*PALAR (Pakuan Law Review)*
*https://journal.unpak.ac.id/index.php/palar*

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

# Fragmentation of Authority in National Cyber Defense A Legal Analysis of Overlapping Inter-Agency Authority and the Urgency of Integrated Command

**Restu Putri Pamungkas[1]; Bambang Kustiawan[2]; Asep Adang Supriyadi[3]; Guntur Eko Saputro[4].**

[1,2,3] *Doctoral of Defense Science, Indonesia Defence University, Indonesia.*
*E-mail:* restu.pamungkas@doktoral.idu.ac.id, bkustiawan168@gmail.com
aadangsupriyadi@idu.ac.id guntur.saputro@idu.ac.id
Manuscripts received : 02/01/2026, Revision and Review : 28/01/2026, Approved 16/02/2026

**Abstract**

**The evolution of cyberspace as the fifth domain of warfare has transformed the national defense landscape, where hybrid threats can now disrupt sovereignty without physical war declarations. Indonesia responds to this challenge through the Total People's Defense and Security System (Sishankamrata) doctrine, yet its implementation is hindered by acute institutional fragmentation. This study aims to analyze the implications of regulatory disharmony on strategic defense effectiveness and formulate an ideal legal construction for national cyber governance. Using normative legal research methods with statutory and conceptual approaches, this study finds that current sectoral regulations create legal antinomy between defense mandates (Military/TNI), law enforcement (Police/Polri), and administrative security (National Cyber and Crypto Agency/BSSN). An asymmetry of authority is identified where BSSN, as the coordinator, is based only on a Presidential Regulation, lacking operational coercive power over institutions established by Law. The absence of legal escalation mechanisms in the "grey zone" leads to decision-making paralysis during crises. This study concludes the need for legal reconstruction through the enactment of a Cyber Security and Defense Law as lex specialis. This law must institutionalize a Unified Command System that establishes a single authority and clear thresholds for transferring operational control from civil to military domains, ensuring a rapid, integrated, and legally certain state response.**

**Keywords: National Cyber Security Policy, Strategic Defense, Authority Fragmentation, Unified Command, Total Defense System.**

## A. Introduction

Global geopolitical transformation has positioned cyberspace as the fifth domain in modern defense doctrine, which has a complexity equivalent to that of traditional kinetic domains[1]. This recognition has significant legal implications, whereby cyber attacks can

[1] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.

Volume 12, Number 01, January-March 2026, Pages 105-116
**e-ISSN:2614-1485**
**p-ISSN:2716-0440**
**Doi: https://doi.org/10.33751/palar.v12i1**
**Sinta 3; decree No. 0173/C3/DT.0500/2025**

now be categorized as "use of force" under Article 2(4)[2] of the UN Charter if the impact is equivalent to a physical attack[3]. However, the asymmetric and borderless nature of cyberspace creates challenges for international law in establishing uniform standards for digital sovereignty defense, forcing countries to formulate robust yet adaptive domestic cyber defense policies[4].

The main issue in strategic cyber defense is the exploitation of the "Grey Zone," where state actors carry out intrusions that fall just below the threshold of armed attack in order to avoid legitimate military retaliation[5]. The problem of legal attribution is a major obstacle; determining state responsibility for attacks carried out by non-state actors or pro-state hackers requires evidence that exceeds conventional criminal law standards[6]. This ambiguity calls for a national legal framework capable of defining the boundary between civilian cybersecurity disruptions and cyber aggression that threatens national defense.

Indonesia has a philosophical-defensive foundation through the Universal People's Security Defense System (Sishankamrata) mandated in Law Number 3 of 2002[7] concerning National Defense. This doctrine emphasizes the involvement of all components of the nation, but its implementation in cyberspace faces integration challenges. In the cyber context, Sishankamrata requires seamless collaboration between the military and civilians, but legally, the distribution of authority in Indonesia is still stuck in a sectoral model that threatens the principle of strategic defense unity[8].

In response to cyber challenges, the Indonesian government has issued Presidential Regulation No. 47 of 2023 concerning the National Cyber Security Strategy and Cyber Crisis Management[9]. This regulation establishes the National Cyber and Crypto Agency (BSSN) as the main coordinator based on Presidential Regulation No. 28 of 2021[10]. On the other hand, the Indonesian National Armed Forces (TNI) has officially integrated its functional units through Article 45 of Presidential Regulation No. 66 of 2019 concerning the Organizational Structure of the TNI, which forms the TNI Cyber Unit (Satsiber TNI) as a central supporting element[11]. Although the structure has been established, the working relationship between

---

[2] Christian Tams, "Article 2 (4)," in *The Charter of the United Nations: A Commentary*, ed. Bruno Simma et al. (Oxford University Press, 2024), https://doi.org/10.1093/law/9780192864536.003.0010.

