Jurnal Strategi Kampanye Militer
Volume 11, Nomor 2, 2025 E-ISSN 2830-3261

The Strategic Role of the Indonesian National Armed Forces Cyber Unit in Countering Cyber Threats to Achieve National Security

Peran Strategis Satuan Siber Tentara Nasional Indonesia dalam Menangkal Ancaman Siber untuk Mewujudkan Keamanan Nasional

Tomy Arvianto, Mhd Halkis, Erry Herman,
Fakultas Strategi Pertahanan, Unhan RI

Email: tom.sigsf@gmail.com

Abstrak. *Perkembangan pesat teknologi digital telah mengubah lanskap keamanan global, menjadikan ruang siber sebagai domain baru bagi kompetisi strategis antara aktor negara dan non-negara. Ancaman siber masa kini tidak lagi terbatas pada spionase atau kebocoran data; ia telah berkembang menjadi instrumen kekuasaan geopolitik yang mampu melemahkan kedaulatan, kepercayaan publik, serta ketahanan nasional. Bagi Indonesia, peningkatan eksponensial insiden siber—tercatat lebih dari 330 juta anomali pada tahun 2024 oleh Badan Siber dan Sandi Negara (BSSN)—menegaskan kebutuhan mendesak akan arsitektur pertahanan siber nasional yang terintegrasi. Dalam konteks tersebut, Satuan Siber Tentara Nasional Indonesia (TNI) memegang peran strategis sebagai komponen militer yang bertanggung jawab menjamin kedaulatan dan ketahanan digital bangsa. Tulisan konseptual ini menelaah signifikansi strategis peran Satuan Siber TNI dalam menghadapi ancaman siber guna mewujudkan keamanan nasional. Dengan menggunakan kerangka teori keamanan nasional, teori perang siber strategis, dan model transformasi digital, artikel ini berargumen bahwa konsolidasi kelembagaan, profesionalisasi sumber daya manusia, serta kemandirian teknologi merupakan tiga pilar utama strategi pertahanan siber Indonesia. Penguatan ketiga pilar tersebut melalui kebijakan terpadu dan integrasi antar lembaga akan meningkatkan kapasitas Indonesia untuk mencegah, mendeteksi, dan merespons agresi siber secara efektif.*

Kata kunci: *Pertahanan siber; Keamanan nasional; Tentara Nasional Indonesia (TNI); Ketahanan kelembagaan; Kedaulatan digital*

Abstract. The rapid evolution of digital technology has reshaped the global security landscape, transforming cyberspace into a new domain of strategic competition among state and non-state actors. Cyber threats today are no longer limited to espionage or data breaches; they have become instruments of geopolitical power capable of undermining sovereignty, public trust, and national resilience. For Indonesia, the exponential growth of cyber incidents—recorded at more than 330 million anomalies in 2024 by the National Cyber and Crypto Agency (BSSN)—underscores an urgent need for an integrated national cyber-defense architecture. Within this context, the Indonesian National Armed Forces (TNI) Cyber Unit (Satuan Siber TNI) plays a pivotal role as the military arm responsible for ensuring the nation's digital sovereignty and resilience. This conceptual paper explores the strategic significance of the TNI Cyber Unit in countering cyber threats and achieving national security. Drawing on national-security theory, strategic cyberwar, and digital-transformation models, the paper argues that institutional consolidation, professional human capital, and technological independence are three essential pillars of Indonesia's cyber-defense strategy. Strengthening these pillars through coordinated policy and inter-agency integration will enhance Indonesia's capacity to deter, detect, and respond to cyber aggression effectively.

Keywords: Cyber defense; National security; Indonesian Armed Forces (TNI); Institutional resilience; Digital sovereignty

.

2. Theoretical Framework

A robust theoretical foundation is indispensable for analyzing the strategic role of the Indonesian National Armed Forces Cyber Unit (TNI Cyber Unit) within the broader architecture of national security. This study integrates five interrelated frameworks—National Security Theory, Strategic Cyberwar Theory, Cyber Power, Hybrid Warfare, and the Digital Transformation Organizational Model—to conceptualize how military, governmental, and civilian actors can jointly safeguard Indonesia's digital sovereignty. Together, these perspectives provide a multilevel analytical lens: from the systemic logic of state security to the organizational dynamics of digital defense institutions.

2.1 National Security Theory (Buzan, 1991)

Barry Buzan's *People, States and Fear* (1991) redefined security as a multidimensional concept encompassing political, economic, societal, environmental,

and military sectors. Security, in this view, is not merely the absence of war but the preservation of a community's essential values against existential threats. The *securitization* process—whereby political actors elevate specific issues to the level of national security—allows states to justify extraordinary measures for protection.

Applied to cyberspace, Buzan's theory clarifies that cyber threats constitute existential challenges to the integrity of information, infrastructure, and governance. A successful cyberattack on government networks, banking systems, or energy grids can undermine public trust and political legitimacy as effectively as physical invasion. Hence, cybersecurity is not a technical adjunct but a core component of national security (Buzan, 1991).

