Society, 13 (2), 1056-1071, 2025
P-ISSN: 2338-6932 | E-ISSN: 2597-4874
https://societyfisipubb.id

Cybersecurity Politics in Building Cyber Sovereignty in Indonesia Through Strengthening the Role of the National Cyber and Crypto Agency

Muhammad Prakoso Aji *
Universitas Pembangunan Nasional Veteran Jakarta,
South Jakarta City, Special Capital Region of Jakarta, 12450, Indonesia
* Corresponding Author: prakosoaji@upnvj.ac.id

ARTICLE INFO

Publication Info:
Research Article

How to cite:
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.

DOI: *10.33019/society.v13i2.960*

Received: February 28, 2025;
Accepted: April 27, 2025;
Published: July 7, 2025;

ABSTRACT

In an increasingly interconnected digital world, cybersecurity has emerged as a crucial element of national resilience and global political competition. The growing frequency of cyberattacks and data breaches underscores the urgency for Indonesia to strengthen its institutional capacity in securing cyberspace and protecting national sovereignty. In this context, cybersecurity politics determine how state institutions negotiate authority, coordinate policies, and mobilize resources to build digital resilience. This study analyzes the dynamics of cybersecurity politics and their influence on Indonesia's efforts to achieve cyber sovereignty through the strengthening of the National Cyber and Crypto Agency (BSSN). Using a qualitative descriptive approach supported by literature review and policy analysis, the study applies the theory of state sovereignty and the framework of cybersecurity political factors. Findings reveal that BSSN plays a pivotal role as the state's representative in maintaining cyber sovereignty amid complex inter-agency coordination, overlapping mandates, and regulatory uncertainty. Political, technological, and institutional factors significantly shape Indonesia's cybersecurity governance, influencing how the state responds to both domestic vulnerabilities and international cyber threats. Nevertheless, the persistence of sectoral ego, fragmented authority, and the absence of a comprehensive Cyber Security and Resilience Law continue to hinder policy integration and weaken institutional effectiveness. The study concludes that strengthening BSSN's authority, through legal ratification, increased budgetary support, organizational reform, and enhanced cyber diplomacy, is essential to establish an integrated and adaptive national cybersecurity system *capable of safeguarding Indonesia's sovereignty in cyberspace while aligning with global best practices in cyber governance.*

Keywords: *Cybersecurity Politics; Cyber Sovereignty; Governance; National Cyber and Crypto Agency (BSSN); Policy Integration*

1. Introduction

Cybersecurity politics relates to all factors that influence the implementation of a national cybersecurity system. It encompasses state structures, policy frameworks, and the allocation of resources required to ensure cyber resilience (Dunn Cavelty & Wenger, 2020). In contemporary global politics, cybersecurity is no longer a purely technical domain but a strategic field intertwined with issues of power, sovereignty, and international competition (Dunn Cavelty & Wenger, 2020; Romaniuk & Manjikian, 2021). Cybersecurity policy determines the development of a country's cyber capabilities and reflects how governments manage the intersection between technological innovation, national security, and political power (Romaniuk & Manjikian, 2021). Both internal and external factors shape these policies. Internally, the effectiveness of cybersecurity depends on regulatory support, budget allocation, and sectoral coordination among state institutions, which reflect the level of political commitment to cyber governance (Chotimah, 2019). Externally, it is influenced by international cooperation, cyber diplomacy, and transnational institutional relationships that define a country's strategic posture in global cyberspace (Baezner & Robin, 2018). Therefore, cybersecurity politics can be viewed as a multidimensional arena in which state and non-state actors negotiate influence, legitimacy, and control over digital infrastructures that are increasingly vital to economic and political stability (Hao, 2017; Qiao-Franco, 2024).

Developing cyber sovereignty in Indonesia is essential, particularly in response to the rapid evolution of global information technology that now shapes fundamental aspects of statehood and nation-building (Hao, 2017). The concept of cyber sovereignty has emerged as a central tenet of national security discourse, emphasizing a state's full authority to regulate, protect, and manage its digital ecosystem within its jurisdiction (Walter et al., 2020). Cyber sovereignty represents a country's authority and control over its digital domain, positioning cyberspace as an extension of national territory and a key driver of development (Qiao-Franco, 2024). Achieving cyber sovereignty requires integrated management of cyberspace supported by strong cybersecurity capabilities and coherent policy coordination. In the Indonesian context, this challenge is further complicated by overlapping institutional authorities, sectoral egos, and uneven technical capacity among agencies responsible for digital governance (Sembiring & Pattihahuan, 2025). A comprehensive national cybersecurity policy enables the realization of cyber sovereignty and reinforces national interests in the face of global technological and political challenges (Voo et al., 2022). Within this framework, the establishment of a specialized agency with a central coordinating role, such as the National Cyber and Crypto Agency (BSSN), becomes a strategic pillar for realizing Indonesia's cyber sovereignty (Chotimah, 2019). BSSN's formation in 2017 signaled the state's commitment to institutionalize cybersecurity governance; however, the absence of a Cybersecurity and Resilience Law (RUU KKS) continues to hinder the agency's full mandate implementation (Sudarmadi & Runturambi, 2019).