[3] Daniel Silver, "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter," *International Law Studies* 76, no. 1 (2002), https://digital-commons.usnwc.edu/ils/vol76/iss1/21.

[4] Eldar Haber and Lev Topor, "Sovereignty, Cyberspace, and the Emergence of Internet Bubbles," *Journal of Advanced Military Studies* 14 (June 2023), https://doi.org/10.21140/mcuj.20231401006.

[5] Pauline C. Reich et al., "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity," *European Journal of Law and Technology* 1, no. 2 (2010), https://ejlt.org/index.php/ejlt/article/view/40.

6 Duncan B. Hollis, The Oxford Guide to Treaties, Second Edition, Second Edition, ed. Duncan B. Hollis (Oxford University Press, 2020).

7 Indonesia Governance, "Law No 3, 2002," Database Peraturan | JDIH BPK, accessed January 2, 2026, http://peraturan.bpk.go.id/Details/44421/uu-no-3-tahun-2002.

8 Andi Cinrapole and Arianty Mangarengi, "DILEMA YURIDIKSI DI RUANG SIBER: TANTANGAN DAN STRATEGI PENEGAKAN KEAMANAN LINTAS NEGARA," JUDICATUM: Jurnal Dimensi Catra Hukum 3 (June 2025): 221–35, https://doi.org/10.35326/judicatum.v3i1.7734.

9 Indonesia Governance, "Presidential Regulation," Database Peraturan | JDIH BPK, accessed January 2, 2026, http://peraturan.bpk.go.id/Details/255542/perpres-no-47-tahun-2023.

10 Indonesia Governance, "Presidential Regulation No 28 of 2001," Database Peraturan | JDIH BPK, accessed January 2, 2026, http://peraturan.bpk.go.id/Details/165493/perpres-no-28-tahun-2021.

11 Indonesia Governance, "Presidential Regulation No 66 of 2019," Database Peraturan | JDIH BPK, accessed January 2, 2026, http://peraturan.bpk.go.id/Details/123703/perpres-no-66-tahun-2019.

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

BSSN (civilian-coordinative) and TNI (military-defensive) still leaves room for broad interpretation in crisis situations.

This study identifies the occurrence of "Authority Fragmentation" rooted in unclear demarcation of authority. BSSN has a mandate on government information security and critical infrastructure, Polri on law enforcement through the ITE Law (most recently Law No. 1 of 2024), and TNI on defense of sovereignty[12]. Problems arise when a cyberattack is hybrid in nature, targeting civilian data but aiming to paralyze defense stability[13]. Without a Unified Command mechanism regulated at the law level, the state's response will be trapped in deadly bureaucratic coordination inefficiencies[14].

From a constitutional law perspective, there is a serious issue of regulatory hierarchy. The BSSN was established and given coordination authority through a Presidential Regulation, which is normatively subordinate to the law. This condition creates a weakness in the legal bargaining position when the BSSN has to coordinate institutions such as the TNI and Polri, whose main mandates are directly regulated by law (Law No. 34/2004 and Law No. 2/2002)[15]. As a result, coordination instructions are often voluntary and lack the operational coercive power necessary for strategic defense[16].

The failure to protect the National Data Center (PDN) in late 2024 and early 2025 is irrefutable empirical evidence of the failure of Indonesia's integrated command system. This incident shows that even though a national cyber strategy policy has been issued (Presidential Regulation 47/2023), without clarity on who holds the highest authority (Single Point of Command) during a crisis, responsibilities become scattered and the recovery process becomes slow. The absence of an "escalation" protocol from the civilian sphere to the national defense sphere is a very risky legal loophole.

Internationally, countries with high cyber resilience tend to adopt more cohesive structures. By comparison, Singapore's Cybersecurity Act 2018 grants extraordinary powers to the Commissioner of Cybersecurity to take control of critical infrastructure during emergencies[17]. Meanwhile, the United States integrates cyber operations through US Cyber Command, which works closely with the National Cybersecurity and Communications Integration Center (NCCIC). These models emphasize that the effectiveness of cyber defense is highly dependent on legal clarity regarding leadership during crises.

12 Indonesia Governance, "Law No 1 of 2024," accessed January 2, 2026, https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024.

