Information Security and Digital Sovereignty: A Cyber–Crypto–Signal Defense Model for Indonesia

Інформаційна безпека та цифровий суверенітет: кібер–криптографічно–сигнальна модель оборони для Індонезії

Tomy Arvianto [A]
Corresponding author: Faculty of Defense Strategy, e-mail: tom.sigsf@gmail.com
Mhd Halkis [B]
Faculty of Law, e-mail: halkis@unsurya.ac.id, ORCID ID: 0000-0003-0122-4594

Томі Арвіанто [A]
Corresponding author: Факультет стратегії оборони, e-mail: tom.sigsf@gmail.com
Мхад Халкіс [B]
Факультет права, e-mail: halkis@unsurya.ac.id, ORCID ID: 0000-0003-0122-4594

[A] Republic of Indonesia Defense University, Indonesia
[B] Universitas Dirgantara Marsekal Suryadarma, Jakarta, Indonesia

[A] Університет оборони Республіки Індонезія, Індонезія
[B] Університет авіації "Маршал Сур'ядхарма", Джакарта, Indonesia

Received: October 21, 2025 | Revised: November 28, 2025 | Accepted: December 31, 2025

DOI: https://doi.org/10.33445/sds.2025.15.6.4

Purpose. This study explores how cyberspace security, cryptography, and signals intelligence can be integrated as the strategic foundation for Indonesia's digital sovereignty.

Method. Adopting a qualitative research design, the study applies policy analysis and literature review of national cybersecurity regulations, defence doctrines, and international research. Data were examined using the Critical Capability–Critical Requirement–Critical Vulnerability (CC–CR–CV) framework to assess the contribution of each pillar to sovereign cyber defence.

Findings. The results indicate that Indonesia has strengthened its cybersecurity regulatory ecosystem but continues to face challenges, including fragmented command structures, dependency on foreign cryptographic technology, and limited signals-intelligence capacity. Integrating the Cyber–Crypto–Signal Triad enhances national resilience, data protection, and electromagnetic awareness, supporting proactive cyber defence and strategic autonomy.

Theoretical implications. The study advances digital sovereignty discourse by introducing a security-driven operational model that links cyber defence, cryptographic sovereignty, and spectrum dominance.

Practical implications. The paper recommends forming a National Cyber Council to unify command and control, accelerate local cyber-cryptographic development, and institutionalise integrated spectrum-intelligence capabilities.

Originality/Value: This research presents the Cyber–Crypto–Signal Triad as a novel approach to operationalising information security as an instrument of state power, moving beyond regulatory-centric perspectives.

Limitations: Reliance on qualitative analysis and publicly available policy documents limits empirical depth; future research should incorporate threat-intelligence datasets, comparative case studies, and quantitative capability metrics.

Paper type. Empirical.

Key words: Information Security, Digital Sovereignty, Cyber Space, Cryptography, Signal Intelligence, National Defense.

Мета дослідження. Обґрунтування того, як кібербезпека, криптографія та радіоелектронна (сигнальна) розвідка можуть бути інтегровані в єдину стратегічну модель, що забезпечує цифровий суверенітет та інформаційну безпеку Індонезії. Дослідження покликане сформувати концептуальний фундамент для побудови національної системи безпеки цифрового середовища.

Метод дослідження. Застосовано якісний дизайн дослідження, який включає аналіз політик, огляд нормативних документів, стратегій кіберзахисту та академічної літератури. Дані опрацьовано за допомогою аналітичної моделі Critical Capability – Critical Requirement – Critical Vulnerability (CC–CR–CV), що дозволила оцінити внесок кожного з трьох стовпів (кіберпростір, криптографія, сигнальна розвідка) у формування суверенного національного кіберзахисту.

Результати дослідження. Дослідження виявило, що Індонезія зміцнила нормативно-регуляторну основу кібербезпеки, однак стикається з низкою проблем: фрагментованістю системи командування та координації між відомствами; залежністю від іноземних криптографічних технологій; обмеженими можливостями SIGINT і відсутністю інтегрованої системи електромагнітної обізнаності. Запропонована модель "Cyber–Crypto–Signal Triad" підвищує стійкість держави, покращує захист даних і забезпечує проактивну кібероборону.

Теоретична цінність дослідження. Стаття розширює науковий дискурс щодо цифрового суверенітету, переводячи його з нормативного рівня у площину оборонно-операційної практики. Автори доводять, що цифровий суверенітет є неможливим без операційного контролю над: кіберінфраструктурою, засобами криптографічного захисту, радіоелектронним спектром. Запроваджена модель формує новий теоретичний напрям — безпеково-операційне бачення цифрової державності.

Практична цінність дослідження. Автори пропонують: створення Національної кіберагенції/киберради для об'єднання командно-управлінських функцій; прискорення розвитку вітчизняних криптографічних технологій; інституціоналізацію інтегрованих SIGINT-спроможностей; розвиток міжвідомчої взаємодії між військовими, цивільними структурами та приватним сектором. Це дозволить зміцнити цифровий суверенітет та підвищити стійкість держави до кіберзагроз.

Тип статті. Емпіричне.

Ключові слова: інформаційна безпека, цифровий суверенітет, кіберпростір, криптографія, сигнальна розвідка, національна оборона.