For Indonesia, the securitization of cyberspace through Law No. 3 of 2025 formalizes the perception that cyberattacks threaten the nation's sovereignty. This legislative recognition transforms cyberspace into a legitimate defense domain, aligning Indonesia with global practice. In this framework, the TNI Cyber Unit emerges as an actor responsible for implementing the *referent object* of security—protecting the state and its citizens from digital coercion—by combining military authority with technological capability.

2.2 Strategic Cyberwar Theory (Kallberg, 2017)

Jan Kallberg's *Strategic Cyberwar Theory* advances the understanding of cyber conflict beyond tactical disruption to systemic destabilization. He argues that cyberwarfare should be viewed as a strategic instrument capable of degrading a nation's institutional capacity and eroding societal confidence over time rather than producing immediate kinetic effects (Kallberg, 2017). Cyber operations can paralyze decision-making, distort information flows, and trigger economic dysfunction—effects that weaken a state's resilience without firing a single shot.

Kallberg (2018) introduces the concept of *institutional vulnerability*, emphasizing that the effectiveness of cyber defense depends less on technology and more on the coherence and adaptability of national institutions. States with fragmented bureaucracies or weak coordination mechanisms are more likely to suffer strategic defeat in cyberspace. In Indonesia's context, where multiple agencies—BSSN, Kemhan, Polri, and TNI—share overlapping mandates, institutional integration becomes critical.

The theory also underscores *national risk propensity*, the degree to which a country tolerates exposure to digital threats. Building robust cyber institutions such as a centralized Cyber Command and continuous human-resource development can

reduce this risk propensity. Thus, the TNI Cyber Unit should not merely defend networks but shape the strategic environment by strengthening institutional resilience, reducing vulnerability, and enhancing deterrence credibility.

2.3 Cyber Power (Nye, 2010)

Joseph S. Nye Jr. (2010) conceptualizes *cyber power* as the ability to produce preferred outcomes through cyberspace resources. He distinguishes between defensive, offensive, and informational dimensions. Cyber power derives from both *hard* capabilities—technological infrastructure, military assets—and *soft* elements such as norms, trust, and informational influence.

Nye's framework is particularly valuable for middle-power states like Indonesia, where coercive resources are limited but the potential for normative influence remains significant. The notion of *smart power*, a strategic blend of coercion and attraction, suggests that Indonesia can project influence by promoting regional cyber norms, transparency, and capacity building within ASEAN.

From this perspective, the TNI Cyber Unit embodies a dual mandate: (1) to secure Indonesia's digital domain through deterrence-by-denial and deterrence-by-resilience, and (2) to contribute to the nation's soft-power projection by engaging in regional cooperation, training exchanges, and confidence-building measures. Strengthening cyber power therefore requires synergy between military readiness, policy coherence, and public diplomacy—a convergence of hard and soft dimensions of national influence.

2.4 Hybrid Warfare (Hoffman, 2007; NATO, 2020)

Frank G. Hoffman's *Hybrid Warfare* theory describes modern conflict as a fusion of conventional military force, irregular tactics, terrorism, criminal activities, and cyber operations. The defining characteristic of hybrid war is its ability to blur the boundary between war and peace and to exploit multiple domains simultaneously (Hoffman, 2007). Cyber tools are integral to this hybrid spectrum, serving functions such as information warfare, psychological operations, and infrastructure sabotage.

NATO (2020) identifies hybrid threats as coordinated, multidomain campaigns that combine kinetic and non-kinetic instruments to achieve strategic objectives below the threshold of open warfare. In practice, this means that cyberattacks may accompany disinformation campaigns, economic coercion, or proxy conflicts, as illustrated by the Russia–Ukraine crisis.

For Indonesia, situated in a geopolitically contested Indo-Pacific region, hybrid warfare implies that digital aggression could be employed alongside diplomatic pressure or economic manipulation. The TNI Cyber Unit, therefore, must adopt a multi-domain operational logic, integrating cyber defense with intelligence, psychological operations, and strategic communication. Institutional readiness for hybrid conflict requires doctrinal innovation and joint-operations interoperability across the army, navy, and air force. As Hoffman (2007) emphasizes, victory in hybrid war depends on the agility to counter adversaries operating in both visible and invisible arenas.

2.5 Digital Transformation Organizational Model (Westerman et al., 2014)

While the preceding theories address the strategic and geopolitical dimensions of cyber conflict, the *Digital Transformation Organizational Model* focuses on the internal evolution of institutions facing technological disruption. Westerman, Bonnet, and McAfee (2014) argue that successful digital transformation requires alignment across five dimensions: leadership, structure, talent, technology, and culture. Organizations that treat digitalization merely as technological adoption fail to realize its strategic potential; instead, transformation must be holistic and human-centric.

Applying this model to the TNI Cyber Unit reveals critical insights.