13 Dhiraj Kelly Sawlani and Asep Adang Supriyadi, "Bridging Public Policy And Defense Strategy To Combat Hybrid Warfare: An Analytical Study On National Security," Jurnal Praksis Dan Dedikasi Sosial 7, no. 2 (2024): 292–307; Roedy and Asep Adang Supriyadi, "Integrasi Kebijakan Pertahanan Dan Kebijakan Publik Dalam Penanggulangan Ancaman Perang Hibrida: Pendekatan Analisis Keamanan Nasional," Inovasi Pembangunan : Jurnal Kelitbangan 13, no. 1 (2025), https://doi.org/10.35450/jip.v13i1.992.

14 Muhammad Faiq Qushayyi, "The Dynamics of Cyber Security Cooperation Between Countries: A Case Study of Indonesia and the Netherlands," Journal of Peace, Security and Democracy 1, no. 1 (2025): 37–56, https://doi.org/10.63280/jpsd.v1i1.42626.

15 Indonesia Governance, "Law No. 2 of 2002," Database Peraturan | JDIH BPK, accessed January 2, 2026, http://peraturan.bpk.go.id/Details/44418/uu-no-2-tahun-2002; Indonesia Governance, "Law No 1 of 2024."

16 Nurul Aini and Fauziah Lubis, "TANTANGAN PEMBUKTIAN DALAM KASUS KEJAHATAN SIBER," Judge : Jurnal Hukum 5, no. 02 (2024): 55–63.

17 Haber and Topor, "Sovereignty, Cyberspace, and the Emergence of Internet Bubbles."

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

This study argues that Indonesia urgently needs a "Cyber Security and Defense Law" as a lex specialis that can harmonize various sectoral regulations. Legal reconstruction is necessary to clearly define the classification of cyber attacks, command escalation mechanisms, and legal protection for military cyber operators in conducting active defense operations. Without a strong legal basis, any strategic defense action risks violating the principles of legality and national legal sovereignty.

The novelty of this research lies in its legal-normative approach, which focuses on developing an Integrated Command model that is in line with the characteristics of administrative and defense law in Indonesia. Unlike previous studies that focused on information security techniques, this study contributes to the formulation of jurisdictional divisions between the National Cyber and Encryption Agency (BSSN), the Indonesian National Armed Forces (TNI), and the Indonesian National Police (Polri) within the strategic defense ecosystem. The aim is to create legal certainty that enables a rapid, integrated, and legally binding state response to future cyber threats.

## B. Research Method

This study was conducted using normative legal research methodology, which views law as a closed system of norms consisting of principles, rules, and legislation. Given that the object of this study focuses on the fragmentation of authority and cyber defense strategy policies, this study uses secondary data as the main basis for analysis, with an emphasis on vertical and horizontal legal synchronization. Technically, this study does not conduct empirical field observations, but rather conducts an in-depth examination of "written law" to identify contradictions in norms, regulatory gaps, and jurisdictional ambiguities that hinder the effectiveness of national strategic defense.

In order to achieve a comprehensive depth of analysis, this study integrates four main approaches in legal science. First, the statute approach is used to dissect the hierarchy of regulations, starting from the 1945 Constitution of the Republic of Indonesia, the State Defense Law, the TNI Law, to technical regulations such as the Presidential Regulation on National Cyber Security Strategy (Presidential Regulation 47/2023) and the Presidential Regulation on BSSN. Second, the conceptual approach is applied to explore legal doctrines of defense such as Unity of Command, digital sovereignty, and the Sishankamrata principle as ideal parameters in assessing existing regulations. Third, the comparative approach is carried out by examining the legal framework of cyber authorities in other countries such as, Singapore and the United States as international best practice standards. Finally, an analytical case approach is used to dissect systemic failures such as attacks on the National Data Center as clear evidence of the dysfunction of existing coordination norms.

The legal materials in this study are rigidly classified into three main categories. Primary legal materials consist of legislative and regulatory instruments that have legally binding force, including the latest revision of the ITE Law (Law No. 1 of 2024) and the Tallinn Manual 2.0 as a reference for international law related to cyber operations. Secondary legal materials include academic literature, reputable international journals, and the thoughts of

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

legal and defense experts who provide interpretations of primary legal materials. Meanwhile, tertiary legal materials in the form of legal dictionaries and encyclopedias are used to clarify multidisciplinary technical terminology in the fields of law, military, and information technology. All of these legal materials were collected through systematic library research using classification and categorization techniques based on clusters of issues of authority.