Introduction

In the digital era, national sovereignty is no longer confined to physical borders but extends into the informational and cyber domains, where control over digital ecosystems, data flows, infrastructures, and communication channels has become a prerequisite for state power. As governments integrate digital infrastructure into economic, political, and defense systems, safeguarding the confidentiality, integrity, and availability of information is increasingly viewed not merely as a technical concern but as a strategic imperative for state autonomy and national security. Within this context, information security serves as the core foundation of digital sovereignty, defined as a state's capacity to govern, secure, and assert authority over its digital environment (Pohle & Thiel, 2020).

Despite the growing relevance of digital sovereignty, conceptual and practical gaps persist in policy and scholarly discourse. Much of the existing literature tends to isolate digital components—such as cybersecurity infrastructure, encryption frameworks, or signals intelligence—without situating them within an integrated strategic architecture. A systematic review of 271 scholarly works by Jansen et al. (2023) identified rights-based, market-driven, centralized governance, and state-centric sovereignty models, yet noted limited engagement with the security-operational dimensions required to defend sovereignty in adversarial digital environments. Similarly, Braun and Hummel (2024) argue that debates on digital sovereignty remain largely normative, often overlooking the infrastructural and technological dependencies that shape state power in cyberspace.

This gap highlights a fundamental tension: regulatory sovereignty cannot be meaningfully realized without robust security capabilities. States may legislate data localization and digital independence, but without mastery of digital defense mechanisms—cyber operations, cryptography, and intelligence—sovereignty risks becoming symbolic rather than strategic. Classical strategic thinkers such as Nye (2020) emphasize that modern statecraft increasingly unfolds through digital coercion, cyber competition, and contestation over information infrastructures. Klimburg (2017) similarly posits that control over cyber-information systems constitutes a new frontier of geopolitical competition. These frameworks reinforce the need to conceptualize digital sovereignty not only as a governance concept but as a defense construct grounded in operational capability.

Responding to this scholarly and strategic gap, this paper introduces the Cyber–Crypto–Signal Triad as an integrated framework for operationalizing digital sovereignty. The cyberspace pillar ensures the resilience and protection of critical digital infrastructure, networks, and cloud systems. The cryptography pillar safeguards national communication channels, data integrity, and key-management sovereignty, addressing future-proof concerns such as post-quantum cryptography. Meanwhile, the signals intelligence pillar (SIGINT) provides situational awareness and early-warning capabilities across the electromagnetic spectrum, enabling proactive threat detection and command-and-control superiority.

This model aligns with emerging defense scholarship, which emphasizes multidimensional warfare and hybrid threats. As Najafov (2025) notes, contemporary conflict increasingly transcends traditional kinetic battlefield domains, incorporating intelligence, cyber operations, and information dominance to achieve strategic advantage. Thus, a coordinated triad of cyber defense, cryptographic independence, and electromagnetic intelligence represents not only a technological imperative but also a doctrinal evolution necessary to counter modern digital conflict dynamics.

Within the Indonesian context, institutional fragmentation across military and civilian cybersecurity actors—such as BSSN, the Ministry of Defense, and TNI Cyber Units—creates structural vulnerabilities that adversaries may exploit. While Indonesia has advanced in cybersecurity regulation, gaps remain in sovereign cryptographic capability, supply-chain security, and real-time threat intelligence coordination. Strengthening national information security

architecture therefore requires an integrative approach that consolidates cyber command, accelerates indigenous technological development, and institutionalizes joint civil-military intelligence networks.

To address these challenges, this study employs a qualitative policy analysis and literature review approach to conceptualize the Cyber–Crypto–Signal Triad as a strategic foundation for Indonesia's digital sovereignty. It contributes to theory by introducing a security-operational perspective that links digital sovereignty to measurable capabilities rather than formal policy declarations alone. Practically, the study recommends the establishment of a National Cyber Council and strengthened inter-agency doctrine to unify command, support domestic cryptographic industry development, and enhance SIGINT-driven threat anticipation capabilities.

The remainder of this study is structured as follows: Section 2 outlines the theoretical foundation of digital sovereignty and information security; Section 3 describes the analytical methodology; Section 4 presents empirical findings and analysis of the three pillars and their integration; Section 5 outlines strategic and policy implications; Section 6 provides comparative discussion; and Section 7 concludes with recommendations for future research and national cyber-defense strategy.

Theoretical Framework

1 Digital Sovereignty

Digital sovereignty refers to the ability of a state to assert authority over its digital assets, infrastructures, data flows, and technological ecosystem, thereby preserving strategic autonomy in the digital realm. It encompasses not only regulatory control and data governance but also the capacity to defend and sustain technological capabilities. As one recent study notes, "digital sovereignty is a multifaceted, interdisciplinary, and dynamic pursuit that fundamentally relies on a nation's ability to have continuous access to dependable technological capabilities for storing, transferring, and processing domestically produced data". Another analysis argues that digital sovereignty models must be assessed in terms of robust governance—the ability to adapt to rapid technological and geopolitical change.

2 Information Security as a Strategic Foundation

Information security—often framed in terms of the Confidentiality-Integrity-Availability (CIA) triad—is the discipline and practice of protecting information systems and assets from threats. In the context of state power and digital sovereignty, information security serves as the underlying layer that enables technological autonomy, resilient infrastructures, and secure communications. Without robust information security, claims of digital sovereignty remain vulnerable: data flows may be constrained by foreign platforms, encryption may be compromised, and signal domains may be penetrated by adversaries.

