Available at https://journalenrichment.com/index.php/jr/

Enrichment: Journal of Multidisciplinary Research and Development

Defending the Nation in the Cyber Era: Indonesia's Response to Non-Military Security Threats

Arief Prayitno, Rudiyanto
Universitas Pertahanan RI, Indonesia
Email: rudiyanto@idu.ac.id, ariefprayitno@idu.ac.id

ABSTRACT

The rapid development of information and communication technology has brought Indonesia into a complex era of digital transformation. On the other hand, this advancement has also given rise to new challenges in the form of non-military cyber threats that pose significant risks to national stability. This research aims to examine the forms and characteristics of non-military threats in cyberspace and to analyze the effectiveness of Indonesia's national defense strategies in responding to these threats. The research employs a descriptive qualitative method with a literature study approach. The findings indicate that although the government has established the *Badan Siber dan Sandi Negara* (BSSN) and issued various regulations, such as Law No. 27 of 2022 on Personal Data Protection and Minister of Defense Regulation No. 82 of 2014, the strategies implemented have not been fully effective. This is due to weak interagency coordination, limited human resources, and suboptimal law enforcement. Therefore, strengthening governance, improving digital literacy, and fostering cross-sector collaboration are essential to building a resilient national cyber defense system.

Keywords: Non-Military Threats; BSSN; National Defense.

INTRODUCTION

The rapid expansion of digital infrastructure in Indonesia has brought numerous socio-economic benefits while simultaneously exposing the nation to an unprecedented wave of cyber threats. Between 2019 and 2023, Indonesia recorded at least 79 data breach incidents, many of which targeted governmental bodies and national digital infrastructure. The increasing frequency and sophistication of such threats mark a critical shift in national security paradigms, where non-military challenges have become as consequential as traditional military aggression (Mustikasari et al., 2025).

The rise of cyber warfare has become a pressing threat to national defense systems. This risk has been exemplified by high-profile cyber intrusions targeting government digital infrastructure (Rai et al., 2022; Ullah et al., 2024). A striking example occurred during Indonesia's 2018 simultaneous regional elections (*Pilkada*), when the General Elections Commission (KPU) site came under sustained cyber assault, forcing its temporary shutdown to prevent public confusion. Another breach occurred in 2018, involving the Directorate General of Taxes site (*pajak.go.id*), attributed to a group calling itself 'Anonymous Arabe,' underscoring the disruptive potential of non-state cyber actors. These incidents highlight the urgent need to reframe cyber threats as hybrid or strategic threats, beyond traditional non-military categorizations, demanding robust and integrated national defense strategies (Candra et al., 2021; Setiyawan, 2019). Indonesia has responded through institutional initiatives such as ID-SIRTII, led by the Ministry of Communication and Information and coordinated by BSSN. This aims at enhancing incident response, data protection, and multi-stakeholder

cybersecurity alignment (Arianto & Anggraini, 2019; Wulandari et al., 2025). In a significant milestone, President Joko Widodo ordered the formation of the Indonesian Cyber Force on 3 September 2024, elevating cyber defense to a formal military domain as the fourth branch of the armed forces. This signals a strategic shift in national defense posture (Rai et al., 2022; Ullah et al., 2024).

These challenges are collectively known as non-military threats—forms of threats that do not rely on armed force but pose serious dangers to national sovereignty and public order. In the cyber domain, such threats manifest through espionage, disinformation, data breaches, and the disruption of critical infrastructure. Recognizing the magnitude of these challenges, the Indonesian government established the National Cyber and Encryption Agency (BSSN) in 2017 under a Presidential Decree. BSSN functions as the leading authority responsible for orchestrating national cybersecurity strategy, ensuring threat mitigation, and safeguarding digital sovereignty. The establishment of BSSN marked a paradigm shift in national defense, from a military-centric model to a multidimensional security approach that integrates technological, legal, and societal components. As elaborated by Chotimah (2019), BSSN plays a pivotal role not only in cyber governance but also in representing Indonesia's interests in cyber diplomacy forums at both bilateral and multilateral levels (Chotimah, 2019).

Moreover, the agency consolidates national efforts in early detection, response coordination, digital literacy campaigns, and resilience-building initiatives across multiple sectors including government, defense, economy, and public services. Studies show that prior to BSSN, Indonesia's cybersecurity framework lacked coordination, leaving critical gaps in policy implementation and technical defense capabilities (Mulyadi & Rahayu, 2018).