The final stage of this methodology is a qualitative analysis of legal materials using deductive-prescriptive reasoning. Deductive analysis is conducted by drawing conclusions from general principles of defense law to specific phenomena in the form of overlapping authorities between cyber institutions in Indonesia. Researchers use systematic interpretation methods to examine the interrelationships between regulations and teleological interpretations to understand the fundamental objectives of each national cyber policy. Technically, this analysis aims to produce a prescriptive formulation in the form of a regulatory reconstruction model that is capable of eliminating fragmentation of authority and realizing an integrated command structure that has legal certainty, so that the results of this study can serve as an academic basis for the formation of future strategic policies.

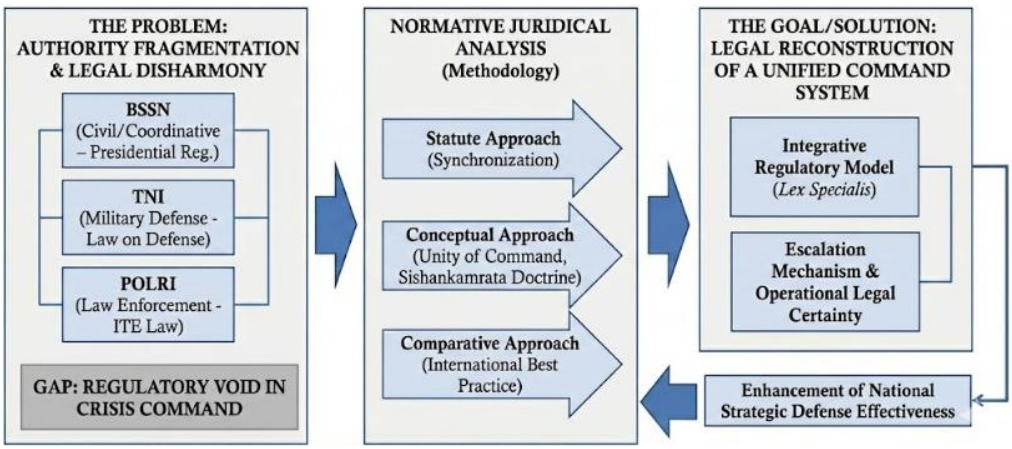


Figure 1. Research Design

## C. Results and Discussion

### a. Jurisdictional Fragmentation in National Cyberspace Governance

An analysis of Indonesia's cyber law architecture reveals a fundamental disharmony rooted in a sectoral approach to regulation. Instead of adopting an integrated "Whole-of-Government" framework as suggested in modern cyber governance literature[18], Indonesia has divided its cybersecurity mandate into three isolated jurisdictional clusters: military defense (TNI), law enforcement (Polri), and administrative security (BSSN). A study conducted by Aini & Lubis. (2022) confirms that this kind of institutional fragmentation creates a "vulnerability gap" in which the state's response becomes incoherent due to the absence of an umbrella act that synchronizes civil and military roles[19].

Normatively, the role of the TNI is regulated in Law Number 34 of 2004 concerning the

18 Alexander Klimburg, "National Cyber Security Framework Manual," 2012, https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.
19 Aini and Lubis, "TANTANGAN PEMBUKTIAN DALAM KASUS KEJAHATAN SIBER."

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
**Sinta 3; decree No. 0173/C3/DT.0500/2025**

TNI, specifically Article 7 paragraph (2) concerning Military Operations Other Than War (OMSP)[20]. However, this law does not explicitly define "cyber attacks" as a form of aggression that justifies the deployment of military force. This creates an operational dilemma highlighted by Schmitt (2017) in the Tallinn Manual 2.0. According to Schmitt, without a clear legal definition of the threshold for an "Armed Attack" in cyberspace, military involvement in responding to cyber incidents risks violating international and domestic law[21]. As a result, Indonesia's enemy-centric military doctrine (focused on neutralizing threats to sovereignty) becomes difficult to activate quickly, as it is hampered by a legal vacuum that determines when a cyber incident shifts from a civil matter to a matter of national defense[22].

In the realm of law enforcement, jurisdiction is dominated by the criminal justice model through Law No. 1 of 2024 (Second Amendment to the ITE Law)[23]. This approach views every cyber attack as a cybercrime that must be resolved through investigation and prosecution mechanisms. However, international academic literature criticizes this approach when applied to state-sponsored attacks. Shackelford (2012) argues that dealing with strategic cyber attacks solely with criminal law instruments is a strategic mistake, because foreign state actors have immunity and cannot be reached by ordinary legal processes[24]. By categorizing attacks on critical infrastructure as merely "criminal acts," Indonesia indirectly "belittles" the status of these threats, thereby losing the legitimacy to take defensive countermeasures (active defense) or cyber deterrence that are common in defense doctrine[25].