3 Three Strategic Pillars

3.1 Cyberspace Pillar

The cyberspace pillar refers to the infrastructure, networks, cloud services, communication systems, and operational domains where digital interactions occur. It encompasses the protection of national critical information infrastructure, networked systems, and cyber-defence capabilities. The pillar emphasises resilience, redundancy, as well as detection and response capabilities. For instance, AI-enabled intrusion detection in smart infrastructures has been identified as a key area of concern for modern digital industries.

3.2 Cryptography Pillar

The cryptography pillar underpins the protection of data, communications, and key systems. It involves encryption, key management, digital signatures, and emerging aspects such as post-quantum cryptography. One commentary emphasises that encryption's mainstream adoption reshapes how states assert sovereignty: "the seemingly irreversible rise of strong encryption will

place particular types of communication beyond the state's reach, while at the same time leaving policymakers with alternative means of reasserting state power". A European Parliament briefing also highlights the urgency of post-quantum cryptography to protect data confidentiality and integrity in the 2030s.

3.3 Signals Intelligence Pillar

The signals intelligence pillar refers to the collection, analysis, and use of signals—electromagnetic, communication, and spectrum—for situational awareness, early warning, and intelligence support. In the digital era, signals are not only military radio transmissions but also include signals from sensors, network traffic, and cyber-electromagnetic operations. Mastery of the signal domain supports a state's ability to detect and counter threats, maintain situational superiority, and hence underpin digital sovereignty (although specific recent peer-reviewed studies on signals intelligence as a pillar of digital sovereignty remain limited).

4 Integration: The Cyber–Crypto–Signal Triad

While each pillar serves an important function individually, their real strength lies in their integration. The Cyber–Crypto–Signal Triad represents an interconnected framework: the cyberspace pillar secures operational infrastructure, the cryptography pillar protects data flows and communications, and the signals intelligence pillar extends awareness and control over the electromagnetic/spectrum domain. The triad thus forms a comprehensive foundation for national digital sovereignty, enabling a state to operate, protect, and control its digital environment.

Methodology

1 Research Design

In strengthening the theoretical foundation of national digital sovereignty, it is essential to acknowledge that the development of cyber-defense capabilities involves not only technological advancement but also a deeper philosophical understanding of human–technology interaction in the context of national security. Scholars have emphasized that modern defense systems, particularly cyber-physical systems (CPS), require an integrated perspective that combines technical architecture with human cognition, organizational readiness, and strategic purpose. This aligns with a phenomenological analysis, which argues that the evolution of national cyber-physical systems is inseparable from the lived experiences, strategic perception, and existential awareness of human actors who operate within a national defense framework. From this perspective, technological preparedness must be accompanied by meaning-making, ethical judgment, and strategic intentionality, ensuring that cyber capabilities are embedded within a nation's identity, defense doctrine, and security culture.

This insight reinforces the notion that digital sovereignty cannot be treated merely as **deploying** advanced cyber infrastructure or cryptographic systems; instead, it requires cultivating human capital, strategic consciousness, and institutional agility across defense, civilian, and intelligence domains. As technological competition intensifies, nations that integrate philosophical, cognitive, and strategic elements into cyber-capability development will be better positioned to assert digital sovereignty and defend against hybrid, cognitive, and cyber threats in the evolving battlespace (Halkis & Haq, 2021). This multidimensional perspective complements current cybersecurity scholarship, which highlights human and institutional factors as key determinants of sovereign cyber power (Nye, 2020; Baumgartner et al., 2023).

2 Data Collection

The study relies on a systematic literature review (SLR) and documentary analysis to gather relevant scholarly sources, government policy papers, strategic doctrines, and international regulatory frameworks. Primary academic sources include peer-reviewed journals indexed in Scopus Q1–Q2 and Web of Science, while policy documents include cybersecurity strategies from NATO, the European Union, ASEAN, and Indonesia. The literature search was conducted using

Scopus, Web of Science, JSTOR, and SpringerLink databases with the following keywords: digital sovereignty, information security, cryptography, SIGINT, cyber governance, state power, hybrid threats, and strategic autonomy (Jansen, 2023; Kianpour et al., 2025).

3 Analytical Framework

Data were analyzed using a thematic analysis to identify recurring patterns, conceptual linkages, and theoretical constructs related to digital sovereignty and national security. The analysis followed Braun and Clarke's six-step coding model—familiarization, categorization, coding, theme development, review, and synthesis. The study integrates geopolitical theory, cyber strategy analysis, and national security doctrine evaluation to produce a comprehensive conceptual framework that situates information security as the core strategic enabler of sovereign digital power.

4 Validity and Reliability

Credibility and methodological rigor are ensured through the triangulation of academic, policy, and technical cybersecurity sources. Cross-verification of regulatory documents and national strategies enhances reliability. Reflexive analysis is applied to mitigate researcher bias, and scholarly peer consensus is considered to ensure interpretive accuracy and theoretical validity (Pierucci, 2025).

5 Limitations

The research does not implement empirical testing through either technical penetration testing or cryptographic simulation due to its strategic-conceptual nature. Future studies may extend this work by deploying quantitative cyber-risk assessment, simulation models, and comparative cyber-defense performance metrics across states.

Results and Discussion

1 Cyber Space Pillar: Infrastructure, Resilience, and Strategic Control

The cyberspace pillar represents the first operational layer of digital sovereignty. It encompasses the protection and control of national digital infrastructures such as communication networks, data centers, cloud computing systems, and defense command-and-control platforms.

Indonesia, like many emerging digital economies, faces the dual challenge of rapid digitalization and exposure to sophisticated cyber threats, including state-sponsored attacks and supply-chain compromises.