In practice, BSSN collaborates with ministries, state-owned enterprises, and private sector stakeholders to implement the National Cybersecurity Strategy. These efforts are complemented by educational campaigns and capacity-building programs aimed at increasing digital literacy and public awareness about cyber hygiene. Sudarmadi and Runturambi (2019) emphasize that BSSN's strategy involves strengthening inter-agency coordination, enhancing encryption standards, and fostering legal clarity for effective cyber defense governance (Sudarmadi & Runturambi, 2019).

A growing body of literature underscores the critical role of Indonesia's regulatory framework in shaping national cybersecurity resilience. Central among these are the Presidential Regulation on BSSN and the Minister of Defense Regulation (Permenhan) No. 82/2014, which provide legal guidance for safeguarding national critical infrastructure. These instruments reflect a robust governmental commitment to developing a structured and enforceable foundation for cyber defense, particularly in sectors deemed vital to national survival. However, despite their strategic intent, the practical implementation of these regulations has encountered considerable obstacles. Studies reveal that inter-agency coordination remains suboptimal, compounded by disparities in institutional readiness, technological resources, and cybersecurity expertise. Mulyadi and Rahayu (2018) emphasized that prior to the formal establishment of BSSN, the Indonesian cybersecurity landscape was characterized by fragmented authority and a lack of strategic synergy, which severely limited national response effectiveness (Mulyadi & Rahayu, 2018). Moreover, overlapping jurisdictions, unclear interoperability protocols, and absence of a unified threat response architecture have led to inefficient incident mitigation. Aulianisa and Indirwan (2020) argue

that regulatory insufficiencies and slow adaptation to new cyber threat vectors put national digital assets at risk, calling for the codification of lex specialis legislation tailored specifically to cybersecurity and resilience efforts (Indirwan & Aulianisa, 2020).

To overcome these gaps, there is a pressing need for regulatory reform accompanied by institutional capacity-building. This includes allocating higher budgets for cybersecurity infrastructure, investing in specialized training for digital forensics and threat analysis, and establishing a cross-sector coordination mechanism that facilitates agile decision-making and collective incident response. Setiyawan (2019) further recommends that the government urgently define and classify critical national infrastructure in accordance with modern cyber risk assessments, thereby enabling targeted protection and defense prioritization (Setiyawan, 2019).

In the rapidly evolving digital landscape, traditional defense strategies rooted in conventional military strength are no longer sufficient to safeguard national security. The cyberspace domain has emerged as a strategic battleground, where asymmetric, non-military threats can severely compromise sovereignty, public trust, and political stability (Setiyawan, 2019). These threats often stem from state and non-state actors who exploit the anonymity and transnational nature of cyberspace to disrupt a nation's internal order (Rizal & Yani, 2016). From a policy standpoint, the Indonesian government has taken institutional steps and issued regulations to address these challenges. However, factual gaps remain, especially concerning low levels of inter-agency synergy, fragmented cyber literacy, and limited technological autonomy (Sudarmadi & Runturambi, 2019).

On the theoretical front, much of the literature still focuses on cyber threats as isolated technical or legal issues. There remains a lack of systemic, integrative models that position cyber defense within a multidimensional national security framework involving policy coherence, digital diplomacy, and socio-political resilience (Buana, 2024). This study addresses that gap by analyzing cyber threats as asymmetrical national security risks and positioning cyber defense as a core function of national resilience rather than merely a technological mandate. Hence, this research seeks to explore the typologies and operational characteristics of non-military threats in Indonesia's cyber domain, evaluate the strategic policies implemented by the state, and assess their effectiveness in maintaining digital sovereignty. By doing so, it aims to contribute both strategic insight and critical reflection on the readiness of Indonesia's defense ecosystem to navigate the uncertainty of the cyber era.

METHOD

This research adopted a qualitative descriptive methodology employing a library research approach. This method was particularly suited for examining complex, dynamic, and multidimensional phenomena. Qualitative methods allowed researchers to capture rich contextual understanding, trace discursive developments, and identify patterns across institutional, regulatory, and strategic dimensions. Library research in this context involved a systematic review of both primary and secondary sources, including official government regulations (e.g., Presidential Decrees, Permenhan No. 82/2014), strategic reports from agencies such as the National Cyber and Crypto Agency (BSSN) and the Ministry of Defense, as well as peer-reviewed journal articles, scholarly books, white papers, and credible digital

resources. This approach aligned with the principles of desk-based document analysis, a well-established technique in policy and security studies.

Data collection and analysis were carried out through thematic content analysis, emphasizing context-sensitive interpretation, classification of recurring motifs, and critical examination of conceptual frameworks. Key themes were extracted based on their relevance to cybersecurity governance, national resilience mechanisms, and the evolving nature of asymmetric, non-military threats. The process was iterative, allowing for conceptual triangulation and validation of interpretations through cross-source comparison.