The coordination problem is exacerbated by the position of the National Cyber and Crypto Agency (BSSN), which was established based on Presidential Regulation No. 28 of 2021. In the hierarchy of norms, a presidential regulation has a lower status than the law that forms the basis for the establishment of the TNI and Polri. Qushayyi (2023), in their analysis of inter-agency cooperation in Indonesia, emphasize that a coordinative mandate without command authority is a recipe for failure in crisis management[26]. The BSSN does not have the coercive power to direct TNI or Polri resources when a crisis occurs. This is in line with the Command and Control (C2) theory, which states that the effectiveness of cyber defense depends on unity of command, not merely voluntary coordination that is vulnerable to bureaucratic sectoral egos[27].

The combination of the above legal factors has resulted in the absence of a legal escalation mechanism. There is no article that regulates "when and how" operational control

20 Indonesia Governance, "Law No 34 of 2004," Database Peraturan | JDIH BPK, accessed January 2, 2026, http://peraturan.bpk.go.id/Details/40774/uu-no-34-tahun-2004.
21 Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.
22 Cinrapole and Mangarengi, "DILEMA YURIDIKSI DI RUANG SIBER."
23 Indonesia Governance, "Law No 1 of 2024."
24 Scott Shackelford, "Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace," Managing Cyber Attacks in International Law, Business, and Relations in Search of Cyber Peace, January 1, 2012, 1–393, https://doi.org/10.1017/CBO9781139021838.
25 Martin C. Libicki, Cyberdeterrence and Cyberwar (2009), https://www.rand.org/pubs/monographs/MG877.html.
26 Qushayyi, "The Dynamics of Cyber Security Cooperation Between Countries."
27 Haber and Topor, "Sovereignty, Cyberspace, and the Emergence of Internet Bubbles."

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

should be transferred from the National Police (peace/criminal phase) to the Commander of the Indonesian National Armed Forces (conflict/crisis phase) when a cyber attack escalates. This situation places Indonesia in a reactive and passively defensive position, which is contradictory to the needs of modern strategic defense that demands speed of response and total integration of national resources (Sishankamrata).

**b. Asymmetry of Authority in Cyber Crisis Management**

The issue of regulatory disharmony in Indonesia does not stop at overlapping mandates, but stems from a fundamental problem in the design of state institutions, namely asymmetry of authority. In cyber defense governance, there is an axiom that "responsibility must be accompanied by equal authority." However, an analysis of the hierarchy of laws and regulations shows that the BSSN is burdened with significant responsibilities as the national cyber security coordinator through Presidential Regulation No. 28 of 2021 and Presidential Regulation No. 47 of 2023, without being equipped with a sufficiently strong legal basis to mobilize national resources in the event of a crisis.

Referring to Hans Kelsen's theory of the hierarchy of legal norms Stufenbau des Rechts, the binding force of a regulation depends on the validity of higher regulations. In Indonesia, this principle is adopted in Article 7 of Law Number 12 of 2011 concerning the Formation of Legislation. A structural problem arises because BSSN operates based on Presidential Regulations, while the entities it is supposed to coordinate, such as the TNI (Defense), Polri (Law Enforcement), and the Ministry of Communication and Information Technology (Regulation) to operate based on laws. Theoretically and practically, legal products at the level of a Presidential Regulation do not have coercive operational power over institutions established by law[28]. As a result, the coordination function mandated to the BSSN is often degraded to a mere administrative-advisory function, which is ineffective in critical situations that require absolute command compliance.

The most dangerous implication of this asymmetry of authority is the absence of clear legal protocols for states of transition. The cyber crisis management literature written by Tagarev (2010) emphasizes the importance of Crisis Management Procedures (CMP) that are automatically activated when threats exceed certain thresholds. In Indonesia, positive law has not yet regulated the parameters for when civilian control must be handed over to the military[29]. Law No. 23 of 1959 concerning States of Emergency is considered outdated and incompatible with the characteristics of cyber attacks, which are silent and fast[30]. Without a Trigger Mechanism regulated by law (for example, in the form of a Cyber Security Law), policymakers will always experience legal uncertainty: "Is a ransomware attack on

28 Jimly Asshiddiqie, Perihal Undang-Undang (Rajawali Press, 2020), https://simpus.mkri.id/opac/detail-opac?id=10382.

29 Tador Tagarev, "The Art of Shaping Defense Policy: Scope, Components, Relationships (but No Algorithms)," Connections The Quarterly Journal, n.d., accessed January 2, 2026, https://www.researchgate.net/publication/267374585_The_Art_of_Shaping_Defense_Policy_Scope_Components_Relationships_but_no_Algorithms.