2021 saw frequent cyber incidents. One strategic factor is that these cyber incidents led to various data leaks. These data leaks affected state data held by different government agencies,

https://doi.org/10.33019/society.v13i2.960

as well as personal data held by citizens held by multiple government agencies, and even private sector companies. According to data released by the National Cyber and Crypto Agency (BSSN), at least 1.6 billion cyberattacks occurred throughout 2021. Meanwhile, according to data from The Record, Insikt Group, an internet security agency, reported by CNN Indonesia, Chinese hackers were able to penetrate the firewalls used by several ministries and agencies in Indonesia (CNN Indonesia, 2021). They were detected in approximately 10 government agencies. They even breached the firewall of the State Intelligence Agency (BIN). The hacks were potentially carried out by Mustang Panda, a Chinese hacker who frequently targets several countries in Southeast Asia.

Regarding the frequent data leaks in various agencies in Indonesia, one of the leading causes is the lack of integration of national cybersecurity policies between the relevant ministries and agencies. This is due to the lack of an agency authorized to play a central role in maintaining national cybersecurity. This recurring pattern of fragmented response highlights the urgency of consolidating Indonesia's cybersecurity governance framework under a single coordinating body, in line with international best practices seen in other jurisdictions such as Singapore and Australia (Romaniuk & Manjikian, 2021; Voo et al., 2022).

In line with the lack of concrete national cybersecurity policies in Indonesia, developments in several other countries have been much better. Based on the research report of Voo, Hamian, Cassidy at the Belfer Center for Science and International Affairs, at Harvard Kennedy School, conveyed about the National Cyber Power Index in 2022 with results showing the ranking of 30 countries referring to eight aspects, namely: 1) Surveillance and Monitoring of Groups within the Country, 2) Strengthening and Improving National Cyber Defense, 3) Controlling and Manipulating the Information Environment, 4) Collecting Intelligence Data from Other Countries for National Security, 5) Growing National Cyber and Technological Competence for Commercial, 6) Destroying or Disabling Infrastructure to Opponent Capabilities, 7) Understanding International Cyber Norms and Technical Standards, 8) Accumulating Wealth and/or Extracting Cryptocurrency. Based on the report of the Belfer Center, Harvard Kennedy School, the ranking of the National Cyber Power Index in 2022 is:

Table 1. National Cyber Power Index Tahun 2022

RANK	COUNTRY	RANK	COUNTRY
1.	United States	16.	Japan
2.	China	17.	Singapore
3.	Russia	18.	New Zealand
4.	England	19.	Israel
5	Australia	20.	Swedia
6.	Netherland	21.	Saudi Arabia
7.	Vietnam	22.	Swiss
8.	South Kore	23.	Turkey
9.	France	24.	Egypt
10.	Iran	25.	Estonia
11.	Germany	26.	India
12.	Ukraine	27.	Italia
13.	Canada	28.	Malaysia
14.	North Korea	29.	Lithuania

https://doi.org/10.33019/society.v13i2.960

RANK	COUNTRY	RANK	COUNTRY
15.	Spain	30.	Brazil

Source: (Voo et al., 2022)

This research report refers to research conducted two years earlier, namely in 2020, which then shows the comparative results of the National Cyber Power Index in 2020 and 2022, which can be seen in the following table:

Table 2. Ranked in the Top 10 in the 2022 National Cyber Power Index

RANK	2020	2022
1	United States	United States
2	China	China
3	England	Russia
4	Russia	England
5	Netherland	Australia
6	France	Netherland
7	Germany	South Korea
8	Canada	Vietnam
9	Japan	France
10	Australia	Iran

Source: (Voo et al., 2022)

Based on the results of the research report, it can be seen that Indonesia is not included in the top 30 countries in the 2022 National Cyber Power Index. The data shows that several of Indonesia's closest neighbors, namely Vietnam, Singapore, and Malaysia, are included in the top 30 countries in the 2022 National Cyber Power Index. In fact, Vietnam ranks eighth. Singapore is ranked 17th. Meanwhile, Malaysia, our closest neighbor, is ranked 28th. This indicates Indonesia's weak cyber capabilities, even compared to several other countries in the Southeast Asian region. Such a gap suggests that Indonesia's cyber capacity-building has not yet matched its regional ambitions. It underscores the need for strategic investments in institutional capability, talent development, and international cooperation (Amiruddin & Yazid, 2023). This illustrates Indonesia's weak capabilities in cybersecurity, which is crucial for realizing cyber sovereignty. Various policies issued by the government can be said to be unable to recognize a competent national cyber capability. Various data leak incidents reflect the weakness of national cybersecurity capabilities as a bulwark of Indonesia's cyber sovereignty. The BSSN (National Cyber and Crypto Agency) plays a central role in maintaining national cybersecurity. Strengthening the BSSN requires political support for cybersecurity from both internal and external perspectives. In the national context, there is a need for regulations that can enhance the role and function of BSSN as the main captain of national cybersecurity. Therefore, this study seeks to analyze how cybersecurity politics shape Indonesia's pursuit of cyber sovereignty and to identify the institutional and political prerequisites necessary for strengthening BSSN's role as the central coordinator of national cybersecurity governance.

https://doi.org/10.33019/society.v13i2.960

2. Literature Review

2.1. State and Cyber Sovereignty

Over time, several theories regarding sovereignty have emerged. The Theory of State Sovereignty explains that sovereignty resides with the state, not with God. All must obey the state because it is the state that makes the law. Jean Bodin and Paul Laband put forward this idea. The state is the best unified idea. Therefore, the state is considered to have a right to the lives of its citizens. However, there is also the Theory of Legal Sovereignty, which explains that everyone within the state must obey applicable laws (Bakhri, 2018).