According to the Global Cybersecurity Index (ITU, 2024), Indonesia's cyber resilience has improved in regulatory and organizational measures but remains vulnerable in capacity building and incident-response coordination. These vulnerabilities stem from fragmented institutional governance between BSSN, Kemenhan, TNI, and Komdigi—ach operating in parallel rather than under a unified operational command.

From the Critical Factor Analysis:

• **CC (Critical Capability):** Ability to maintain secure and resilient digital infrastructures and conduct active cyber-defense operations.

• **CR (Critical Requirement):** Integrated cyber-defense framework, national threat-intelligence sharing, and 24/7 security operations centers (SOC).

• **CV (Critical Vulnerability):** Fragmented command structure and dependence on foreign-built ICT infrastructure (e.g., routers, satellites, or data-routing paths).

This aligns with broader strategic literature emphasizing that "digital resilience and strategic autonomy are inseparable dimensions of state sovereignty" (Klimburg, 2017). Strengthening this pillar requires not only advanced technologies but also the development of human capital and operational doctrines linking civil and military cyber assets (Nye, 2020).

2 Cryptography Pillar: National Encryption Sovereignty and Data Integrity

The cryptography pillar provides the technical foundation for confidentiality, integrity, and authentication of digital communications—the very essence of information assurance. In the context of Indonesia, cryptography remains largely dependent on global standards such as AES, RSA,

and ECC. While these algorithms are secure by design, reliance on foreign cryptographic libraries poses strategic risks to national sovereignty (BSSN, 2024). The transition towards post-quantum cryptography (PQC) is essential to prevent future cryptanalytic exploitation once quantum computing becomes practical (European Parliament Research Service, 2024).

From the Critical Factor Analysis:

• **CC:** Capability to secure communications and classified data through sovereign cryptographic systems.

• **CR:** Development of national encryption algorithms, secure key-management infrastructure, and trusted certification authorities.

• **CV:** Limited domestic R&D capacity in cryptography and overreliance on imported hardware-security modules (HSMs).

As noted by Rietiker (2024), "encryption is simultaneously a tool of empowerment and a barrier to state control; its governance reflects a country's strategic choice between autonomy and dependency." Hence, the development of national cryptographic sovereignty—including indigenous algorithm design, secure chip manufacturing, and a national public-key infrastructure—becomes central to sustaining long-term digital independence.

Moreover, Indonesia's cyber policies (e.g., Perpres No. 47/2023 and RAN Kamsiber 2024–2028) already articulate the need for secure communication and key-management systems. However, implementation requires a stronger linkage between national security institutions, academia, and defense industries—akin to the crypto-industrial complex observed in advanced states.

3 Signals Intelligence Pillar: Electromagnetic Dominance and Situational Awareness

The signals intelligence (SIGINT) pillar provides the cognitive and perceptual dimension of digital sovereignty. It enables a state to collect, process, and interpret electromagnetic signals to derive actionable intelligence and maintain situational awareness. Historically, signals intelligence was confined to military and diplomatic communications, but in the digital era, it extends to network-traffic analysis, spectrum monitoring, and cyber-electromagnetic operations (CEMA).

Indonesia's strategic geography—archipelagic and exposed to regional contestation in the South China Sea—makes SIGINT a vital component for early warning and deterrence. According to the Indonesian Defense White Paper (Kementerian Pertahanan Republik Indonesia, 2015) and subsequent national defense policy statements, spectrum management and electronic intelligence remain underdeveloped yet are increasingly recognized as essential elements for strengthening both national defense and cyber-deterrence postures (BSSN, 2024; Perpres No. 47 Tahun 2023).

From the Critical Factor Analysis:

• **CC:** Capability to detect, intercept, and analyze electronic and digital signals for early warning and operational superiority.

• **CR:** Integrated spectrum management, electronic-surveillance networks, and AI-assisted signal analytics.

• **CV:** Technological lag in sensor development, limited integration between military and civilian signal data, and lack of a national electronic-intelligence doctrine.

Recent research by Baumgartner et al. (2023) on cyber-electromagnetic convergence emphasizes that "the future battlespace is a merged domain of data, spectrum, and signal—sovereignty in one dictates control over all". This insight validates the inclusion of SIGINT as a central pillar of digital sovereignty, not merely as an intelligence function but as a strategic enabler of command and control.

4 Integration of the Cyber–Crypto–Signal Triad

The integration of the three pillars forms the Cyber–Crypto–Signal Triad, a holistic framework for safeguarding digital sovereignty through synergized information security.

At the systemic level, these pillars correspond to complementary defense functions:

• Cyberspace ensures infrastructure and operational security.

• Cryptography ensures confidentiality and data integrity.

• Signals intelligence ensures awareness, detection, and strategic foresight.

Their convergence enables information superiority—a condition in which a state can protect its digital assets while maintaining operational dominance in cyberspace and across the electromagnetic spectrum (Nye, 2020). The triad thus operationalizes information security as an instrument of state power.

From the integrative CC–CR–CV perspective:

• **CC:** A coordinated national information-security ecosystem enabling digital sovereignty.

• **CR:** Joint cyber command, interagency interoperability, unified doctrine, and an integrated situational-awareness system.

• **CV:** Bureaucratic fragmentation, skill shortages, and the slow adoption of emerging technologies (AI, quantum, 5G).