By using this approach, the study aimed to produce a comprehensive and critical account of (1) the typology and dynamics of cyber-based non-military threats in Indonesia, and (2) the strategic, institutional, and regulatory responses developed to defend national sovereignty in the digital era. The qualitative orientation ensured depth over breadth, which was crucial in understanding the intersection of security policy, cyber law, and strategic defense discourse.

RESULTS AND DISCUSSION

Digital Expansion, Strategic Exposure: Cybersecurity Governance in Indonesia's National Defense Framework

Recent data reveals a dramatic surge in cybersecurity threats targeting Indonesia. In 2023 alone, the nation recorded over 1.2 billion cyber incidents, while in the first quarter of 2024, reported cyberattacks approached 6 million cases, indicating a significant upward trajectory. This escalation closely correlates with the rapid expansion of Indonesia's digital footprint, particularly the growth in internet users, which has now surpassed 221 million individuals, placing Indonesia among the world's top five internet markets (Mamduh, 2024).

The proliferation of digital connectivity, while enhancing access to public services and e-commerce, also exponentially increases the attack surface available to malicious actors. As highlighted in regional threat assessments, cyberattacks in Southeast Asia have become more sophisticated, targeted, and frequent, often exploiting systemic vulnerabilities in public and critical infrastructure (Mustikasari et al., 2025).

This duality, between digital opportunity and cyber exposure, underscores the necessity for a proactive, state-level cybersecurity response.The Indonesian experience reflects a broader global pattern, where the expansion of digital ecosystems outpaces the institutional capacity to secure them. In the absence of robust national strategies, coordinated threat intelligence, and public cyber awareness, the country risks not only economic and data loss but also an erosion of digital trust and sovereignty (Mahendra & Pinatih, 2020). These findings align with trends discussed where the rise in cyber risk is framed as a consequence of uneven digital maturity and weak governance in cybersecurity policy (Al-Daraiseh, 2023). As such, the observed growth in cyber incidents should not be dismissed as mere statistical anomalies. Rather, they signal critical vulnerabilities in Indonesia's national defense posture, requiring immediate investment in cyber resilience, public-private partnerships, and institutional reform.

As outlined in the Indonesian Ministry of Defense Regulation No. 82 of 2014 on Cyber Defense Guidelines, the spectrum of cyber threats addressed by national defense policy includes a diverse array of malicious activities, each posing unique risks to digital infrastructure and national security. The regulation categorizes the following types of cyber threats:

a) Advanced Persistent Threats (APTs), Denial of Service (DoS), and Distributed Denial of Service (DDoS) Attacks. These attacks are typically carried out by overwhelming system capacity with illegitimate traffic or access requests, thereby denying legitimate users access to targeted systems or services. APTs, in particular, involve long-term, stealthy intrusions that aim to exfiltrate sensitive data or disrupt strategic operations over extended periods.
b) Website Defacement Attacks. These involve unauthorized modification or replacement of a website's content to display messages or visuals aligned with the attacker's intent. Such attacks not only compromise technical security but also pose reputational risks to public and institutional entities.
c) Phishing Attacks. Phishing is executed by creating deceptive websites that mimic legitimate ones, with the intent of capturing sensitive user information such as usernames, passwords, and financial credentials. It remains a primary vector for identity theft and credential compromise.
d) Malware Infections. Malicious software, or malware, refers to harmful code or programs designed to disrupt normal computer operations, steal data, or gain unauthorized access to systems. This category includes viruses, worms, ransomware, trojans, and spyware.
e) Cyber Intrusions via Credential Exploitation. These attacks occur through unauthorized system access by exploiting vulnerabilities or stealing valid credentials such as usernames and passwords. The goal is to infiltrate networks covertly and often serves as a precursor to more damaging actions.
f) Spam (Unsolicited Bulk Emails). Spam involves the mass distribution of unsolicited email messages, which can clutter communication channels, spread malware, or serve as vectors for phishing attacks.
g) Protocol Abuse. Attackers may exploit weaknesses in communication protocols (e.g., TCP/IP, DNS, HTTP) to disrupt data transmission, hijack sessions, or perform reconnaissance. This form of abuse can compromise system reliability and expose sensitive information. Indonesia continues to experience a substantial rise in diverse forms of cyber threats, reflecting both the country's growing digital dependency and underlying cybersecurity vulnerabilities. Among the most prevalent threat vectors are:

a) Malware and Ransomware

Indonesia ranks among the top ten countries globally in terms of ransomware infections, with a marked escalation observed since 2017 (Mulyadi & Rahayu, 2018). These attacks target both individuals and institutions, often resulting in data breaches, operational paralysis, and significant financial losses. The payloads range from basic trojans to sophisticated ransomware variants that encrypt entire networks and demand cryptocurrency-based ransom payments.