Guangyu Qiao-Franco's research explains that a state-centered policy approach that should be coordinated and formulated to address these challenges has gained global attention (Qiao-Franco, 2024). Such an approach is fundamentally built on the principle of cyber sovereignty, suggesting a return to the "Westphalian model" of managing digital space. In this state-centered model, states have mutually recognized supreme authority over cyber infrastructure and activity within their territories. This challenges traditional standards for internet governance, which feature an open, minimalist, and decentralized design. As a pioneer of the principle of cyber sovereignty, China not only practices it within its borders but also actively promotes this supposedly "fairer" and "more reasonable" model of internet governance through the China-initiated World Internet Conference and various other multilateral organizations. These include the United Nations (UN), the Shanghai Cooperation Organization (SCO), the Association of Southeast Asian Nations (ASEAN), and the BRICS (Brazil, Russia, India, China, and South Africa) institutions. Cyber sovereignty has become a central concern in the Global South 2 (and Russia). Meanwhile, the Global North, led by the United States, remains firmly behind the traditional approach of defending "cyber freedom" and an open internet, and opposes the state-centric model. The North-South axis has thus become more pronounced in cyber politics over the past three decades.

2.2. Cybersecurity Politics

Regarding the influencing factors in cybersecurity politics, according to Dunn Cavelty and Wenger, the link between technological possibilities and the political choices of state actors, combined with scientific factors, and then focusing on the "state," is necessary and appropriate (Dunn Cavelty & Wenger, 2020). This is because political stability is often related to issues concerning authority. However, the state is not the only relevant actor in this context, as it functions as a bridge between various parties on the national and global stage, which then becomes a characteristic of cybersecurity politics. Related to this, six factors drive cybersecurity politics.

Table 3. Six Factors Driving Cybersecurity Politics

Main Factor	Description
Technology	The development and advancement of digital technology determine the scope and dynamics of cybersecurity politics. Technological innovations both reflect and shape political ideas, power structures, and the possibilities for state and non-state actors to exercise influence in cyberspace.
Important Events (Cyber-Related Incidents)	Critical events, whether originating in cyberspace or in the broader political environment, significantly influence cybersecurity agendas. Cyberattacks, data breaches, or international crises often trigger shifts in policy priorities and security strategies.
International Politics	Cybersecurity is embedded within global power relations, where beliefs in

https://doi.org/10.33019/society.v13i2.960

Main Factor	Description
	new forms of "cyber power" drive patterns of competition, cooperation, and conflict among major states. International politics thus frames cybersecurity as both a diplomatic and strategic domain.
National Politics	Domestic political negotiations and inter-agency dynamics determine how roles, responsibilities, and resources are distributed among state institutions, private sectors, and civil society. These negotiations often create tension between national security objectives and democratic governance principles.
Academic Debate	Theoretical discussions and paradigmatic shifts in International Relations and Security Studies shape how cybersecurity is conceptualized, studied, and addressed. Academic debates influence how states and institutions understand the political nature of cyber threats.
Institutionalization	The level of institutional support, including research funding, publication opportunities, and academic or policy networks, creates both opportunities and constraints for advancing cybersecurity knowledge and policy development. Institutional frameworks determine how cybersecurity becomes embedded in national and international governance structures.

Source: (Dunn Cavelty & Wenger, 2020)

2.3. National Cybersecurity Policy

Chotimah's research employed qualitative methods, and its data collection techniques were conducted entirely through desk research (Chotimah, 2019). This study employed institutional theory as the primary theory, supported by concepts in cybersecurity. This research explains that cybersecurity governance in Indonesia has become a very urgent need, making it appropriate to establish the National Cyber and Crypto Agency (BSSN). However, in the future, institutional strengthening is needed. The BSSN will play a significant role in maintaining Indonesia's cyberspace security. In carrying out this role, the BSSN also plays a role in developing cyber diplomacy. Cyber diplomacy is fundamental in building a nation's capabilities and resilience through collaboration with other nations, particularly those in the same region, thus mutually strengthening each other's cyber defenses within the region.

Research by Haryanto and Sutra examines the cybersecurity enhancement strategies implemented by the National Cyber and Crypto Agency (BSSN), Indonesia's national cybersecurity agency (Haryanto & Sutra, 2023). The analysis was conducted using the Securitization Theory framework and the Cybersecurity Concept. Based on the data obtained, the establishment of the National Cyber Security Agency (BSSN) is regulated by a presidential regulation, mandated to effectively and efficiently carry out cybersecurity tasks through the utilization, development, and consolidation of various elements related to cybersecurity. From the perspective of Securitization Theory, the establishment of the BSSN reflects the Indonesian government's strong commitment to the securitization of cybersecurity issues, which is seen as an effort to increase national security capacity. This is motivated by the position of cyber issues as an existential security threat to society or certain entities. Thus, cyberspace users in Indonesia are positioned as vulnerable objects to various forms of cyber threats, while the Indonesian government and BSSN act as securitizing actors in this securitization process. Furthermore, functional actors emerge as parties that determine the various strategic and operational steps implemented by BSSN in its capacity as a securitizing actor to strengthen national cybersecurity. This effort is realized through the implementation of five pillars referenced by the Global Cybersecurity Index, encompassing legal, technical, organizational, capacity building, and cooperation dimensions.