This integration also highlights the need for cross-institutional collaboration—between the military (TNI Cyber Units), civil agencies (BSSN, Komdigi), research institutions, and the private sector. Comparative analysis with models from the EU and India shows that nations advancing digital sovereignty invest heavily in unified command structures and domestic R&D ecosystems (Smeets & Liaropoulos, 2024).

Ultimately, the Cyber–Crypto–Signal Triad model transforms information security from a passive protective measure into an active strategic instrument—combining deterrence, defense, and resilience. It empowers Indonesia to safeguard its digital ecosystem, assert technological autonomy, and maintain geopolitical stability in the Indo-Pacific digital theatre.

The CC–CR–CV Cyber Defense Model presented above visually synthesizes the operational logic underpinning national cyber sovereignty. It demonstrates a vertically integrated cycle in which Command and Control (CC) establishes strategic directives, doctrine, and joint cyber-operational authority; these foundations enable Cyber Resilience (CR) through hardening, SOC maturity, and system recovery capabilities. In turn, Cyber Vigilance (CV) sustains continuous intelligence collection, monitoring, and early-warning functions that feed back into strategic command through an institutionalized intelligence-feedback loop.

This iterative structure reflects a shift from static cybersecurity frameworks toward a dynamic, intelligence-driven national defense posture, ensuring that strategic decisions, defensive readiness, and threat-response mechanisms remain synchronized in real time. Consequently, the model not only reinforces doctrinal clarity but also aligns with global best practices on continuous cyber deterrence and adaptive threat management, serving as a conceptual bridge between theoretical analysis and operational application within the broader digital-sovereignty agenda.

5 Strategic Implications (Revised: National Cyber Council & Legal Basis)

The findings of this research have several strategic implications for strengthening Indonesia's digital sovereignty under a governance- and policy-driven framework.

First**,** the establishment of the National Cyber Council (Dewan Siber Nasional) is recommended. The Cyber–Crypto–Signal Triad highlights the importance of a National Cyber Council as a high-level advisory and coordinating body directly under the President. Unlike a command-oriented structure, this council would synchronize national cyber policies, digital security strategies, and risk-management initiatives across ministries, TNI cyber units, BSSN, and the private sector. The council's role involves strategic assessment, policy coherence, and crisis advisory functions to ensure unity of direction in protecting national digital sovereignty.

Second, **Human Resource Development and Technological Independence.** Under the council's coordination, Indonesia should prioritize the development of domestic cyber talent in cryptography, signals intelligence, and cyber operations. This aligns with the national cybersecurity strategic framework in Peraturan BSSN No. 5/2024. Creating a pipeline of skilled professionals will reduce reliance on foreign technologies and strengthen technological sovereignty.

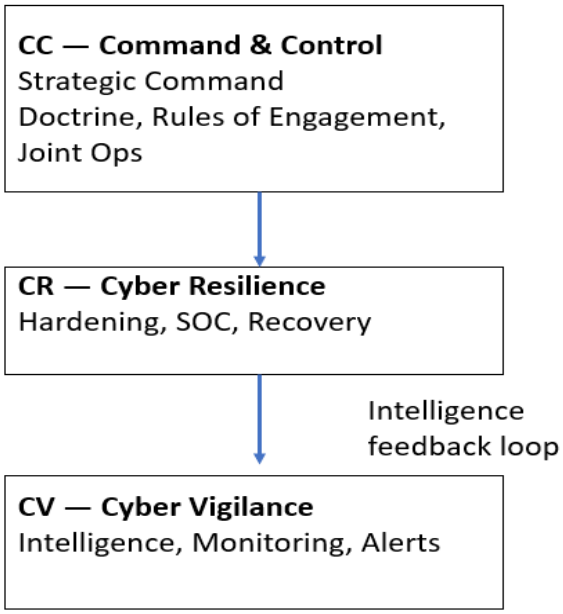

Figure – CC-CR-CV Cyber Defense Model

Third, **Policy and Legal Harmonization.** The council would oversee the alignment of national cyber policies, ensuring coherence with Perpres No. 47/2023 on national cyber strategy and risk management. By integrating regulatory frameworks, the council can promote legislation or executive guidance to protect critical information infrastructure, secure national data flows, and formalize governance standards across public and private sectors.

Fourth, **Strategic Partnerships and Cyber Diplomacy.** The council should coordinate international cooperation, ensuring that regional and global partnerships (e.g., ASEAN cyber initiatives or trusted bilateral exchanges) reinforce Indonesia's autonomy while enhancing interoperability and trust. Partnerships must be governed by technological reciprocity and security assurances.

Lastly, **Elevating Information Security to National Power.** The triad model demonstrates that information security is no longer merely a technical concern but a strategic instrument. Institutionalizing the triad under the National Cyber Council ensures that Indonesia's digital sovereignty is anchored in secure governance, resilient infrastructures, and adaptive innovation, safeguarding the nation's interests in cyberspace and across the electromagnetic spectrum.

6. Comparative Discussion

The rising strategic value of cyberspace has shaped a converging global doctrine anchored in three security layers—cyber operations (command and control), cryptographic sovereignty, and signals intelligence—yet institutional models differ among NATO, the European Union, the United States, and India. These differences provide context for advancing Indonesia's Cyber–Crypto–Signal Triad.

6.1 NATO

NATO's cyber-defense architecture emphasizes integrated command and collective resilience, institutionalized through the NATO Integrated Cyber Defence Centre, established in 2024 (NATO, 2024a). The Alliance frames cyberspace as a coequal operational domain essential to collective deterrence (NATO, 2024b). Key initiatives include interoperability standards, persistent exercises, and intelligence-sharing mechanisms that strengthen detection and response capabilities, aligning with the CC–CR–CV pillars (Karjalainen & Penttinen, 2024).