b) Phishing and Social Engineering Attacks

Phishing continues to pose a significant and pervasive threat in Indonesia, largely driven by low public and employee awareness of cybersecurity risks. A systematic literature review on public awareness of phishing highlights that inadequate educational measures have facilitated the success of social engineering attacks, underscoring the need for broad-based, sustained awareness campaigns (Candra et al., 2021).

c) Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

> DoS and DDoS attacks are increasingly deployed to disrupt digital services in both the public and private sectors. These attacks operate by flooding targeted systems with excessive traffic, causing temporary or prolonged outages. In the Indonesian context, such disruptions have affected government portals, e-commerce platforms, and financial services, revealing critical weaknesses in infrastructure resilience (Hapsari & Pambayun, 2023).

These threat categories collectively underscore the systemic fragility of Indonesia's cyber ecosystem and the urgency for integrated, multilevel cyber defense frameworks. As studies have shown in comparable contexts, such vulnerabilities are exacerbated by low investments in security infrastructure, insufficient workforce capacity, and a lack of coordinated national response mechanisms.

One of the most alarming indicators of cybersecurity fragility in Indonesia is the massive data breach involving sensitive government and intelligence records, as seen in the widely publicized case involving the anonymous figure "Bjorka." This incident not only exposed vulnerabilities within critical digital infrastructure, but also shook public confidence in state institutions. The breach created widespread social alarm, destabilized perceptions of state legitimacy, and attracted global scrutiny regarding Indonesia's cyber readiness.

According to Sukmawan & Setyawan (2023), breaches of this nature go beyond mere administrative disruptions. They should be classified as multidimensional threats which posing risks to national defense, public safety, human security, and state sovereignty. What renders these threats particularly complex is the involvement of non-state actors, such as hacktivists and transnational cyber syndicates, who systematically exploit systemic vulnerabilities for ideological, economic, or geopolitical objectives.

Recent research in cybersecurity studies supports this classification. For instance, Al-Daraiseh (2023) argues that cyberattacks are no longer isolated technical incidents, but rather part of hybrid warfare tactics that target the informational legitimacy of governments. These incidents create a domino effect, leading to institutional distrust, political destabilization, and weakened digital sovereignty, especially in countries with limited regulatory enforcement and low cyber literacy.

In response, scholars emphasize the need for governments to adopt a preventive and adaptive cybersecurity posture. This includes investing in proactive threat intelligence, enhancing cross-sectoral cyber governance, and cultivating public cyber hygiene through national education programs (Mahendra & Pinatih, 2020). Merely reactive approache (such as patching systems after a breach) are insufficient in the face of coordinated, transboundary cyber aggression. Thus, the Indonesian case exemplifies the global imperative: states must treat cybersecurity not as an IT issue, but as a core pillar of national resilience, embedded in security doctrine, legal frameworks, and strategic culture.

Cyber threats differ fundamentally from conventional security threats due to their transnational, anonymous, and stealthy nature. Unlike traditional military threats, cyberattacks often cross national jurisdictions and are conducted by actors, either state-sponsored or independen, who are difficult to trace or hold accountable. Attackers can operate remotely, conceal their identities, and exploit global digital infrastructures without breaching physical borders (Taddeo, 2018).

One defining characteristic is the invisible onset of attacks. Cyber intrusions can remain undetected for extended periods, with organizations often realizing the breach only after significant damage has occurred. These attacks may involve data theft, infrastructure manipulation, or espionage, and are often executed silently and progressively. Compounding the challenge, threat actors no longer need sophisticated capabilities; widely available hacking tools and malware kits allow individuals with moderate or even basic technical skills to launch impactful cyberattacks (Zhang et al., 2022).

Moreover, cyberattacks frequently utilize advanced technologies such as malware, ransomware, Advanced Persistent Threats (APTs), and the increasingly dangerous Highly Evasive Adaptive Threats (HEAT) (Rahakbauw, 2024). These require high-level detection capabilities and rapid-response mechanisms to prevent cascading failures across interconnected systems. APTs in particular are known for their stealth and persistence, aiming to maintain long-term unauthorized access to critical infrastructures. The targets of cyber threats are also evolving, ranging from financial institutions, public service platforms, and transportation systems to military communication and energy grids. These infrastructures are vital to national functionality, and their disruption can paralyze state operations without a single shot being fired. As such, cybersecurity has become a fundamental pillar of modern national defense strategies.