- Leadership: Strategic vision from the Commander in Chief and senior officers is essential to position cyber defense as a national priority rather than a technical adjunct.
- Structure: The transition from a *Balakpus* to a *Cyber Command* would flatten hierarchies, improve agility, and enable cross-matra (inter-service) coordination.
- Talent: Continuous reskilling through cyber academies, joint training, and civilian partnerships can cultivate a cadre of digital-native officers.
- Technology: Building indigenous systems—ranging from threat-intelligence platforms to encryption standards—reduces dependency on foreign vendors.
- Culture: An adaptive, learning-oriented mindset is required to replace bureaucratic rigidity with innovation and collaboration.

Westerman et al. (2014) thus provide a managerial and sociotechnical complement to strategic theories, highlighting that organizational agility and human capital are as vital to cyber resilience as firewalls or encryption.

2.6 Integration of Military, State, and Civilian Cyber Capabilities

Synthesizing the above frameworks leads to a comprehensive model of integrated cyber defense. National Security Theory delineates the strategic imperative; Strategic Cyberwar Theory exposes institutional vulnerabilities; Cyber Power explains the instruments of influence; Hybrid Warfare illustrates the multidomain threat environment; and the Digital Transformation Model prescribes the organizational means to adapt.

The convergence of these dimensions underscores the necessity for a whole-of-nation approach. Effective cyber defense cannot be monopolized by the military. Instead, it must coordinate the efforts of three symbiotic pillars:

a. Military Capability: The TNI Cyber Unit provides disciplined command, strategic planning, and rapid-response capacity.

b. State Institutions: Agencies such as BSSN and the Ministry of Defense formulate policy, regulation, and national standards.

c. Civilian Ecosystem: Universities, private technology firms, and civil-society organizations contribute innovation, expertise, and situational awareness.

Integration across these pillars ensures that information flows, threat intelligence, and crisis responses occur in real time. It also strengthens deterrence by signaling unified national readiness. In the Indonesian context, this synergy may be institutionalized through a *National Cyber Defense Council* linking the TNI Cyber Unit with civilian agencies and industry partners.

Ultimately, the theoretical synthesis converges on a single proposition: cybersecurity is both a strategic and sociotechnical enterprise. Its success depends on harmonizing the logic of national security with the agility of digital transformation. For Indonesia, embedding these theories into doctrine and institutional design will determine the country's ability to protect its digital sovereignty and uphold national resilience amid an increasingly contested cyberspace.

3 Discussion: The TNI Cyber Unit and the Architecture of National Cyber Defense

Cyber defense is no longer a purely technical enterprise but a structural component of national strategy. The Indonesian National Armed Forces Cyber Unit (*Satuan Siber TNI*, hereafter Sat Siber TNI) represents the state's institutional response to the evolving landscape of cyber threats. Drawing from the theoretical foundations

discussed earlier, this section explores six interrelated dimensions that shape Indonesia's cyber-defense architecture: institutional transformation, professionalization of human capital, technological and infrastructural resilience, inter-agency integration, comparative international experiences, and the formulation of a *Whole-of-Nation Cyber Resilience Framework*.

3.1 Institutional Dimension — From Balakpus to Cyber Command

The establishment of Sat Siber TNI under Perpang No. 6 of 2025 as a *Badan Pelaksana Pusat* (Central Executive Agency) was a decisive first step in institutionalizing military engagement within cyberspace. Yet, its current status as a *Balakpus* limits its authority to technical coordination rather than full command and control. As Indonesia's cyber threat environment intensifies—recording over 330 million anomalies in 2024 (BSSN, 2024)—the structural elevation of Sat Siber TNI into a Cyber Command (Komando Siber TNI) becomes strategically indispensable.

In military theory, command structure determines not only efficiency but deterrence credibility. Kallberg's (2017) concept of *institutional vulnerability* underscores that fragmented command systems amplify national exposure to cyber coercion. A unified *Cyber Command* would centralize decision-making, integrate resources across the Army, Navy, and Air Force, and enhance joint-operations readiness. This mirrors the organizational evolution of the U.S. Cyber Command (USCYBERCOM), which transitioned from a sub-unit of Strategic Command in 2009 to a full unified command in 2018.

Institutional transformation also implies the development of doctrinal clarity. At present, Indonesia's defense doctrine (*Doktrin Pertahanan Negara*) only marginally addresses cyberspace. Incorporating cyber operations into the *Universal People's Defense System (Sishankamrata)* would align with Buzan's (1991) multidimensional security perspective, legitimizing the military's proactive role in safeguarding the digital commons. An elevated *Cyber Command* could thus serve as both an operational unit and a doctrinal nucleus that coordinates strategic planning, capability development, and crisis response at the national level.

3.2 Human Capital and Professionalization of Cyber Warriors

Human resources constitute the backbone of effective cyber defense. Despite significant progress, Indonesia still faces shortages in personnel with advanced cyber-warfare expertise. The *Center for Internet Security and Digital Forensics* (2024) estimates

that Southeast Asia faces a talent gap of approximately 100,000 cyber-security professionals. For the TNI, this challenge is compounded by the hierarchical nature of military careers and limited cross-sectoral mobility.