30 Indonesia Governance, "Government Regulation in Lieu of Law No 23 of 1959," Penetapan Keadaan Bahaya, accessed January 2, 2026, http://peraturan.bpk.go.id/Details/53973/perpu-no-23-tahun-1959.

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

the National Data Center (PDN) sufficient to activate the national defense protocol?" This uncertainty creates decision-making paralysis, where the golden time for mitigation is wasted on cross-sectoral coordination meetings.

In modern military strategy doctrine, response speed is determined by the Observe-Orient-Decide-Act (OODA Loop) cycle. Research by Catota et al. (2019) shows that a fragmented command structure drastically slows down the Decide phase[31]. In the case of Indonesia, when a hybrid cyber attack occurs, the flow of intelligence information is divided between BSSN (Civil Signal Intelligence), BIN (State Intelligence), and BAIS TNI (Military Intelligence). The absence of a single authority with the right to consolidate all intelligence data (Single Source of Truth) results in a partial response from the state. The National Police may respond by blocking websites (Act), while the TNI has not yet received a presidential order because the threat data has not been centrally verified. This lack of synchronization in the OODA Loop cycle is a fatal flaw that is exploited by the enemy in asymmetric warfare.

Based on the above analysis, maintaining the status quo where the leading cyber sector is only backed by a Presidential Regulation is a strategic flaw. The argument put forward by Chen (2020) regarding Digital Governance emphasizes that in order to deal with existential threats, cyber authorities must have the highest political and legal legitimacy[32]. Therefore, the need to elevate the legal basis of cyber governance from the level of a Presidential Regulation to the level of a Law is not merely an administrative issue, but an absolute prerequisite for the formation of a responsive universal defense system. Without a law that explicitly grants command authority to a single entity during a crisis, Indonesia will continue to be trapped in the bureaucratic coordination trap.

### c. Comparison of Authority Models

To find a solution to the problem of fragmented authority in Indonesia, this study compares cyber governance in developed countries that have successfully overcome similar issues. This comparison is important to show that the success of cyber defense does not only depend on advanced technology, but also on clarity regarding "who is in charge" when a crisis occurs. Singapore provides the best example of how a small country can strengthen its cyber defense through centralization of power. The Singaporean government realizes that cyber threats cannot be handled through voluntary coordination between agencies. Therefore, they passed the Cybersecurity Act 2018.

This law grants the Cyber Security Agency (CSA) considerable authority. Unlike Indonesia's BSSN, which only plays a coordinating role, Singapore's CSA has a legal mandate to inspect computer systems belonging to both the public and private sectors, as well as to order emergency measures in the event of a threat. There is no debate over whether the police or military should take action, as the law has designated the CSA as the main authority

31 Frankie E Catota et al., "Cybersecurity Education in a Developing Nation: The Ecuadorian Environment," Journal of Cybersecurity 5, no. 1 (2019), https://doi.org/10.1093/cybsec/tyz001.

32 Yu-che Chen, "Managing Digital Governance: Issues, Challenges, and Solutions," Routledge & CRC Press, accessed January 2, 2026, https://www.routledge.com/Managing-Digital-Governance-Issues-Challenges-and-Solutions/Chen/p/book/9781439890912.

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

under the Prime Minister. The United States implements a slightly different but still integrated model. They strictly separate civil and military roles but have strict cooperation protocols. The civilian sector is led by CISA (Cybersecurity and Infrastructure Security Agency) under the Department of Homeland Security, while the military sector is led by US Cyber Command (USCYBERCOM). An important lesson for Indonesia is the existence of a clear "handover" mechanism for authority. Research findings from Liff (2012) explain that the US has a Defend Forward doctrine[33]. When cyber attacks on civilian infrastructure (e.g., power grids) are deemed a threat to national security, operational command can be transferred to the military to take active measures to stop the attack at its source. In Indonesia, this transfer mechanism has not been regulated, leading to confusion about who should take action when cyber attacks become a threat to sovereignty.

**d. Legal Reconstruction and Integrated System**

Based on the analysis of regulatory disharmony and the international comparative study above, this research formulates a legal reconstruction design that aims to end the overlapping of authority between BSSN, TNI, and Polri. The prescriptive solution offered does not recommend the dissolution of existing institutions, but rather focuses on the creation of a new governance system through the institutionalization of a Unified Command System. A fundamental step in this reconstruction is the elevation of the legal basis for cyber governance from the level of Presidential Regulation to Law. Indonesia urges the enactment of a Cyber Security and Defense Law that functions as lex specialis to resolve the asymmetry of authority. This regulation must explicitly demarcate the division of operational jurisdiction: BSSN and Polri have full control in peacetime for civil order and handling cyber crimes, while the TNI has full command when a situation is declared a Cyber Emergency or war. Without this elevation in legal status, BSSN's command function will continue to be ineffective due to its weak bargaining position in the legislative hierarchy..