For Indonesia, this means cybersecurity must be treated as a multi-dimensional and cross-sectoral priority, involving not just technological enhancement but also institutional regulation, public education, and international cooperation. The establishment of the National Cyber and Crypto Agency (BSSN) marks a significant institutional response, but further steps are required to strengthen legal frameworks, foster interagency synergy, and improve digital literacy at all levels of society. An integrated approach which covering legal, technical, educational, and diplomatic dimensions, is essential to ensuring resilient and adaptive national cybersecurity in the face of rapidly evolving threats.

Government Strategy in Facing the Non-Military Threat

In response to the escalating spectrum of cyber threats, the Government of Indonesia has adopted a multi-faceted defense strategy grounded in Minister of Defense Regulation No. 82 of 2014. Drawing on the tripartite classification developed by McDonnell and Sayers, threats are categorized into hardware, software, and data/information domains. Hardware threats involve the introduction of physical components capable of compromising or damaging systems; software threats encompass malicious code or applications designed to disrupt operations or exfiltrate data; and data/information threats pertain to the unauthorized access, manipulation, or dissemination of information for political, economic, or ideological purposes. This classification enables a targeted response strategy, aligning institutional capabilities with specific threat vectors and integrating them into broader national security planning.

To synchronize national responses, the National Cyber and Crypto Agency (BSSN) serves as the central authority for cyber governance. BSSN's operational scope spans:

1) Policy formulation for cyber defense and data protection.
2) Interagency coordination across ministries, law enforcement, and critical infrastructure operators.

3) International engagement, including ASEAN Cybersecurity Cooperation programs and bilateral partnerships with Japan, Australia, and Singapore (ASEAN Secretariat, 2024).

Recent literature emphasizes that BSSN's role is expanding from reactive crisis management to proactive threat hunting, with integrated threat intelligence platforms being piloted in collaboration with telcos and fintech companies (Putra et al., 2025).

In addition to institutional development, Artificial Intelligence (AI) has become a strategic tool in enhancing Indonesia's cyber defense. AI enables early detection and rapid response by analyzing massive data flows in real-time, identifying attack patterns, and recommending proactive mitigation steps based on predictive modeling. The integration of AI supports the creation of adaptive, intelligent, and resilient digital defense systems capable of evolving alongside emerging threats (Siti Maesaroh, 2025). Academic studies, have emphasized the crucial role of automated threat intelligence and AI-driven defense mechanisms in strengthening national resilience (Shaw et al., 2022). Moreover, Mustikasari et al. (2025) argue that technological advancement alone is insufficient. Building cross-sectoral collaboration between public and private stakeholders, along with synchronized regulatory efforts, is essential for a responsive and robust cybersecurity ecosystem.

Ministerial Regulation No. 82/2014 also outlines three main countermeasures to cyber threats:

a) Cyber defense: A preventive and responsive mechanism focused on safeguarding critical functions in government, finance, and energy through real-time surveillance and structured data recovery efforts.
b) Legal action: Cybercrimes are prosecuted under Indonesia's legal frameworks anchored in the Electronic Information and Transactions Law (ITE) and Personal Data Protection Law (PDP). This action requiring coordinated investigation among BSSN, the National Police's Cyber Directorate, the Ministry of Communications and Information Technology (Kominfo), and the Attorney General's Office. However, challenges persist, including limited digital forensic capacity and evidence admissibility in court. Scholars note that aligning Indonesia's cybercrime prosecution standards with the Budapest Convention on Cybercrime could improve admissibility and cross-border cooperation.
c) Cyber counter-attack: Although theoretically considered, this offensive approach raises ethical and legal dilemmas under international humanitarian law and digital sovereignty principles. While not formally adopted in Indonesian policy, cyber deterrence is gaining attention in defense discourse, particularly within military cyber units under the Ministry of Defense and TNI. This acton faced with several risks include attribution uncertainty, potential diplomatic escalation, and violations of international humanitarian law.

Cyber defense has emerged as a cornerstone of Indonesia's national security strategy in cyberspace, serving as both a preventive and responsive mechanism. It is particularly critical in ensuring the continuity of essential government functions and protecting strategic sectors such as public administration, energy, and finance. The National Cyber and Crypto Agency (BSSN) plays a central role by operating real-time monitoring systems, coordinating incident responses, and facilitating structured recovery protocols after cyberattacks.

Beyond technical defense, the government integrates legal enforcement to address cyber threats that escalate into criminal activities. Cybercrime handling requires effective inter-agency coordination among BSSN, the Ministry of Communication and Informatics

(Kominfo), the Indonesian National Police's Cybercrime Directorate, and the Attorney General's Office. Although Indonesia has enacted key regulatory frameworks such as the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law), law enforcement efforts often face obstacles such as insufficient digital evidence and a lack of forensic capabilities (Anjelina, 2023).