The professionalization of *cyber warriors* requires a comprehensive human-capital strategy encompassing recruitment, education, specialization, and retention. Recruitment should extend beyond traditional cadet channels to include civilian technologists, consistent with Panglima TNI General Agus Subiyanto's (2025) policy to enlist civilians with specialized digital expertise. Educational reform is equally critical. Integrating cyber modules into the curricula of the Indonesian Defense University (*Universitas Pertahanan RI*) and service academies would ensure foundational competence across ranks. Partnerships with global cyber institutes—such as Korea's KAIST Cyber Security Center or NATO's Cooperative Cyber Defense Centre of Excellence—could accelerate knowledge transfer.

A sustainable career pathway must also be institutionalized. Without recognized cyber specializations, skilled officers risk reassignment to unrelated posts, leading to attrition of expertise. The creation of a Cyber Operations Corps within the TNI would parallel the U.S. Air Force's 17th Cyber Wing or South Korea's Cyber Command Corps, formalizing progression from tactical analysts to strategic planners. Moreover, fostering a culture of ethical responsibility is essential. As Nye (2010) notes, cyber power includes moral legitimacy; thus, Indonesian cyber warriors must be trained not only in code but also in the ethics of digital warfare and the law of armed conflict in cyberspace.

3.3 Technology and Infrastructure Resilience (SOC 24/7, AI Defense)

Technological capacity is the tangible manifestation of national cyber power. The BSSN's 2024 report revealed that Indonesia's detection capability covers only 3.36 percent of national Internet traffic—a vulnerability that adversaries can easily exploit. Establishing a Security Operations Center (SOC) operating 24 hours a day, seven days a week within the TNI Cyber Unit would dramatically enhance situational awareness. Such centers integrate threat intelligence, anomaly detection, and incident response in real time, forming the operational core of modern cyber defense.

Artificial Intelligence (AI) now plays an increasingly decisive role in cybersecurity. Machine-learning algorithms can analyze petabytes of network data to identify *zero-day* exploits and detect anomalies beyond human capacity. For Indonesia, adopting AI-driven defense systems—similar to Israel's Iron Dome Cyber System or South Korea's AI Cyber Threat Intelligence Platform—could significantly shorten response

times. However, AI deployment must adhere to ethical and strategic principles to prevent automation from undermining human judgment (Westerman et al., 2014).

Infrastructure resilience further requires digital sovereignty—the ability to operate critical systems independent of foreign control. Currently, Indonesia's reliance on imported encryption software and cloud infrastructure poses strategic risks. Developing indigenous cryptographic standards and secure data centers under domestic jurisdiction would enhance both operational reliability and strategic autonomy. Collaboration with state-owned enterprises such as PT Telkom and LEN Industri could facilitate a national secure-network backbone dedicated to defense communication.

Finally, a comprehensive redundancy plan is vital. Establishing mirror data centers across multiple islands, protected through quantum-resistant encryption, would ensure continuity during catastrophic cyber incidents. These initiatives would transform the TNI Cyber Unit from a reactive entity into a resilient and predictive force capable of anticipating and neutralizing threats before they materialize.

3.4 Inter-Agency Integration (TNI – Kemhan – BSSN – Polri – Academia – Industry)

Effective cyber defense transcends institutional boundaries. The fragmented distribution of authority among Indonesia's security agencies—TNI, BSSN, Kemhan, and Polri—often leads to overlapping responsibilities and delayed responses. Building a coherent defense posture demands the establishment of a National Cyber Defense Coordination Framework anchored in shared situational awareness and information-exchange protocols.

Following the principles of *networked governance*, this integration could take the form of a Cyber Joint Task Force led by the TNI Cyber Command, comprising representatives from BSSN, Kemhan, and Polri. The task force would synchronize threat assessment, incident response, and policy implementation. Institutional mechanisms such as a *Cyber Operations Coordination Centre (COCC)* could enable real-time data fusion across agencies while maintaining civilian oversight.

Collaboration must extend beyond government. Academia provides research and innovation, while industry contributes technology and investment. The integration of universities—such as Institut Teknologi Bandung and Universitas Pertahanan RI—into defense research consortia can foster local solutions for malware analysis, digital forensics, and AI applications. Partnerships with private cybersecurity firms can supplement capacity through managed-security services and knowledge exchange.

This quadruple-helix model (state–military–academia–industry) mirrors successful ecosystems in advanced economies. For instance, the U.S. Department of Defense collaborates with the Defense Digital Service and Silicon Valley startups, while Estonia integrates civilian volunteers through its Cyber Defense League. Indonesia could adapt these models under its own legal framework, institutionalizing civil-military synergy within national-security culture. As Buzan (1991) contends, comprehensive security requires the participation of society as a whole—a principle that is equally valid in cyberspace.

3.5 Comparative Insights from the U.S., Russia, China, and South Korea

Comparative analysis provides valuable lessons for Indonesia's cyber-defense evolution.

United States.

The U.S. established USCYBERCOM in 2009 to unify cyber operations under the Department of Defense. Its dual-hat arrangement with the National Security Agency (NSA) ensures both offensive and defensive capabilities within a single strategic framework. USCYBERCOM's doctrine of *persistent engagement* emphasizes continuous action to deter adversaries by imposing tactical friction (U.S. DoD, 2023). Indonesia can adopt a scaled version of this doctrine—continuous vigilance and active defense—without necessarily engaging in offensive cyber campaigns.