https://doi.org/10.33019/society.v13i2.960

The research by Sudarmadi and Runturambi is a descriptive study using a qualitative approach that aims to explain the strategy of the National Cyber and Crypto Agency (BSSN) in strengthening national cybersecurity commitments to address cyber threats in Indonesia (Sudarmadi & Runturambi, 2019). Organizationally, Indonesia does not yet have an integrated national cybersecurity strategy or policy. In this regard, BSSN is expected to be the central institution in formulating and developing such a strategy. Although established, BSSN is still in the stage of internalization and institutional harmonization to build a solid organizational foundation. As the coordinator of national cybersecurity implementation, BSSN is required to collaborate with all relevant stakeholders. Currently, Indonesia does not have an official reference used to measure cybersecurity developments, risk assessment strategies, cybersecurity audits, or performance evaluation tools and methods that can serve as a basis for future improvements. In terms of capacity development, Indonesia already has a National Standardization Agency (BSN) that plays a role in national standardization. However, no incentive program encourages the market to produce cybersecurity products and services. Therefore, BSSN is expected to be able to initiate incentive policies to support the development and improvement of the quality of cybersecurity technology in Indonesia.

3. Research Methodology

This study employs a qualitative research design using a descriptive–analytical approach to explore how cybersecurity politics influence the realization of cyber sovereignty in Indonesia, with particular attention to the institutional role of the National Cyber and Crypto Agency (BSSN). The qualitative approach is considered appropriate because the study aims to interpret social and political dynamics, institutional interactions, and policy coordination processes rather than quantify variables. By focusing on meaning, context, and interpretation, this approach enables the researcher to capture the complexity of cybersecurity governance within the political and institutional framework of the Indonesian state.

The research adopts a case study strategy centered on BSSN as the primary unit of analysis. This allows for an in-depth and contextual exploration of how cybersecurity governance is formed, contested, and institutionalized through political processes. The case study design also facilitates a critical linkage between empirical data and theoretical perspectives, particularly the theory of state sovereignty and the framework of cybersecurity political factors (Dunn Cavelty & Wenger, 2020). The researcher seeks to understand how state institutions negotiate authority and coordination in cybersecurity governance and how such interactions affect Indonesia's pursuit of cyber sovereignty.

The data used in this research consist of both primary and secondary sources. Primary data were collected through semi-structured interviews and observations of institutional practices, including coordination meetings, policy briefings, and public communications related to cybersecurity. Informants were selected purposively based on their relevance and involvement in cybersecurity policy, such as officials from BSSN, the Ministry of Communication and Informatics, the State Intelligence Agency (BIN), and the Ministry of Defense. Secondary data were obtained from official documents, academic journal articles, policy papers, books, government regulations, and reliable online and printed media. The researcher also utilized reports from international institutions, notably the National Cyber Power Index 2022 published by the Belfer Center for Science and International Affairs, as a comparative reference to evaluate Indonesia's cyber capability development.

Data analysis was carried out through a descriptive and interpretive process involving the stages of organizing, coding, and interpreting data thematically. Thematic analysis was used to

https://doi.org/10.33019/society.v13i2.960

identify patterns and relationships among key variables such as sovereignty, cybersecurity politics, institutional authority, and policy integration. Triangulation of data sources was applied by comparing findings from interviews, documents, and literature to ensure credibility and validity. The analytical process aimed to connect empirical realities to theoretical constructs, thereby providing a comprehensive understanding of how political and institutional factors shape Indonesia's cybersecurity governance.

The unit of analysis in this study is the National Cyber and Crypto Agency (BSSN), which is examined as the central state institution responsible for coordinating national cybersecurity policy and ensuring the protection of Indonesia's digital sovereignty. To provide a broader institutional perspective, the study also considers the roles of other agencies such as the Ministry of Communication and Informatics, BIN, and the Ministry of Defense, which interact with BSSN in policy formulation and implementation. The integration of these perspectives enables the study to describe the systemic challenges of inter-agency coordination and political commitment in achieving effective and sovereign cybersecurity governance in Indonesia.

4. Results and Discussion

Various agencies in Indonesia have also experienced multiple data leaks and cyberattacks, both government and private. Even the personal data of Indonesian citizens is being traded on several websites, providing personal gain to irresponsible individuals. This is undoubtedly very detrimental to the data owners. The national digital ecosystem also lacks cybersecurity guarantees, which can hamper the development of community activities in cyberspace due to the lack of adequate security guarantees. Several data leak incidents and cyberattacks in Indonesia that have occurred over the past few years can be seen in the following table:

Table 4. Major Data Breaches and Cyberattack Incidents in Indonesia (2020–2024)