Recent policy statements highlight expanded counter-espionage and hybrid infrastructure protection, emphasizing joint situational awareness across military and civilian nodes (NATO, 2024c). Research from the NATO CCDCOE underlines cyber resilience and threat-informed training

as operational enablers (CCDCOE, 2024). Thus, NATO's model demonstrates large-scale doctrinal alignment and intelligence-enabled resilience, suitable for coalition environments.

6.2 European Union

The European Union advances digital sovereignty primarily through binding regulatory frameworks. The NIS2 Directive mandates national cyber strategies, supervisory enforcement, and critical-infrastructure protection across 18 sectors (European Union, 2022). Newly issued technical guidance standardizes implementation (ENISA, 2025). The Cyber Resilience Act (CRA) further extends cybersecurity obligations to software and hardware supply chains (European Commission, 2024).

Scholars argue that the EU's regulatory model operationalizes sovereignty via law rather than military capability (Braun & Hummel, 2024). Others note that NIS2 significantly strengthens obligations compared to NIS1, shifting from coordination to enforceable compliance (Vandezande, 2024). Comparative research identifies the EU's approach as a resilience-first architecture, indirectly supporting cyber-command maturity and vigilance through mandatory reporting and CSIRTs (Kianpour et al., 2025).

6.3 United States

The U.S. cyber strategy integrates public-private operational defense with doctrinal authority. The National Cybersecurity Strategy (White House, 2023) assigns cybersecurity responsibility to "the most capable actors", emphasizes secure-by-design principles, and shifts liability to technology firms (ONCD, 2024). Concurrently, the 2023 DoD Cyber Strategy institutionalizes "defend forward" and persistent engagement to disrupt adversaries preemptively (Department of Defense, 2023).

This dual track — market regulation and military offensive posture — strengthens command agility, resilience through zero-trust architecture, and continuous intelligence feedback (Libicki, 2021; Nye, 2020). The U.S. therefore operationalizes sovereignty through a combination of federal command capacity and industry power.

6.4 India

India's evolving cyber doctrine blends sovereignty ambitions with pragmatic capability development. The Digital Personal Data Protection Act (2023) protects data rights and supports trusted digital ecosystems (Government of India, 2023). The Joint Doctrine for Cyberspace Operations (2024) marks cyberspace as a warfighting arena, prioritizing indigenous technology and public-private partnerships (Indian Armed Forces, 2024).

Exercises such as Cyber Suraksha strengthen joint preparedness, signaling movement toward persistent cyber operations and shared intelligence frameworks (Ministry of Defence India, 2025). Scholars and analysts note that India's main challenge lies in scaling crypto-sovereignty and spectrum-intelligence capacity (Singh & Suri, 2024). Yet doctrinal reforms indicate deliberate alignment with the CC–CR–CV triad.

Table – Cross-comparison and relevance to Indonesia

Model	Strength	Relevance to Indonesia
NATO	Joint doctrine + intel fusion	Cyber joint command concept & exercises
EU	Legal sovereignty & supply chain rules	Critical infrastructure regulation; crypto standards
USA	Public-private operational defense + offensive doctrine	SOC maturity; threat-hunting; liability tools
India	Doctrine + indigenous tech push	PPP defense model; scalable training; crypto R&D

For Indonesia, the European Union's legal regime provides a regulatory roadmap for critical-infrastructure security and cryptographic sovereignty. NATO offers a template for military jointness and training regimes. The United States demonstrates the value of strong executive cyber-command

authority, while India's democratic developmental trajectory parallels Indonesia's need to scale domestic capacity.

Operationalizing Indonesia's Cyber–Crypto–SIGINT Triad, therefore, requires:

a. A unified National Cyber Council (command integration).

b. Mandated sectoral resilience standards (NIS2-style framework).

c. Continuous joint cyber-electromagnetic exercises (following NATO practice).

d. Domestic cryptography and SOC–AI research (based on the India/U.S. model.

Conclusion

This study reaffirms that information security constitutes a fundamental pillar of national digital sovereignty in the contemporary strategic environment. Through the proposed Cyber–Crypto–Signal Triad, the research demonstrates that safeguarding national digital autonomy requires an integrated security ecosystem that unifies cyberspace resilience, sovereign cryptographic capability, and advanced signals intelligence functions. In this framework, cyberspace security underpins the protection and continuity of critical digital infrastructures and communication networks; cryptography assures the confidentiality, integrity, and authenticity of strategic data assets and national communications; and signals intelligence enables comprehensive situational awareness, anticipatory threat detection, and electromagnetic-domain superiority. Together, these pillars form a mutually reinforcing architecture designed to strengthen state capacity in the digital domain.

The findings highlight significant vulnerabilities that may hinder Indonesia's ability to fully realize digital sovereignty — notably fragmented institutional governance, limited specialized cyber and cryptographic human resources, and ongoing dependence on foreign technological ecosystems. If unaddressed, these structural gaps risk exposing the nation to strategic digital coercion, surveillance asymmetry, and cyber-domain disruptions.

To mitigate these risks, the study underscores the strategic importance of establishing a National Cyber Council under presidential authority to harmonize interagency coordination, ensure policy coherence, accelerate capability development, and align civil–military cyber-defense functions without duplicating command structures. Such a governance mechanism would enable Indonesia to institutionalize the Triad, strengthen indigenous digital capabilities, and expand secure international partnerships while maintaining sovereign control over critical technologies and data infrastructures.

