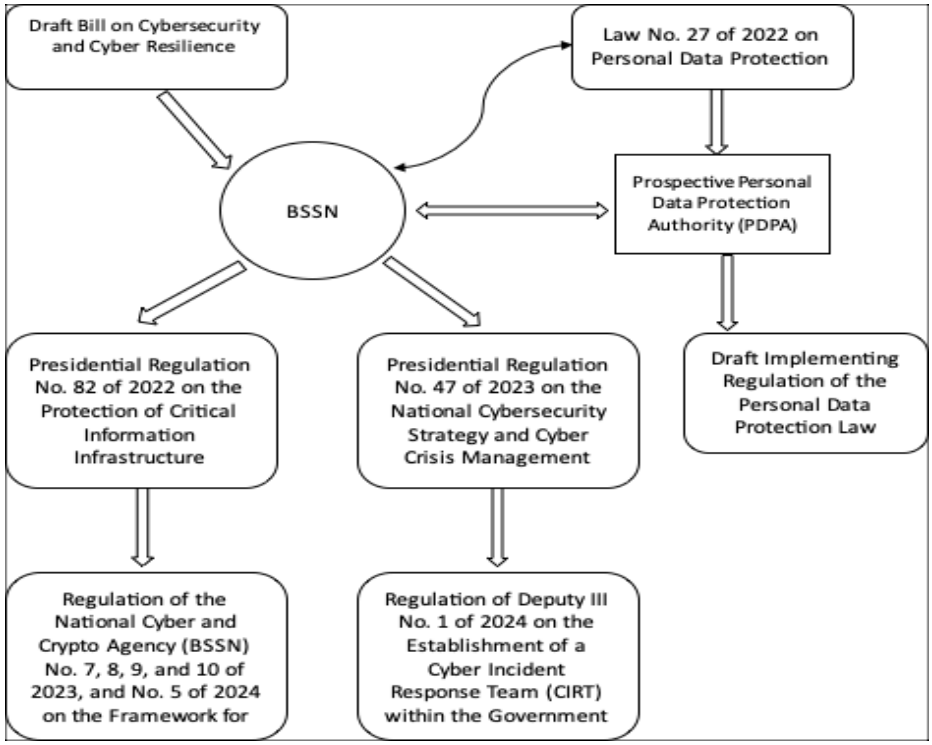

Fig 3. Regulatory Framework of Cybersecurity Governance in Indonesia
Source: Processed by the Author

Based on the regulatory framework concerning cybersecurity and data protection implemented in Indonesia, it can be observed that BSSN still lacks a strong legal foundation, namely a comprehensive Cybersecurity and Resilience Act, which has not yet been enacted but has been reintroduced into the 2025 National Legislative Program (Prolegnas). Although the agency does not yet have a legal umbrella in the form of a dedicated law, BSSN has issued regulations under Presidential Decrees enacted in 2022 and 2023. These include Presidential Decree No. 82/2022 on the Protection of Critical Information Infrastructure and Presidential Decree No. 47/2023 on the National Cybersecurity Strategy and Cyber Crisis Management. Nevertheless, this progress is relatively slow, given that BSSN was established in 2017. It took at least five years for the agency to issue regulations, and even then, they are still in the form of Presidential Decrees rather than a law with stronger binding authority.

In addition, one of the existing laws that could indirectly strengthen BSSN's legal foundation is Law No. 27/2022 on Personal Data Protection (PDP). However, this law has not yet been accompanied by its implementing regulations. In principle, these regulations should have been issued within two years after the law's enactment, meaning by 2024. Furthermore, the PDP Law mandates the establishment of a Personal Data Protection Authority (LOPDP), which, to date, has not yet been formed. If established, this institution could overlap with BSSN's mandate, necessitating a more thorough assessment before creating another regulatory body. The absence of these follow-up measures indicates that the political will to provide BSSN with a strong legal framework remains weak. This observation strengthens the argument that the government and parliament have yet to demonstrate sufficient commitment to reinforcing the national cybersecurity sector. Such commitment is crucial to ensuring the realization of cyber sovereignty in Indonesia.