No.	Institution / Organization	Year	Type and Scope of Incident
1	Lazada	2020	A data breach involving approximately 1.1 million customer records was allegedly leaked online.
2	Tokopedia	2020	Large-scale breaches exposed data from around 91 million user accounts, including personal information and credentials.
3	General Elections Commission (KPU)	2020	An alleged hacking incident in which data of 2.3 million registered voters was claimed to have been compromised.
4	Social Security Administration for Health (BPJS Kesehatan)	2021	Massive breach where personal data of approximately 270 million Indonesian citizens was allegedly sold on dark web forums.
5	BRI Life Insurance	2021	Cyber incidents in which data from around two million customers were reportedly offered for sale for USD 7,000 on illicit platforms.
6	State Intelligence Agency (BIN)	2021	Alleged intrusion into the official BIN website, suspected of compromising sensitive government information.
7	Ministry of Communication and Informatics (Kominfo)	2022	Breach of the Electronic System Operators (PSE) website, affecting access to several public digital services.

https://doi.org/10.33019/society.v13i2.960

No.	Institution / Organization	Year	Type and Scope of Incident
8	Ministry of Defense	2023	Alleged hacking of the official Ministry of Defense website attributed to unidentified foreign threat actors.
9	Ministry of Home Affairs (Dukcapil Directorate)	2023	Suspected leak of 337 million population database records, reportedly accessible through online hacker forums.
10	General Elections Commission (KPU)	2024	Permanent Voter List (DPT) data allegedly leaked, raising concerns ahead of the 2024 general elections.

Source: Compiled and synthesized from various credible media and institutional reports (2020–2024).

The COVID-19 pandemic has had a number of impacts, including a decline in Indonesia's Gross Domestic Product (GDP). However, Indonesia experienced rapid digital economic growth in 2020, reaching 11%, which is estimated at around US$44 billion. Indonesia also boasts a vibrant digital business ecosystem, home to approximately 2,000 startups operating in the country, significantly impacting the market share of cloud computing services in Indonesia. Indonesia also boasts five of the 13 unicorns in the ASEAN region, each with significant budgets for cloud computing services (Amiruddin & Yazid, 2023). These factors demonstrate Indonesia's strategic market share in the digital economy, both domestically and internationally. Therefore, a powerful agency is needed to realize cyber sovereignty and ensure that this potential positively impacts the Indonesian nation.

In the context of national cybersecurity policy, political support is needed to establish the National Cyber and Crypto Agency (BSSN) as a competent institution in safeguarding national cybersecurity. Various factors in national cybersecurity policy are essential for the fulfillment and seriousness of the state in representing its presence in cyberspace. The state's commitment, represented by the government and the House of Representatives (DPR) in the revitalization of the BSSN, should provide support for various necessary regulatory certainties. The existence of strong regulations is directly proportional to budgetary support, which is also greatly needed by the BSSN. Regarding the cybersecurity and cryptography regulations and policies described by the researcher in the previous chapter, various factors appear to influence the existence of national cybersecurity policy. This aligns with Cavelty and Wenger's (2020) explanation of six factors influencing cybersecurity policy. The researcher will explain these factors as follows:

Table 5. Analysis of Six Factors Driving Cybersecurity Politics in Indonesia

Main Factor	Conceptual Definition	Contextual Analysis in Indonesia
Technology	The development and advancement of digital technology influence the formation of cybersecurity policies and the capacity of the state to secure its cyberspace.	Political awareness of cybersecurity urgency in Indonesia only began to emerge in 2017 with the establishment of the National Cyber and Crypto Agency (BSSN). However, this institutional formation was not accompanied by strong regulatory backing, resulting in limited authority and suboptimal performance.

https://doi.org/10.33019/society.v13i2.960

Main Factor	Conceptual Definition	Contextual Analysis in Indonesia
Important Events (Cyber-Related Incidents)	Significant events, whether originating in cyberspace or external to it, often trigger changes in cybersecurity priorities and policy responses.	Political attention to cybersecurity remained limited until several high-profile data leak incidents and the Surabaya BSSN case, which highlighted the urgency of establishing a coordinated national cybersecurity system and elevating cybersecurity as a strategic national agenda.
International Politics	Global power relations and the emergence of "cyber power" shape national responses, as countries seek to assert digital sovereignty and strategic defense.	The evolving international landscape, marked by cyber espionage and competition among major powers, has compelled Indonesia to strengthen its cyber defense. This includes discussions on forming cyber defense units and enhancing bilateral cooperation with partner countries to secure critical infrastructure.
National Politics	Domestic political negotiations determine the distribution of roles, authority, and accountability among state institutions.	The leadership transition at BSSN in 2025 presents a strategic opportunity to accelerate the Cyber Security and Resilience Bill (RUU KKS), which has re-entered the National Legislation Program (Prolegnas). Political will at the national level will be decisive in ensuring legal certainty and effective coordination.
Academic Debate	Academic discussions influence how cybersecurity is conceptualized, debated, and legitimized within policy and public discourse.	Scholarly debate on national cybersecurity remains limited and has yet to gain significant public attention. Research on cyber politics, sovereignty, and digital governance in Indonesia is still fragmented and concentrated in a few institutions.
Institutionalization	The process of embedding cybersecurity within formal structures of education, research, and policy development.	Institutionalization of cybersecurity studies is still at an early stage. Only a few universities and research centers have developed dedicated programs or research clusters focusing on cybersecurity governance and policy. Strengthening these institutions is crucial to support evidence-based policymaking.