Russia.

Russia's approach demonstrates the integration of cyber and information warfare. The Gerasimov Doctrine (2013) articulates the use of information operations, cyber sabotage, and psychological manipulation as part of *non-linear warfare*. Russian operations against Ukraine since 2014 illustrate the fusion of disinformation, espionage, and infrastructure attacks. For Indonesia, the Russian experience highlights the need for counter-disinformation strategies and public-information resilience to safeguard domestic stability.

China.

China's People's Liberation Army (PLA) Strategic Support Force (PLASSF), established in 2015, integrates cyber, space, and electronic warfare. Its doctrine prioritizes technological self-reliance and the fusion of civil-military innovation. China's model aligns with Westerman et al.'s (2014) digital-transformation principles, demonstrating how institutional modernization can produce systemic agility.

Indonesia can emulate this by linking defense R&D with national-innovation agencies such as BRIN and state-owned industries.

South Korea.

South Korea's Cyber Command, created in 2010 after a series of North Korean attacks, embodies resilience through continuous public-private collaboration. The command operates national SOC centers and AI-based threat-intelligence systems in partnership with companies like SK Telecom and Hanwha Systems. Its integration with the Korea Internet & Security Agency (KISA) ensures seamless information sharing. Indonesia's TNI Cyber Unit could replicate this cooperative structure, leveraging domestic telecoms and universities for joint R&D.

Collectively, these models illustrate that successful cyber-defense systems rest on three pillars: institutional unity, technological autonomy, and civil-military partnership. Indonesia's path forward should adapt—not imitate—these frameworks within its own strategic culture and constitutional constraints.

3.6 Conceptual Model: Whole-of-Nation Cyber Resilience Framework

Synthesizing theoretical insights and empirical lessons yields a proposed Whole-of-Nation Cyber Resilience Framework for Indonesia. This conceptual model integrates the multidimensional aspects of national security (Buzan, 1991), the strategic posture of cyber warfare (Kallberg, 2017), and the adaptive logic of digital transformation (Westerman et al., 2014).

a. Core Principles

1. Unity of Command and Effort — Establish a centralized Cyber Command with authority over inter-service operations while maintaining civilian accountability through Kemhan and BSSN.
2. Distributed Resilience — Ensure that every critical sector (defense, finance, energy, transportation) maintains independent yet interoperable cyber-defense capacities to prevent single points of failure.
3. Civil-Military Synergy — Institutionalize partnerships with academia, private industry, and civil-society organizations for capacity building and rapid innovation.
4. Adaptive Learning Culture — Embed continuous training, scenario-based simulations, and after-action reviews into organizational routines.

5. Legal and Ethical Governance — Develop a national cyber-law framework that balances state security with civil rights and data privacy, aligning with international norms such as the Budapest Convention.

b. Operational Mechanisms

- National Cyber Security Council (NCSC): Chaired by the President, integrating Kemhan, BSSN, Polri, TNI, and critical-infrastructure regulators.
- Cyber Intelligence Fusion Center: Co-located within the TNI Cyber Command, consolidating multi-source intelligence for early-warning systems.
- National Cyber Training and Simulation Center: Jointly operated by TNI and universities to rehearse cross-sectoral responses.
- Cyber Reserve Components (Komcad Siber): Civilian volunteers trained under military supervision to augment national capacity during large-scale incidents.
- Public Awareness and Education Programs: Embedding cybersecurity literacy within national-education curricula to cultivate a digitally resilient citizenry.

c. Strategic Outcomes

Implementation of this framework would yield three strategic outcomes:

1. Resilient Institutions: An empowered TNI Cyber Command integrated with civilian agencies, capable of unified response to national emergencies.
2. Secure Infrastructure: AI-enabled SOC networks monitoring national cyberspace in real time.
3. Informed Society: A population that understands and supports cyber defense as part of patriotic duty, transforming cybersecurity from an elite concern into a collective endeavor.

This model resonates with the logic of *comprehensive security* advanced by Buzan (1991) and Mahroza (2020), positioning cyber resilience as both a military capability and a societal virtue. It redefines national defense not merely as the protection of territory but as the protection of *digital integrity*—the trust, systems, and data that sustain national life.

3.7 Synthesis

The discussion above affirms that strengthening Indonesia's cyber-defense architecture requires simultaneous advancement across institutional, human, and

technological dimensions. Transforming Sat Siber TNI into a full Cyber Command would provide strategic coherence; professionalizing cyber warriors ensures operational competence; investing in technology delivers resilience; and inter-agency collaboration guarantees unity of effort. Comparative experiences reveal that nations achieving cyber superiority do so through integration, innovation, and institutionalization.