Therefore, the revitalization of BSSN is necessary to position the agency as the central authority in Indonesia's cybersecurity governance. Strengthening BSSN's institutional role will reinforce the core perspective of the Cyber Sovereignty Theory, thereby ensuring that the three layers of the theory's pyramid can be fulfilled to advance Indonesia's cyber sovereignty. Achieving this, however, requires a strong political will from the government. Sectoral ego among ministries and state institutions must be minimized so as not to obstruct the implementation of an integrated cybersecurity framework. At the same time, the role of society is also critical in responding to the rapid technological developments that bring about profound socio-cultural transformations. Active participation from civil society and support from the private sector will serve as a strong foundation for strengthening Indonesia's path toward building cyber sovereignty.

CONCLUSION

Revitalizing BSSN as the central institution in formulating and implementing national cybersecurity policies is fundamental for developing Indonesia's cyber sovereignty. An analysis through the lens of the Cyber Sovereignty Theory indicates that Indonesia has yet to fulfill all perspectives within the cyber sovereignty pyramid. In particular, Indonesia still lacks a comprehensive Cybersecurity Law at the highest level. Existing regulations are limited to Presidential Regulation No. 47 of 2023 on the National Cybersecurity Strategy and Cyber Crisis Management, and Presidential Regulation No. 82 of 2022 on the Protection of Critical Information Infrastructure. Since its establishment in 2017, BSSN has not been supported by a strong and clear legal framework to serve as the backbone of national cybersecurity governance, and these two presidential regulations remain insufficient to address the escalating cyber threats. Moreover, strong political will from the government is required to position BSSN as the main authority in the national cybersecurity architecture. Sectoral egos across government institutions can no longer be left unaddressed, as they hinder the creating of a coordinated cybersecurity system. In addition, the role of the private sector and civil society is crucial in navigating the massive socio-cultural transformations occurring in cyberspace. Therefore, the Cybersecurity and Resilience Bill (RUU KKS) should be prioritized for immediate ratification to provide BSSN with a more robust legal mandate, enabling effective coordination with other government agencies and ensuring the realization of Indonesia's cyber sovereignty.

REFERENCES

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies in the improvement of cybersecurity education. Computers & Security, 119, 102754.

Badan Keahlian DPR RI. (2021). Budget Issue Brief: Politik dan Keamanan (Vol. 01, Issue 17).

Baldoni, R., & Di Luna, G. (2025). Sovereignty in the digital era: The quest for continuous access to dependable technological capabilities. IEEE Security & Privacy, 23(1), 91–96.

Belli, L., Gaspar, W. B., & Jaswant, S. S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. Computer Law & Security Review, 54, 106017.

BSSN RI. (2023). Lanskap Keamanan Siber Indonesia 2023. BSSN: Jakarta.

BSSN RI. 2024. Survei Kesadaran Keamanan Siber. BSSN: Jakarta.

BSSN RI. 2024. Kajian Ketahanan Siber: Manajemen Kerentanan. BSSN: Jakarta.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 10(2), 113–128.

de Jong-Chen, J. (2015). Data sovereignty, cybersecurity, and challenges for globalization. Geo. J. Int'l Aff., 16, 112.

Fischer, E. A. (2012). Federal laws relating to cybersecurity: discussion of proposed revisions. Congressional Research Service, Washington, DC.

Gordon, G. (2024). Digital sovereignty, digital infrastructures, and quantum horizons. AI & SOCIETY, 39(1), 125–137. https://doi.org/10.1007/s00146-023-01729-7

Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. Global Political Studies Journal, 7 (1), 56–69.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, 8(1), 2053951720982012.

Lune, H., & Berg, B. L. (2017). Qualitative research methods for the social sciences. Pearson.

Mirza, M. N., Ali, L. A., & Qaisrani, I. H. (2021). Conceptualising Cyber Sovereignty And Information Security: China's Image Of A Global Cyber Order. Webology, 18(5), 598–610.

Parkin, S., Kuhn, K., & Shaikh, S. A. (2023). Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception. Journal of Cybersecurity, 9(1), tyad018.

Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. Digital Society, 4(1), 1–19.

Qiao-Franco, G. (2024). An emergent community of cyber sovereignty: the reproduction of boundaries? Global Studies Quarterly, 4(1), ksad077.

Sagar, R. (2021). Top Cybersecurity Budgets Around The World. Analytics India Magazine.

Sumartias, S. (2018). Keamanan siber dan pembangunan demokrasi di Indonesia. Pusat Penelitian Badan Keahlian DPR RI.

von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data sovereignty in information systems. Electronic Markets, 34(1), 15.

Yeli, H. (2017). A three-perspective theory of cyber sovereignty. Prism, 7(2), 108–115.