Source: Adapted and contextualized from Dunn Cavelty & Wenger (2020) and national cybersecurity developments in Indonesia (2017–2025).

Based on this analysis, researchers observed that the significant political factors affecting cybersecurity in Indonesia are related to political and technological factors. Meanwhile,

https://doi.org/10.33019/society.v13i2.960

scientific factors have not significantly influenced national cybersecurity policy. This is interesting because political factors are key factors in developing a national cybersecurity strategy. The new leadership at the National Cyber and Crypto Agency (BSSN) is expected to accelerate various programs that have been delayed due to a lack of political support for the agency.

Efforts to achieve cyber sovereignty require a strong commitment from all political institutions in Indonesia. However, bureaucratic dynamics are often characterized by sectoral egos, with each institution tending to prioritize its own interests. This phenomenon is a fundamental obstacle to the process of integrating cybersecurity policies. Sectoral and partial governance and work mechanisms create an urgent need for coordinated and integrated cross-institutional cooperation. This lack of institutional integration opens up significant vulnerabilities to cyber threats. Numerous data breach incidents in the public sector indicate that the government lacks the capacity to manage public personal data fully. Over the past five years, several data breaches have been recorded, including those involving the eHAC application, BPJS Kesehatan (Healthcare Social Security Agency), the General Elections Commission (KPU) Permanent Voter List (DPT), e-KTP (e-KTP), and PDNS2 (National Data Protection Agency). This fact indicates that the government has been unable to provide a comprehensive solution to the data breach problem (Sembiring & Pattihahuan, 2025).

The personal data leak on the Temporary National Data Center 2 (PDNS2) server should no longer lead to shifting responsibilities between the National Cyber and Cyber Security Agency (BSSN), the Ministry of Communication and Informatics, and Telkomsigma. Based on Article 38 of Presidential Regulation No. 28 of 2021, BSSN is obligated to coordinate with other institutions in maintaining cybersecurity. Although BSSN argues that cyber protection is a shared responsibility, BSSN's position as the leading sector in cybersecurity, as affirmed in Article 2 of Presidential Regulation No. 28 of 2021, cannot be ignored. Therefore, BSSN cannot simply relinquish responsibility to other institutions, as this would contradict the principles of synchronization and coordination between institutions as stipulated in the same Presidential Regulation. Therefore, synergy between BSSN and the Ministry of Communication and Informatics is crucial in handling the PDNS2 data leak. If sectoral egos continue to be maintained, it will lead to ambiguity and uncertainty in public data protection. Ultimately, the primary responsibility for cybersecurity remains with BSSN, but its implementation must involve collaboration with relevant ministries, agencies, and institutions (Sembiring & Pattihahuan, 2025).

According to Guna in Sembiring and Pattihahuan, the practice of governance in Indonesia often faces various long-standing bureaucratic obstacles (Sembiring & Pattihahuan, 2025). These obstacles primarily stem from the problem of sectoral ego, namely the tendency of state institutions to prioritize their own interests over building synergistic cooperation. This condition is usually triggered by weak coordination and communication between institutions, so that each institution tends to operate independently without a precise integration mechanism. This phenomenon of sectoral ego is often referred to as silo mentality, namely a bureaucratic mentality characterized by the reluctance of institutions to share information, coordinate, or cooperate with other actors within a single government system. This mentality not only creates distance between institutions but also gives rise to rigid, exclusive relationship patterns that are prone to conflicts of interest. In practice, silo mentality generally arises due to internal and external competition between state institutions, which ultimately worsens communication and hinders the development of shared understanding. Thus, sectoral ego can

https://doi.org/10.33019/society.v13i2.960

be said to be one of the crucial factors that hinders the effectiveness of bureaucracy and reduces the government's capacity to provide optimal public services (Sembiring & Pattihahuan, 2025).

Regarding cross-sectoral coordination between ministries/institutions, the author also wishes to link it to the Sovereignty Theory proposed by Jean Bodin and Paul Laband (Bakhri, 2018). The Theory of State Sovereignty explains that sovereignty resides with the state, not with God. All must obey the state because it is the state that makes the laws. The state is the best unity of ideas. Therefore, the state is considered to have rights over the lives of its people.

Meanwhile, Harold J. Laski explains that, "a state is a society that is united because it has the authority that can force and has formal legitimacy with a higher position than the units within a society (Bakhri, 2018). Society is a combination of humans who come together to achieve the goals they aspire to together. Society can be said to be a state if the guidelines for life that must be followed and implemented are regulated by an authority that is coercive and binding. In the context of national cybersecurity politics, various other things cause the slow process of ratifying the Draft Law on Cyber Security and Resilience, which is very necessary for BSSN to be able to carry out its roles and functions. Therefore, the presence of the state as the highest authority is essential to overcome various obstacles that arise due to elite interests and other political factors to achieve the state's goal, namely, strengthening BSSN to become a strong institution to build cyber sovereignty.

Strengthening the authority of the National Cyber and Cyber Security Agency (BSSN) is now essential. Strengthening the BSSN illustrates the importance of state representation in securing cyberspace. The author has analyzed related data and then used it to explain various aspects of strengthening the current BSSN authority. The first aspect is the legal aspect. The legal aspect of strengthening the BSSN's authority depends heavily on the ratification of the Cyber Security and Resilience Bill (RUU KKS), which is currently included in the 2025 National Legislation Program (Prolegnas). The presence of this RUU KKS will significantly determine the direction of the BSSN in carrying out its duties and functions as a key pillar of cybersecurity. The RUU KKS is also crucial for building cyber sovereignty in Indonesia.