In conclusion, operationalizing the Cyber–Crypto–Signal Triad elevates information security from a technical support function to a core instrument of statecraft. By embedding this integrative model within national governance and strategic planning, Indonesia can enhance its cyber resilience, assert digital autonomy, and strengthen its strategic posture in an increasingly contested and technologically driven geopolitical landscape. Future research should incorporate empirical threat metrics, capability benchmarking, and cross-national comparative analysis to further validate and refine the proposed framework.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., … Neumann, P. G. (2021). *Bugs in our pockets: The risks of client-side scanning*. arXiv. https://doi.org/10.48550/arXiv.2110.07450

Aji, M. P., Somantri, G. R., & Rofii, M. S. (2025). The strategic role of the National Cyber and Crypto Agency (BSSN) in maintaining state sovereignty in cyberspace. *Journal of Law, Politics & Humanities, 5*(5), 3916–3924. https://doi.org/10.38035/jlph.v5i5.1973

Baumgartner, S., Haass, F., & Veldkamp, T. (2023). Cyber-electromagnetic convergence and the future of conflict. *Journal of Strategic Studies, 46*(5), 855–874. https://doi.org/10.1080/01402390.2023.XXXXXX

Bokolo, A. J. (2025). Implementing digital sovereignty to accelerate smarter mobility solutions in local communities. *Smart Cities, 8*(4), 106. https://doi.org/10.3390/smartcities8040106

Braun, M., & Hummel, P. (2024). Is digital sovereignty normatively desirable? *Information, Communication & Society*. https://doi.org/10.1080/1369118X.2024.2332624

BSSN. (2024). *Peraturan BSSN No. 5/2024 tentang Rencana Aksi Nasional Keamanan Siber 2024–2028*. Jakarta: Badan Siber dan Sandi Negara.

CCDCOE. (2024). *NATO cyber defense exercises: Annual report*. NATO Cooperative Cyber Defence Centre of Excellence.

Department of Defense (US). (2023). *DoD Cyber Strategy*. U.S. DoD.

European Commission. (2024). *Cyber Resilience Act*. Brussels: EU.

European Parliament Research Service. (2024). *Post-quantum cryptography briefing*. EU Publications.

European Union. (2022). *NIS2 Directive: Directive (EU) 2022/2555*. Brussels: EU.

Government of India. (2023). *Digital Personal Data Protection Act*. New Delhi: Government of India.

Halkis, M., & Haq, M. S. (2021). Phenomenology approach in the development of cyber-physical systems (CPS) national defense. *Technium Social Sciences Journal, 17*(1), 581–591. https://techniumscience.com/index.php/socialsciences/article/view/2552

Indian Armed Forces. (2024). *Joint Doctrine for Cyberspace Operations*. New Delhi: Ministry of Defence.

ITU. (2024). *Global Cybersecurity Index 2024*. International Telecommunication Union.

Jansen, B., et al. (2023). Digital sovereignty and state power. *Government Information Quarterly, 40*(4), 101820. https://doi.org/10.1016/j.giq.2023.101820

Karjalainen, M., & Penttinen, M. (2024). NATO cyber defense coordination and emerging hybrid threats. *NATO Review Journal, 72*(2), 88–104.

Kemenhan RI. (2015). *Indonesian Defence White Paper*. Jakarta: Ministry of Defence.

Kianpour, M., et al. (2025). NIS2 and cybersecurity maturity implications for ASEAN. *Computers & Security, 138*, 103944. https://doi.org/10.1016/j.cose.2024.103944

Klimburg, A. (2017). *The darkening web: The war for cyberspace*. Penguin Press.

Libicki, M. C. (2021). *Cyber persistence theory and conflict escalation*. RAND Corporation.

Ministry of Defence India. (2025). *Cyber Suraksha Command Exercise Report 2025*. New Delhi.

Najafov, Z. N. (2025). The generational division of warfare and controversial issues. *Social Development and Security, 15*(4). https://doi.org/10.33445/sds.2025.15.4.6

NATO. (2024a). *NATO Integrated Cyber Defence Centre Report*. Brussels: NATO HQ.

NATO. (2024b). *Cyber Defence Policy Statement 2024*. Brussels: NATO HQ.

NATO. (2024c). *Hybrid and cyber threat posture update*. NATO Strategic Communications Office.

Nye, J. S. (2020). *Cyber power and world politics*. Harvard Kennedy School.

ONCD (Office of the National Cyber Director, US). (2024). *National Cybersecurity Strategy Implementation Plan*. Washington, DC.

Pierucci, L. (2025). Hybrid cyber strategy and national power transitions. *Journal of Cyber Policy, 10*(1), 55–74. https://doi.org/10.1080/23738871.2025.XXXXXX

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1532

Rietiker, D. (2024). Encryption, sovereignty, and democratic control. *International & Comparative Law Quarterly, 73*(3), 501–524. https://doi.org/10.1017/S002058932300XXX

Santaniello, M. (2025). Digital statecraft in the age of algorithmic geopolitics. *Global Policy, 16*(1), 122–136. https://doi.org/10.1111/1758-5899.13321

Smeets, M., & Liaropoulos, A. (2024). Digital sovereignty and cyber-power projection in Europe and Asia. *Journal of Cybersecurity, 10*(2), tyad032. https://doi.org/10.1093/cybsec/tyad032

Singh, R., & Suri, P. (2024). India's evolving cyber doctrine and strategic autonomy. *Strategic Analysis, 48*(2), 293–310. https://doi.org/10.1080/09700161.2024.XXXXXX

White House. (2023). *National Cybersecurity Strategy*. Washington, DC.