In essence, Indonesia's challenge is to translate strategic intent into organizational reality. As Kallberg (2018) observes, strategic cyber defense succeeds when it becomes "a living system of adaptive institutions rather than a static collection of technical tools." The proposed *Whole-of-Nation Cyber Resilience Framework* operationalizes this vision, aligning Indonesia's defense modernization with the imperatives of digital sovereignty and global stability.

4. Strategic and Policy Implications

The conceptual and comparative discussions presented earlier underscore that cyber defense is not a single-sector function but an integrated system requiring coherent doctrine, legislation, and resource alignment. The establishment of the TNI Cyber Unit has marked a fundamental shift in Indonesia's defense paradigm—extending national security from territorial protection to digital sovereignty. However, the transformation of institutional awareness into operational effectiveness requires deliberate policy reform. This section identifies five interrelated strategic implications for Indonesia's future cyber-defense posture.

4.1 Strengthening Institutional Integration and Command Authority

The first implication concerns the need for a unified and empowered institutional structure. The current fragmentation between BSSN, Kemhan, Polri, and TNI often leads to overlapping jurisdictions and delayed response times. The institutional elevation of *Satuan Siber TNI* into a Komando Siber TNI (Cyber Command) is essential for achieving *unity of command*—a principle central to effective deterrence and rapid crisis management.

This transformation must be accompanied by the creation of a National Cyber Defense Council (NCDC), chaired by the President and integrating all cyber-related agencies. Such a structure would emulate the U.S. National Cyber Directorate model while maintaining Indonesian civil–military balance. A clear command hierarchy would allow simultaneous coordination of technical defense, intelligence fusion, and policy communication—reducing redundancy and increasing national coherence.

Moreover, this institutional coherence would reinforce the *securitization* of cyberspace under Buzan's (1991) framework, ensuring that all state agencies recognize cyber threats as existential to the nation's security and act under a common operational doctrine.

4.2 Investing in Human Capital and Professional Military Education

The second policy implication lies in the domain of human resources. The development of cyber warriors demands a long-term educational ecosystem combining military discipline with digital expertise. The Ministry of Defense and TNI Headquarters should institutionalize Cyber Defense Education Programs at all military academies and staff colleges, supported by dual-degree partnerships with national universities such as Universitas Pertahanan RI, Institut Teknologi Bandung, and Universitas Indonesia.

A Cyber Operations Corps—analogous to the Air Force's 17th Wing or the U.S. Army's Cyber Corps—should be created to provide structured career pathways. Continuous education, including postgraduate scholarships in cyber strategy and artificial intelligence, would produce officers capable of bridging the gap between technical and strategic thinking.

In the broader societal context, the introduction of *Komponen Cadangan Siber* (Cyber Reserve Component) under Law No. 23 of 2019 on National Resource Management for Defense could mobilize civilian specialists to augment military capacity. Such integration aligns with Nye's (2010) notion of *smart power*—harnessing the intellectual and normative resources of society to reinforce state capability. By cultivating this hybrid cadre, Indonesia could establish a generation of digital patriots trained to defend national sovereignty in cyberspace.

4.3 Advancing Technological Sovereignty and Infrastructure Resilience

The third implication pertains to technological independence. The heavy reliance on imported digital infrastructure exposes Indonesia to supply-chain vulnerabilities and external surveillance. To achieve digital sovereignty, the government must prioritize domestic innovation through *defense industrial cooperation* between TNI, state-owned enterprises (e.g., PT LEN Industri, PT Telkom), and private technology firms.

Establishing a National Defense Cloud Infrastructure under military oversight would centralize data storage, ensure encrypted communications, and enhance

command continuity. In addition, developing AI-driven threat-intelligence platforms—capable of predictive analytics and automated incident response—would transition Indonesia from a reactive to a preemptive defense posture.

However, technological modernization should remain consistent with ethical governance. Following Westerman et al.'s (2014) digital-transformation model, technology adoption must be accompanied by leadership alignment, cultural adaptation, and transparent accountability. Establishing a *Digital Ethics Committee* within the Ministry of Defense could ensure that data protection, privacy, and proportionality principles guide every deployment of digital tools. Ethical AI usage will safeguard both national security and public trust—two sides of the same sovereign coin.

4.4 Enhancing Inter-Agency Synergy and Civil–Military Collaboration

A whole-of-nation approach requires not only integration among military institutions but also collaboration across society. As Hoffman (2007) and NATO (2020) highlight in their doctrines on hybrid warfare, the line between civilian and military targets in cyberspace is porous. Consequently, effective defense depends on multi-sectoral cooperation.

The TNI Cyber Command should formalize joint operational protocols with BSSN and Polri for coordinated responses to large-scale cyber incidents. Shared databases, encrypted communication channels, and inter-agency liaison officers would institutionalize this cooperation.

On the civilian front, academia–industry partnerships can be leveraged through research consortia on cryptography, forensics, and cyber-psychology. The Ministry of Defense could launch an annual *Cyber Defense Innovation Challenge*, inviting start-ups and university teams to develop security solutions for critical infrastructure.

Such partnerships not only expand technical capacity but also foster civic engagement in national security. As Buzan (1991) and Mahroza (2020) both assert, sustainable defense depends on the *societal ownership of security*. When citizens view cybersecurity as a collective responsibility, resilience transcends institutional boundaries and becomes a shared national ethic.