Furthermore, this new legal framework must establish clear parameters or thresholds regarding the transfer of operational control. Adopting international standards such as the Tallinn Manual 2.0, the law needs to formulate articles that regulate automatic escalation mechanisms. For example, if a cyber attack has crippled vital state functions, such as shutting down the national power grid or paralyzing government data centers, then the legal status automatically shifts to National Defense Operations. The clarity of this rule provides a legal basis for the TNI to carry out defensive and offensive operations without having to wait for time-consuming bureaucratic deliberations, so that the state's response can match the speed of the enemy's attack.

Another crucial aspect of this reconstruction is the integration of the Universal People's Security Defense System (Sishankamrata) doctrine into the digital realm. Given that technical expertise is often controlled by civilian entities (academics or white hat hacker

33 Adam P. Liff, "Journal of Strategic Studies: 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War,'" Adam P. Liff, Ph.D., May 21, 2012, https://adampliff.com/2012/05/21/publication-cyberwar-a-new-absolute-weapon-the-proliferation-of-cyberwarfare-capabilities-and-interstate-war/.

Volume 12, Number 01, January-March 2026, Pages 105-116
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

communities), the state needs to accommodate this potential through the establishment of a legal Cyber Reserve Component. Legal reconstruction must provide immunity or legal protection for civilian talent mobilized under military command to carry out active defense actions, including counterattacks, which under normal circumstances could be criminalized under the ITE Law. This is in line Cinrapole (2025) finding that without such a legal umbrella, the mobilization of national cyber resources will be hampered. Overall, this reconstruction aims to transform Indonesia's cyber governance from a voluntary coordination system to a legally binding mandatory command system, ensuring a responsive defense system free from regulatory ambiguity[34].

## D. Conclusion and Recommendations

This study concludes that the main vulnerability in Indonesia's strategic cyber defense is not caused by technological limitations, but rather by regulatory disharmony that creates fragmentation of authority between the civilian and military spheres. The sectoral approach that separates the mandates of the TNI, Polri, and BSSN without an integrative legal umbrella has resulted in an asymmetry of authority, where command and control functions have become ineffective due to the lower legal hierarchy of the coordinating agency like BSSN compared to operational institutions like TNI/Polri. The absence of legal escalation protocols in the "gray zone" has caused the state to experience decision-making paralysis when facing hybrid cyber attacks, resulting in a national defense posture that tends to be reactive and vulnerable to threats that erode sovereignty.

To overcome these structural failures, this study recommends legal reconstruction through the establishment of a Cyber Security and Defense Law as lex specialis that functions as a national legal umbrella. This regulation must explicitly institutionalize a Unified Command System that provides a single authority mandate to mobilize all cross-sectoral national resources when a crisis occurs. Furthermore, the law must establish legal parameters or quantitative thresholds that trigger an automatic transfer of operational control from civil law enforcement to military defense operations, in order to ensure legal certainty, integration of the National Defense and Security System, and the speed of the state's response.

34 Cinrapole and Mangarengi, "DILEMA YURIDIKSI DI RUANG SIBER."

Volume 12, Number 01, January-March 2026, Pages 105-116
**e-ISSN:2614-1485**
**p-ISSN:2716-0440**
**Doi: https://doi.org/10.33751/palar.v12i1**
**Sinta 3; decree No. 0173/C3/DT.0500/2025**

## References

### A. Legislation

Indonesia Governance. *Government Regulation in Lieu of Law No. 23 of 1959 on the Declaration of a State of Danger.* Accessed January 2, 2026. http://peraturan.bpk.go.id/Details/53973/perpu-no-23-tahun-1959.

Indonesia Governance. *Law No. 1 of 2024.* Accessed January 2, 2026. https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024.

Indonesia Governance. *Law No. 2 of 2002.* Accessed January 2, 2026. http://peraturan.bpk.go.id/Details/44418/uu-no-2-tahun-2002.

Indonesia Governance. *Law No. 3 of 2002.* Accessed January 2, 2026. http://peraturan.bpk.go.id/Details/44421/uu-no-3-tahun-2002.

Indonesia Governance. *Law No. 34 of 2004.* Accessed January 2, 2026. http://peraturan.bpk.go.id/Details/40774/uu-no-34-tahun-2004.