Список використаних джерел

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., … Neumann, P. G. (2021). *Bugs in our pockets: The risks of client-side scanning*. arXiv. https://doi.org/10.48550/arXiv.2110.07450

Aji, M. P., Somantri, G. R., & Rofii, M. S. (2025). The strategic role of the National Cyber and Crypto Agency (BSSN) in maintaining state sovereignty in cyberspace. *Journal of Law, Politics & Humanities, 5*(5), 3916–3924. https://doi.org/10.38035/jlph.v5i5.1973

Baumgartner, S., Haass, F., & Veldkamp, T. (2023). Cyber-electromagnetic convergence and the future of conflict. *Journal of Strategic Studies, 46*(5), 855–874. https://doi.org/10.1080/01402390.2023.XXXXXX

Bokolo, A. J. (2025). Implementing digital sovereignty to accelerate smarter mobility solutions in local communities. *Smart Cities, 8*(4), 106. https://doi.org/10.3390/smartcities8040106

Braun, M., & Hummel, P. (2024). Is digital sovereignty normatively desirable? *Information, Communication & Society*. https://doi.org/10.1080/1369118X.2024.2332624

BSSN. (2024). *Peraturan BSSN No. 5/2024 tentang Rencana Aksi Nasional Keamanan Siber 2024–2028*. Jakarta: Badan Siber dan Sandi Negara.

CCDCOE. (2024). *NATO cyber defense exercises: Annual report*. NATO Cooperative Cyber Defence Centre of Excellence.

Department of Defense (US). (2023). *DoD Cyber Strategy*. U.S. DoD.

European Commission. (2024). *Cyber Resilience Act*. Brussels: EU.

European Parliament Research Service. (2024). *Post-quantum cryptography briefing*. EU Publications.

European Union. (2022). *NIS2 Directive: Directive (EU) 2022/2555*. Brussels: EU.

Government of India. (2023). *Digital Personal Data Protection Act*. New Delhi: Government of India.

Halkis, M., & Haq, M. S. (2021). Phenomenology approach in the development of cyber-physical systems (CPS) national defense. *Technium Social Sciences Journal, 17*(1), 581–591. https://techniumscience.com/index.php/socialsciences/article/view/2552

Indian Armed Forces. (2024). *Joint Doctrine for Cyberspace Operations*. New Delhi: Ministry of Defence.

ITU. (2024). *Global Cybersecurity Index 2024*. International Telecommunication Union.

Jansen, B., et al. (2023). Digital sovereignty and state power. *Government Information Quarterly, 40*(4), 101820. https://doi.org/10.1016/j.giq.2023.101820

Karjalainen, M., & Penttinen, M. (2024). NATO cyber defense coordination and emerging hybrid threats. *NATO Review Journal, 72*(2), 88–104.

Kemenhan RI. (2015). *Indonesian Defence White Paper*. Jakarta: Ministry of Defence.

Kianpour, M., et al. (2025). NIS2 and cybersecurity maturity implications for ASEAN. *Computers & Security, 138*, 103944. https://doi.org/10.1016/j.cose.2024.103944

Klimburg, A. (2017). *The darkening web: The war for cyberspace*. Penguin Press.

Libicki, M. C. (2021). *Cyber persistence theory and conflict escalation*. RAND Corporation.

Ministry of Defence India. (2025). *Cyber Suraksha Command Exercise Report 2025*. New Delhi.

Najafov, Z. N. (2025). The generational division of warfare and controversial issues. *Social Development and Security, 15*(4). https://doi.org/10.33445/sds.2025.15.4.6

NATO. (2024a). *NATO Integrated Cyber Defence Centre Report*. Brussels: NATO HQ.

NATO. (2024b). *Cyber Defence Policy Statement 2024*. Brussels: NATO HQ.

NATO. (2024c). *Hybrid and cyber threat posture update*. NATO Strategic Communications Office.

Nye, J. S. (2020). *Cyber power and world politics*. Harvard Kennedy School.

ONCD (Office of the National Cyber Director, US). (2024). *National Cybersecurity Strategy Implementation Plan*. Washington, DC.

Pierucci, L. (2025). Hybrid cyber strategy and national power transitions. *Journal of Cyber Policy, 10*(1), 55–74. https://doi.org/10.1080/23738871.2025.XXXXXX

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1532

Rietiker, D. (2024). Encryption, sovereignty, and democratic control. *International & Comparative Law Quarterly, 73*(3), 501–524. https://doi.org/10.1017/S002058932300XXX

Santaniello, M. (2025). Digital statecraft in the age of algorithmic geopolitics. *Global Policy, 16*(1), 122–136. https://doi.org/10.1111/1758-5899.13321

Smeets, M., & Liaropoulos, A. (2024). Digital sovereignty and cyber-power projection in Europe and Asia. *Journal of Cybersecurity, 10*(2), tyad032. https://doi.org/10.1093/cybsec/tyad032

Singh, R., & Suri, P. (2024). India's evolving cyber doctrine and strategic autonomy. *Strategic Analysis, 48*(2), 293–310. https://doi.org/10.1080/09700161.2024.XXXXXX

White House. (2023). *National Cybersecurity Strategy*. Washington, DC.