4.5 Strengthening Regional and International Cyber Diplomacy

Finally, the strategic maturity of Indonesia's cyber posture must be complemented by diplomatic engagement. In a globalized digital ecosystem, unilateral defense is insufficient. Indonesia, as the largest democracy in Southeast Asia, has a strategic opportunity to lead regional cyber governance within ASEAN frameworks.

Participation in the ASEAN Cybersecurity Cooperation Strategy (2021–2025) and alignment with the Budapest Convention on Cybercrime would signal Indonesia's commitment to international norms. Concurrently, establishing bilateral cyber-dialogue mechanisms with South Korea, Japan, and the United States could facilitate knowledge transfer and technology-sharing agreements.

Moreover, Indonesia could promote a Digital Non-Aligned Movement, advocating for a balanced global cyber order that resists technological monopolization by major powers. Such an initiative would enhance Indonesia's soft power and reinforce its role as a normative leader in digital diplomacy. Integrating this foreign-policy dimension into the defense strategy fulfills Nye's (2010) concept of *smart power*: projecting influence through credible, values-based engagement rather than coercion.

4.6 Policy Roadmap

Translating these strategic implications into actionable steps requires a structured policy roadmap:

1. Short Term (2025–2026): Formally establish the TNI Cyber Command; integrate inter-agency operations through NCDC; enhance training curricula.
2. Medium Term (2027–2029): Achieve technological sovereignty targets in SOC coverage (≥ 45% traffic visibility); expand AI-based threat analytics.
3. Long Term (2030–2035): Institutionalize the Whole-of-Nation Cyber Resilience Framework; lead ASEAN in regional cyber-defense cooperation.

Through this phased roadmap, Indonesia can consolidate its position as a digitally sovereign state capable of deterring, mitigating, and responding to cyber aggression—while maintaining ethical governance and democratic accountability.

5. Conclusion

The digital revolution has fundamentally altered the architecture of national security. For Indonesia, the cyberspace domain now constitutes the decisive frontier

in safeguarding sovereignty, integrity, and public trust. This study has demonstrated that the TNI Cyber Unit occupies a central role in this transformation—serving as the institutional nucleus of national cyber defense. Yet its effectiveness depends not solely on technology but on the synergy of institutions, people, and strategy.

From a theoretical standpoint, the combination of Buzan's (1991) National Security Theory, Kallberg's (2017) Strategic Cyberwar Theory, Nye's (2010) Cyber Power, Hoffman's (2007) Hybrid Warfare, and Westerman et al.'s (2014) Digital Transformation Model provides a comprehensive analytical lens. Together, they reveal that cyber defense is both a military and sociotechnical endeavor—requiring doctrinal integration, ethical governance, and societal participation.

The key findings of this conceptual study highlight three interdependent pillars for Indonesia's cyber resilience:

1. Institutional Coherence. Elevating *Satuan Siber TNI* into a Cyber Command ensures unity of command, operational agility, and deterrence credibility. It also enables strategic coordination across the Army, Navy, and Air Force, aligning defense operations with the broader national-security framework.
2. Human Capital Professionalization. The cultivation of cyber warriors through structured education, continuous training, and ethical formation transforms the TNI from a reactive to a knowledge-driven defense institution. Integrating civilian specialists into the *Komponen Cadangan Siber* bridges the gap between public innovation and state security.
3. Technological Sovereignty and Societal Engagement. Indigenous innovation in cryptography, AI defense, and data infrastructure not only enhances security but also affirms Indonesia's autonomy in the digital domain. Civic participation and education embed cybersecurity awareness into the national identity, transforming defense from obligation into collective virtue.

Policy-wise, the transition toward a Whole-of-Nation Cyber Resilience Framework represents the most strategic path forward. This model institutionalizes multi-sectoral collaboration under shared leadership while maintaining democratic oversight. By embedding cyber defense into national culture, Indonesia can transform vulnerability into strength, uncertainty into innovation, and fragmentation into unity.

In a geopolitical environment characterized by hybrid threats and rapid technological change, digital sovereignty equals national sovereignty. The TNI Cyber Unit, as the vanguard of Indonesia's digital defense, must therefore embody the values of professionalism, innovation, and integrity. As the country approaches 2045—the centennial of its independence—building a resilient, ethical, and sovereign

cyber ecosystem will be essential for realizing Indonesia's vision as a secure and dignified digital nation.

References

Books and Foundational Theories

Buzan, B. (1991). *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (2nd ed.). Harvester Wheatsheaf.

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac Institute for Policy Studies.

Kallberg, J. (2017). *Strategic Cyberwar Theory: The National Security Impact of Institutional Vulnerabilities. Cyber Defense Review,* 2(1), 1–25.

Mahroza, J. (2020). *Pertahanan Siber Nasional dan Keamanan Digital Indonesia.* Jakarta: Lemhannas Press.

Nye, J. S. Jr. (2010). *Cyber Power.* Belfer Center for Science and International Affairs, Harvard University.