Indonesia Governance. *Presidential Regulation No. 28 of 2021.* Accessed January 2, 2026. http://peraturan.bpk.go.id/Details/165493/perpres-no-28-tahun-2021.

Indonesia Governance. *Presidential Regulation No. 66 of 2019.* Accessed January 2, 2026. http://peraturan.bpk.go.id/Details/123703/perpres-no-66-tahun-2019.

### B. Books

Asshiddiqie, Jimly. *Perihal Undang-Undang.* Jakarta: Rajawali Press, 2020.

Chen, Yu-che. *Managing Digital Governance: Issues, Challenges, and Solutions.* New York: Routledge, n.d. Accessed January 2, 2026. https://www.routledge.com/Managing-Digital-Governance-Issues-Challenges-and-Solutions/Chen/p/book/9781439890912.

Hollis, Duncan B., ed. *The Oxford Guide to Treaties.* 2nd ed. Oxford: Oxford University Press, 2020.

Klimburg, Alexander. *National Cyber Security Framework Manual.* 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009. https://www.rand.org/pubs/monographs/MG877.html.

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524.

Shackelford, Scott. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace.* Cambridge: Cambridge University Press, 2012. https://doi.org/10.1017/CBO9781139021838.

Volume 12, Number 01, January-March 2026, Pages 105-116
**e-ISSN:2614-1485**
**p-ISSN:2716-0440**
**Doi: https://doi.org/10.33751/palar.v12i1**
**Sinta 3; decree No. 0173/C3/DT.0500/2025**

## C. Journal Articles

Aini, Nurul, and Fauziah Lubis. "Tantangan Pembuktian dalam Kasus Kejahatan Siber." *Judge: Jurnal Hukum* 5, no. 2 (2024): 55–63.

Catota, Frankie E., M. Granger Morgan, and Douglas C. Sicker. "Cybersecurity Education in a Developing Nation: The Ecuadorian Environment." *Journal of Cybersecurity* 5, no. 1 (2019). https://doi.org/10.1093/cybsec/tyz001.

Cinrapole, Andi, and Arianty Mangarengi. "Dilema Yuridiksi di Ruang Siber: Tantangan dan Strategi Penegakan Keamanan Lintas Negara." *Judicatum: Jurnal Dimensi Cakra Hukum* 3 (2025): 221–35. https://doi.org/10.35326/judicatum.v3i1.7734.

Haber, Eldar, and Lev Topor. "Sovereignty, Cyberspace, and the Emergence of Internet Bubbles." *Journal of Advanced Military Studies* 14 (2023). https://doi.org/10.21140/mcuj.20231401006.

Qushayyi, Muhammad Faiq. "The Dynamics of Cyber Security Cooperation Between Countries: A Case Study of Indonesia and the Netherlands." *Journal of Peace, Security and Democracy* 1, no. 1 (2025): 37–56. https://doi.org/10.63280/jpsd.v1i1.42626.

Reich, Pauline C., Stuart Weinstein, Charles Wild, and Allan S. Cabanlong. "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents—and the Dilemma of Anonymity." *European Journal of Law and Technology* 1, no. 2 (2010).

Roedy, and Asep Adang Supriyadi. "Integrasi Kebijakan Pertahanan dan Kebijakan Publik dalam Penanggulangan Ancaman Perang Hibrida: Pendekatan Analisis Keamanan Nasional." *Inovasi Pembangunan: Jurnal Kelitbangan* 13, no. 1 (2025). https://doi.org/10.35450/jip.v13i1.992.

Sawlani, Dhiraj Kelly, and Asep Adang Supriyadi. "Bridging Public Policy and Defense Strategy to Combat Hybrid Warfare: An Analytical Study on National Security." *Jurnal Praksis dan Dedikasi Sosial* 7, no. 2 (2024): 292–307.

Silver, Daniel. "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter." *International Law Studies* 76, no. 1 (2002).

## D. Book Chapters and Other Sources

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." 2012. https://adampliff.com/2012/05/21/publication-cyberwar-a-new-absolute-weapon-the-proliferation-of-cyberwarfare-capabilities-and-interstate-war/.

Tagarev, Tador. "The Art of Shaping Defense Policy: Scope, Components, Relationships (but No Algorithms)." *Connections: The Quarterly Journal*, n.d. Accessed January 2, 2026. https://www.researchgate.net/publication/267374585.

Tams, Christian. "Article 2(4)." In *The Charter of the United Nations: A Commentary*, edited by Bruno Simma et al. Oxford: Oxford University Press, 2024. https://doi.org/10.1093/law/9780192864536.003.0010.