The more controversial strategy, cyber counter-attacks, remains a debated concept in Indonesia's defense discourse. While discussions are growing within military circles and the Ministry of Defense regarding the establishment of cyber command units, no formal policy has endorsed offensive cyber operations. Legal and ethical considerations under international humanitarian law and digital sovereignty norms have made the government cautious. The attribution problem (the difficulty of accurately identifying perpetrators in cyberspace) further complicates retaliation strategies and raises risks of diplomatic conflict. Nevertheless, cyber deterrence remains an important element of Indonesia's cyber diplomacy posture, emphasizing resilience over aggression.

Among the triad of responses (cyber defense, legal action, and counter-attack) Indonesia clearly leans toward defensive and legal approaches, reflecting a constitutional and civilian-centric doctrine. This strategic orientation prioritizes citizen protection and infrastructure continuity, while aligning with global cyber norms and preserving international relations. However, significant implementation challenges persist, including fragmented institutional coordination, limited skilled human capital, and lack of interoperability across platforms and agencies (Setiawan et al., 2024). Addressing these gaps is essential for operationalizing a robust and integrated national cybersecurity architecture.

Assessing the Strategic Effectiveness of National Defense Policies Against Non-Military Threats

Evaluating the effectiveness of cybersecurity strategies which particularlu in the context of national defense against non-military threats, requires comprehensive anallysis of the regulatory frameworks that govern such initiatives. Legal and institutional frameworks serve as the normative foundation for the delegation of authority, coordination mechanisms, and inter-agency accountability in responding to the dynamic and complex nature of cyber threats (Carr, 2016). For Indonesian context, the Presidential Regulatory No. 53, 2017 and Peraturan Menteri Pertahanan No. 82 Tahun 2014 play a foundational role in shaping the operational scope of the national cybersecurity posture. In response to increasing the vulnerabilities, the Indonesian government established the National Cyber and Crypto Agency (BSSN). BSSN function as the principal body tasked with the orchestration on national cyber defense initiatives. The agency's strategy pillars encompass (Haryanto et al., 2023):

Regulatory and Strategic Development

BSSN is responsible for drafting and updating the National Cybersecurity Strategy, aligning with evolving threats and technological advancements. This include enhancing legal instruments, defining standard operational protocols, and strandardizing cybersecurity responsibilites across ministries and institutions.

Capability Building

As emphisizes by Dunn Cavelty (2014), a resilient cyber defense depends not only on infrastructure but also on societal preparadness. In this context, BSSN leads cyber awareness

campaigns, promotes academic and professional training programs, and facilitates cybersecurity sertification. These initiatives aim to bridge the human capital gap and foster a culture of digital resilience (Dunn Cavelty, 2014).

International and Cross-Sector Cooperation

Recognizing the transnational nature of cyber threats, BSSN engages in bilateral and multilateral partnerships, sharing threat intelligence, and participating in regional cybersecurity frameworks. This mirrors global trends in cyber diplomacy and collective security efforts.

Indonesia enactment of Law No. 72/2022 on Personal Data Protection (PDP Law) represents a significant milestone in the nation's journey toward establishing a robust digital governance ecosystem. Prior to this legislation, data protection efforts were fragmented across various sectoral laws such as the Electronic Information and Transactions Law (UU ITE), the Populations administration Law (UU Dikducapil), and the Health Law (UU Kesehatan). This patchwork approach led to overlapping regulations and legal vacuums, undermining the coherence of Indonesia's data governance framework. The PDP Law aims to harmonize these disparate legal instruments, offering a unified regulatory architecture for personal data protection. Its passage aligns with global trends in privacy legislation, such as the European Union's General Data Protection Regulation (GDPR), and reflects Indonesia's ambition to foster digital trust, streghten user rights, and enhance accountability among digital service providers (Budiman, 2023). In theory, the law should catalyze improved cybersecurity practices and bolster public confidence in digital platforms.

However, implementation realities reveal enduring systemic challenges. According to Surfshark's global report, Indonesia ranks 8th globally for the highest number of leaked records, with 94.22 million data breaches reported between 2020 and 2024. This alarming figure underscores several structural vulnerabilities:

a) Low Digital Literacy: A significant portion of the population remains unaware of data privacy risks, making them susceptible to social engineering and phishing attacks. Cybersecurity attitude is a key mediator influencing user's cybersecurity awareness (Al-Misran & Candiwan, 2025).
b) Weak Cybersecurity Infrastructure: Many government and private institutions lack adequate digital safeguards and remain exposed to ransomware, malware, and unauthorized intrusions.
c) Poor Inter-agency Coordination: Regulatory fragmentation persists due to overlapping mandates among supervisory agencies, delaying response times and policy enforcement.
d) Enforcement Gaps: Although legal frameworks are in place, weak digital forensic capabilities and inconsistent penalties have diminished the law's deterrent effect.