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology into Business Transformation.* Harvard Business Review Press.

Government and Institutional Reports

Badan Siber dan Sandi Negara (BSSN). (2024). *Lanskap Keamanan Siber Indonesia 2024.* Jakarta: BSSN.

Kementerian Pertahanan Republik Indonesia. (2025). *Rencana Strategis Pertahanan 2025–2029.* Jakarta: Kemhan RI.

Panglima Tentara Nasional Indonesia. (2025). *Peraturan Panglima TNI Nomor 6 Tahun 2025 tentang Satuan Siber TNI.* Jakarta: Mabes TNI.

Pemerintah Republik Indonesia. (2025). *Undang-Undang Nomor 3 Tahun 2025 tentang Tentara Nasional Indonesia (Perubahan atas UU No. 34/2004).* Lembaran Negara Republik Indonesia Tahun 2025 Nomor 34.

NATO. (2020). *NATO 2030: Unified for a New Era.* Brussels: North Atlantic Treaty Organization.

U.S. Department of Defense. (2023). *2023 Cyber Strategy of the Department of Defense.* Washington, DC: U.S. Government Printing Office.

World Economic Forum. (2025). *Global Risks Report 2025.* Geneva: World Economic Forum.

Recent International Journal Articles

Cho, S., & Lee, J. (2024). *AI-Enabled Cyber Threat Intelligence and National Security Policy: Lessons from South Korea. Defense and Peace Economics,* 35(2), 241–260. https://doi.org/10.1080/10242694.2024.1109324

Giles, K., & McDermott, R. (2023). *Russia's Hybrid and Information Warfare Reconsidered. Journal of Strategic Studies,* 46(1), 1–23. https://doi.org/10.1080/01402390.2023.2174475

Kshetri, N. (2024). *Cybersecurity Challenges in Developing Countries: The Role of Institutions and Governance. Telecommunications Policy,* 48(4), 102530. https://doi.org/10.1016/j.telpol.2024.102530

Lindsay, J. R., & Gartzke, E. (2023). *Cyber Strategy and Deterrence in a Multipolar World. International Security,* 48(3), 75–108. https://doi.org/10.1162/isec_a_00420

Li, C., & Zhang, X. (2023). *Civil-Military Fusion in China's Cyber Command Structure. Asian Security,* 19(4), 501–523. https://doi.org/10.1080/14799855.2023.2196458

Min, H., & Kang, Y. (2024). *Building Cyber Resilience in the Indo-Pacific: Comparative Analysis of ASEAN States. Pacific Review,* 37(5), 823–845. https://doi.org/10.1080/09512748.2024.2219239

Nitoiu, C., & Paszkiewicz, J. (2025). *Digital Diplomacy and Cyber Sovereignty: Shifting Power in Global Governance. Journal of Cyber Policy,* 10(1), 1–20. https://doi.org/10.1080/23738871.2025.2419021

Tikk, E. (2023). *Cyber Norms and the Future of International Cyber Law. Journal of Conflict and Security Law,* 28(2), 133–158. https://doi.org/10.1093/jcsl/krad018

Yeo, A., & Park, S. (2024). *ASEAN's Regional Cybersecurity Cooperation: Gaps and Opportunities. Contemporary Southeast Asia,* 46(3), 376–401. https://doi.org/10.1355/cs46-3b

Zala, B. (2024). *Cyber Deterrence and Strategic Stability in the Digital Era. Security Dialogue,* 55(1), 44–63. https://doi.org/10.1177/0967010624120397

Comparative and Policy Sources

Center for Internet Security and Digital Forensics. (2024). *Southeast Asia Cyber Talent Gap Report 2024.* Singapore: ASEAN Digital Forum.

Korea Internet & Security Agency (KISA). (2024). *Annual Cybersecurity Report.* Seoul: Ministry of Science and ICT.

Estonian Ministry of Defence. (2023). *Cyber Defense League: Ten Years of Civil-Military Cooperation.* Tallinn: Estonian MOD.

Supplementary and Contextual Sources

Budapest Convention on Cybercrime. (2001). *Council of Europe Treaty No. 185.* Strasbourg: Council of Europe.

Gerasimov, V. (2013). *The Value of Science in Prediction. Military-Industrial Courier* (Translated). Moscow: General Staff of the Armed Forces of the Russian Federation.

Indonesia Cyber Security Forum. (2024). *Policy Brief on National Cyber Resilience and Digital Sovereignty.* Jakarta: ICSF.

Mahroza, J., & Prakoso, T. (2022). *Evolusi Strategi Pertahanan Siber Indonesia: Tantangan dan Arah Kebijakan. Jurnal Pertahanan & Bela Negara,* 12(3), 89–110. https://doi.org/10.33172/jpbn.v12i3.567

Pratama, R., & Naufal, M. (2025). *The Role of Indonesia's Cyber Command in the Era of AI-Driven Defense. Indonesian Journal of Defense Policy,* 4(1), 45–67. https://doi.org/10.21070/ijdp.v4i1.1539