The current strategy to strengthen the authority of the National Cyber and Crypto Agency (BSSN) also involves increasing the budget needed to support the structure and function of the agency so that it can play an optimal role. The capabilities and potential of the BSSN's human resources are extraordinary, but this is futile without adequate budgetary support. Further strengthening of the BSSN's authority is related to improving its cyber diplomacy capabilities. This is crucial because some countries that lack adequate cybersecurity capabilities will also receive protection after joining a cybersecurity coalition of countries with strong cybersecurity capabilities. This is similar to what we see in the European Union. Therefore, the BSSN needs to enhance its existing collaborations. Various MoUs with the Netherlands, Australia, and others can be further strengthened. Based on the aspects analyzed by the author regarding the strategy to strengthen the authority of the BSSN, the following table summarizes the following:

Table 6. Strategies for Strengthening the Authority of the National Cyber and Crypto Agency (BSSN–Republic of Indonesia)

No.	Aspect	Focus of Authority Strengthening	Proposed Strategy
1	Legal Framework	Enactment of the Cyber Security and Resilience Act to provide legal certainty and	Accelerate the ratification of the *Cyber Security and Resilience Bill (RUU KKS)* through strong executive–legislative

https://doi.org/10.33019/society.v13i2.960

No.	Aspect	Focus of Authority Strengthening	Proposed Strategy
		clear institutional authority for BSSN.	coordination and policy advocacy.
2	Budget Allocation	Increased national cybersecurity budget to support BSSN's institutional capacity and operational readiness.	Ensure incremental budget allocation in the 2026 National Budget (APBN) to fund infrastructure modernization, training, and strategic operations.
3	Cyber Diplomacy	Expansion of international and domestic cooperation in cybersecurity governance and capacity building.	Increase the number of Memoranda of Understanding (MoUs) and joint initiatives on cybersecurity with foreign partners and domestic institutions to enhance multilateral engagement.
4	Human Resources and Remuneration	Improvement of employee welfare and performance incentives to attract and retain qualified cybersecurity professionals.	Raise remuneration levels and implement performance-based incentives to strengthen professionalism and institutional morale.

Source: Compiled and processed by the researcher from various official and secondary sources (2024–2025).

The next crucial aspect concerns remuneration. BSSN will undoubtedly function more optimally if its employees are also well-off. This requires support from all parties, particularly within the BSSN itself, including the Ministry of Finance and the Ministry of Administrative and Bureaucratic Reform (PAN RB). Strengthening the BSSN's role does not stop at the current context; it is necessary to examine and address the institution's future structure and functions. As time goes by, technological advancements will continue to accelerate. Future challenges for the BSSN will undoubtedly increase in maintaining national sovereignty in cyberspace. The BSSN is a highly strategic institution, and its strengthening must be carried out continuously. Therefore, various strategies are needed to strengthen the BSSN's authority to continue to respond to the challenges of the times.

The new format of national cybersecurity governance following the establishment of the National Cyber and Crypto Agency (BSSN) has undergone significant changes. With the establishment of the BSSN in 2017, this agency became the center of national cybersecurity. Several other government agencies still have roles and functions related to cyberspace, such as Ministry of Communication and Digital, which regulates internet and data regulations, the Ministry of Defense which plays a role in cyber defense, the Police which plays a role in the context of cybercrime, the State Intelligence Agency (BIN) which functions as cyber intelligence, and the Ministry of Foreign Affairs which plays a role in the context of cyber diplomacy. However, related to the context of cybersecurity, it has become the primary domain of the BSSN, which has also transformed hierarchically from Lemsaneg (National Crypto Agency) under the Ministry of Defense to BSSN, a government agency with ministerial-level status. The position of BSSN is also no longer subordinate to the Ministry of Defense, but directly under the President. In the new format of cybersecurity governance in Indonesia, the BSSN plays a

https://doi.org/10.33019/society.v13i2.960

supervisory role in cybersecurity. BSSN has a central role in detecting and monitoring cyber attacks. The National Cyber and Crypto Agency (BSSN) can conduct various cybersecurity expertise certifications; thus, BSSN has a primary role in responding to and mitigating cyber incidents.

To strengthen the foundation of cybersecurity, BSSN has formed various working team units that can play a role in handling cybersecurity issues. The establishment of Gov-CSIRT is intended for the government (ministries/agencies) related to cybersecurity in government agencies. Then, the Cyber Incident Response Teams (TTIS) will be established in various regional governments (provinces/districts/cities) to handle cybersecurity issues in the regions that follow guidance from the central government. Then, the establishment of Sectoral CSIRTs is intended for the private sector and industry, such as banking, health, education, and others. The existence of several divisions can optimize the role of each CSIRT so that they can focus on their respective sectors. The needs and dynamics between the central government sector, local governments, and the private sector and industry certainly have differences, requiring a tailored approach. If national cybersecurity can be optimally maintained, cyber sovereignty can be realized. Sectoral egos between ministries/institutions can be suppressed so that the national cybersecurity policy can position BSSN as the leading agency or coordinator of national cybersecurity.