To enhance the PDP Law's impact, scholars argue for a multidimensional approach that includes public education campaigns, investment in cyber infrastructure, and clear institutional delineation of enforcement responsibilities (Taddeo, 2019; Zhang et al., 2022). Without addressing these root issues, Indonesia's data protection regime risks becoming performative rather than transformative.

Over the past several years, Indonesia has experienced a sharp rise in cyber threats, underscoring the urgent need to strengthen national cybersecurity capacity. Empirical evidence suggests that government capabilities in cybersecurity governance remain insufficient to

address the growing complexity of attacks (Susanto & Almunawar, 2023; Setiawan et al., 2024). Adversaries are increasingly leveraging advanced tools such as AI-driven malware, highly targeted spear-phishing campaigns, and ransomware-as-a-service models operated through transnational criminal networks (Nurdin et al., 2024). The rapid pace of technological advancement has created a double-edged sword: while enabling efficiency in public service delivery and national information systems, it simultaneously exposes vulnerabilities that can be exploited for destructive purposes. Cyber threats now extend beyond purely technical system intrusions to include socio-psychological dimensions such as disinformation campaigns, digital propaganda, and public opinion manipulation via social media (World Bank, 2023). This development necessitates not only reactive measures but also proactive and sustained approaches to resilience-building.

The National Cyber and Crypto Agency (BSSN) serves as the central institution in safeguarding Indonesia's cyberspace. Beyond system protection, BSSN functions as a policy-maker, incident response coordinator, and cross-sectoral liaison. However, optimizing this role requires comprehensive capacity-building initiatives—ranging from human resource development through specialized training and certification programs to investment in state-of-the-art cybersecurity infrastructure (Nurdin et al., 2024). Strategically, the Indonesian government has taken significant steps, including the establishment of BSSN in 2017, the implementation of technical regulations such as Ministerial Regulation No. 20/2016, and the enactment of the Personal Data Protection Law (Law No. 27/2022). These measures have provided a solid legal and institutional foundation. Additionally, international collaboration, through mechanisms such as the ASEAN Cybersecurity Cooperation Strategy 2024–2030 and bilateral partnerships with Japan, Australia, and Singapore, reflects Indonesia's recognition of cybersecurity as a transboundary challenge (ASEAN Secretariat, 2024).

Nevertheless, persistent incidents such as the KPU voter data breach, the National Data Center (PDN) intrusion, and repeated leaks in the health and public service sectors highlight ongoing vulnerabilities. Weaknesses in inter-agency coordination, particularly between BSSN, the Ministry of Communication and Informatics (Kominfo), the Indonesian Armed Forces (TNI), and the National Police, have slowed incident response times and reduced overall defensive effectiveness (Setiawan et al., 2024). A further challenge lies in uneven technological and human capacity across government institutions, especially at the regional level. Many agencies still lack adequate risk management frameworks and early warning systems. Moreover, despite the enactment of the Personal Data Protection Law, the absence of an independent data protection authority continues to hinder oversight and enforcement (World Bank, 2023).

In light of these structural and operational constraints, Indonesia's cyber defense strategy can be seen as moving in the right direction but still hampered by significant implementation gaps. Achieving full effectiveness will require strengthening governance mechanisms, clarifying institutional mandates, investing in advanced technologies, enhancing workforce skills, and fostering higher public awareness of digital security risks. Thus, the strategy must evolve from a normative and reactive posture toward a systematic, adaptive, and collaborative approach that safeguards national sovereignty and information security in the digital era.

CONCLUSION

Cyber threats pose highly sophisticated and borderless challenges to national security, capable of disrupting critical infrastructure, weakening state sovereignty, and destabilizing socio-political order. Indonesia has made significant progress in cyber resilience through institutional reforms, regulations, capacity-building, Computer Security Incident Response Teams (CSIRT), AI deployment, and improved inter-agency coordination. However, ongoing issues such as insufficient inter-agency synergy, limited skilled personnel, technological gaps, and weak cybercrime enforcement hinder these efforts. Addressing these multifaceted challenges requires comprehensive, adaptive strategies that move beyond reactive defense toward proactive prevention, detection, and neutralization of cyber threats. Future research should focus on developing integrative models of cyber defense that fuse technological, institutional, and cultural dimensions to strengthen Indonesia's national resilience and embed cyber defense as a foundational element of its security doctrine and strategic governance.

REFERENCES

Al-Misran, S. A., & Candiwan, C. (2025). Cybersecurity awareness in Indonesia: Factors, attitude, and practical implications. In 2025 11th International Conference on Communication and Signal Processing (ICCSP) (pp. 1563–1568). https://doi.org/10.1109/ICCSP64183.2025.11088470

Anjelina, D. (2023). Fenomena serangan siber Rusia terhadap Ukraina: Sebagai pembelajaran bagi Indonesia dalam pengembangan pertahanan siber. Jurnal Pertahanan & Bela Negara, 13(3), 231–241. https://doi.org/10.33172/JPBH.V13I3.14307

Arianto, A. R., & Anggraini, G. (2019). Building Indonesia's national cyber defense and security to face the global cyber threats through Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). Jurnal Pertahanan & Bela Negara, 9(1), 17–36. https://doi.org/10.33172/JPBH.V9I1.515

Apri Sudarmadi, D., & Josias Simon Runturambi, A. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) dalam menghadapi ancaman siber di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 2(2), 157–178. https://doi.org/10.7454/jkskn.v2i2.10028

Buana, I. G. P. (2024). Strengthening non-military defense to strengthen the Unitary State of the Republic of Indonesia. Jurnal Kajian Lemhanas RI, 12(2), 163–172. https://doi.org/10.55960/JLRI.V12I2.532

Budiman, R. (2023). The development of personal data protection law in Indonesia: Challenges and prospects for the implementation of Law No. 27 of 2022. Jurnal Smart Hukum (JSH), 2(1), 24–36. https://doi.org/10.55299/JSH.V2I1.1352

Candra, A., Suhardi, S., & Persadha, P. D. (2021). Indonesia facing the threat of cyber warfare: A strategy analysis. Jurnal Pertahanan, 7(3), 441–451. https://doi.org/10.33172/JP.V7I3.1424

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Chotimah, H. C. (2019). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara. Jurnal Politica, 10(2), 113–128. https://doi.org/10.22212/JP.V10I2.1447

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and Engineering Ethics, 20(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

Indirwan, & Aulianisa, S. S. (2020). Critical review of the urgency of strengthening the implementation of cyber security and resilience in Indonesia. Lex Scientia Law Review, 4(1), 33–48. https://doi.org/10.15294/lesrev.v4i1.38197

Mahendra, Y., & Pinatih, N. (2020). Mapping on cyber threats in Indonesia related to Indonesia's cyber security agenda. https://doi.org/10.4108/eai.26-11-2019.2295212

Mulyadi, & Rahayu, D. (2018). Indonesia national cybersecurity review: Before and after establishment National Cyber and Crypto Agency (BSSN). In 2018 6th International Conference on Cyber and IT Service Management (CITSM). https://doi.org/10.1109/CITSM.2018.8674265

Mustikasari, W., & A. D. (2025). Strategi pertahanan non-konvensional Indonesia dalam menangkal ancaman siber asimetris: Studi kasus serangan terhadap infrastruktur kritis. Aurelia: Jurnal (Online). http://www.rayyanjurnal.com/index.php/aurelia/article/view/5285

Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). The role of Indonesia to create security and resilience in cyber spaces. Jurnal Politica, 13(1), 43–66. https://doi.org/10.22212/JP.V13I1.2641

Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. Journal of ASEAN Studies, 4(1), 61–78. https://doi.org/10.21512/JAS.V4I1.967

Setiyawan, A. (2019). The urgency of defining Indonesia's national critical infrastructure. Unifikasi: Jurnal Ilmu Hukum, 6(2), 164–175. https://doi.org/10.25134/unifikasi.v6i2.1673

Siti Maesaroh, R. (2025). Tantangan keamanan siber dan implikasinya terhadap hukum kenegaraan: Tinjauan atas peran negara dalam menjamin ketahanan digital. Staatsrecht, 4(2), 255–274. https://doi.org/10.14421/3N8BXW79

Taddeo, M. (2018). Deterrence and norms to foster stability in cyberspace. Philosophy and Technology, 31(3), 323–329. https://doi.org/10.1007/s13347-018-0328-0

Ullah, F., Zeeshan Naseer, M., & Haq, A. (2024). International responses over nontraditional security threats: A comparative analysis into rational and sources. Global Strategic & Security Studies Review, 9(3), 24–39. https://doi.org/10.31703/GSSSR.2024(IX-III).03

Wulandari, R., Priyanto, P., & Hendra, A. (2025). Indonesia's cyber security strategy in the face of evolving modern warfare threats. Formosa Journal of Applied Sciences, 4(2), 615–626. https://doi.org/10.55927/FJAS.V4I2.5