5. Conclusion

Cybersecurity politics play a decisive role in shaping the realization of cyber sovereignty in Indonesia. The study finds that the effectiveness of national cybersecurity governance is determined not only by technological capabilities but also by political configurations, institutional coordination, and the strength of legal foundations that define the state's authority in cyberspace. The National Cyber and Crypto Agency (BSSN) holds a central function as the state's representative in safeguarding national interests in the digital domain. However, its authority remains limited by overlapping institutional mandates, sectoral fragmentation, and the absence of a comprehensive legal framework that can ensure coordination and enforcement.

Strengthening BSSN's role requires clear regulatory support through the ratification of the Cyber Security and Resilience Bill, which will provide legal certainty and establish an integrated national cybersecurity system. Institutional consolidation, adequate budget allocation, and human resource development are equally essential to reinforce its operational effectiveness. These efforts must be supported by strong political will and consistent leadership commitment to build a resilient and sovereign national cybersecurity architecture.

In the broader context, the establishment of a robust cybersecurity governance system will position Indonesia as an active and credible actor in the global digital landscape. The government must accelerate the implementation of national cybersecurity policies and ensure synergy among relevant agencies to minimize duplication and sectoral competition. Building cyber sovereignty is a long-term process that demands collaboration across institutions, adaptive policy frameworks, and public awareness of cybersecurity as part of national resilience. Continuous improvement in policy integration and institutional capacity will enable Indonesia to protect its digital sovereignty and enhance its competitiveness in the era of global interconnection.

https://doi.org/10.33019/society.v13i2.960

6. Acknowledgment

The author expresses gratitude to all parties who have provided excellent cooperation during this research.

7. Declaration of Conflicting Interests

The author affirms that no known financial or personal relationships could have appeared to influence the work reported in this article.

References

Amiruddin, A., & Yazid, S. (2023). Tinjauan Strategis Keamanan Siber Indonesia. In D. F. Priambodo & S. U. Sunaringtyas (Eds.), *Politeknik Siber dan Sandi Negara Press*. Politeknik Siber dan Sandi Negara Press.

Baezner, M., & Robin, P. (2018). *Cyber sovereignty and Data Sovereignty*. ETH Zürich.

Bakhri, S. (2018). *Ilmu Negara: Dalam pergumulan filsafat, sejarah dan negara hukum*. PT. Raja Grafindo Persada.

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. https://doi.org/10.22212/jp.v10i2.1447

CNN Indonesia. (2021). Jaringan BIN dan Kementerian Dilaporkan Dibobol Hacker China. *CNN Indonesia*. https://www.cnnindonesia.com/nasional/20210912112723-20-693110/jaringan-bin-dan-kementerian-dilaporkan-dibobol-hacker-china

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Hao, Y. (2017). A Three-Perspective Theory of Cyber Sovereignty. *PRISM*, *7*(2), 108–115. https://ndupress.ndu.edu/Media/News/Article/1327736/a-three-perspective-theory-of-cyber-sovereignty/

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. https://doi.org/10.34010/gpsjournal.v7i1.8141

Qiao-Franco, G. (2024). An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries? *Global Studies Quarterly*, *4*(1), 1–11. https://doi.org/10.1093/isagsq/ksad077

Romaniuk, S. N., & Manjikian, M. (2021). Routledge Companion to Global Cyber-Security Strategy. In S. N. Romaniuk & M. Manjikian (Eds.), *Routledge Companion to Global Cyber-Security Strategy*. Routledge. https://doi.org/10.4324/9780429399718

Sembiring, F., & Pattihahuan, F. M. (2025). Peran Badan Siber Dan Sandi Negara Dalam Kasus Serangan Siber Yang Mengakibatkan Kebocoran Data Pribadi Pusat Data Nasional Sementara 2 (PDNS2). *Gloria Justitia*, *5*(1), 116–134. https://journal.unpar.ac.id/index.php/gloriajustitia

Sudarmadi, D., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2). https://doi.org/10.7454/jkskn.v2i2.10028

Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index 2022* (Issue September). Belfer Center for Science and International Affairs, Harvard Kennedy School.

https://doi.org/10.33019/society.v13i2.960

www.belfercenter.org/project/cyber-project%0Ahttps://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National Cyber Power Index 2022_v3_220922.pdf

Walter, M., Kukutai, T., Carroll, S. R., & Rodriguez-Lonebear, D. (2020). Indigenous Data Sovereignty and Policy. In *Indigenous Data Sovereignty and Policy*. Routledge. https://doi.org/10.4324/9780429273957

About the Author

Muhammad Prakoso Aji is a Senior Lecturer in the Department of Political Science, Faculty of Social and Political Sciences, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia. He earned his academic qualifications from the University of Indonesia and previously served at the Ministry of Home Affairs of the Republic of Indonesia. His research interests include bureaucracy and politics, cyber politics, cybersecurity, strategic and global studies, and political communication. He frequently employs qualitative research methodologies, particularly case study and phenomenological approaches, in his academic works. He has authored and co-authored several books and peer-reviewed journal articles focusing on public governance and political dynamics in Indonesia.

Email: prakosoaji@upnvj.ac.id

https://doi.org/10.33019/society.v13i2.960