IJCSS 7 (1) (2026) Pages:. 164-173

Journal homepage: http://pcijournal.org/index.php/ijcss

International Journal of Cultural and Social Science

Published: Pena Cendekia Insani

THE POLITICAL ECONOMY OF INDONESIA'S CYBER RESILIENCE: STRATEGIC GAPS IN THE PRIVATE SECTOR AND CRITICAL INFRASTRUCTURE IN FACING ADVANCED PERSISTENT THREATS (APTS)

Muhammad Fawwaz Afif[1], R. Widya Setiabudi Sumadinata[2], Satriya Wibawa[3]
[1,2,3]Padjadjaran University, West Java, Indonesia

Article Info

Keywords:

Advanced Persistent Threats (APT),
Cybersecurity,
Digital Political Economy

ABSTRACT

This research focuses on analyzing cybersecurity threats to Indonesia in the context of digital political-economic transformation, particularly following the implementation of nickel downstreaming policies and the strengthening of Indonesia's position in the global supply chain for critical minerals. This study aims to examine the structural linkages between national industrial policy, the escalation of Advanced Persistent Threats (APT) activity, the failure of public-private partnerships, stagnant cybersecurity regulations, and the limitations of Indonesia's cyber diplomacy in responding to transnational threats. This research uses a qualitative approach with a case study method, relying on analysis of policy documents, cyber threat intelligence reports from 2023-2025, academic publications, and critical reviews of strategic events such as the ransomware attack on the Temporary National Data Center. The results indicate that the cyber threats facing Indonesia are systemic and rooted in global political-economic dynamics, where downstreaming policies and dependence on foreign technology create strategic incentives for foreign actors to conduct cyber espionage against strategic industrial sectors. This study also finds weak public-private collaboration due to a trust deficit, regulatory uncertainty, and the absence of incentives for incident reporting, which leads to the state's partial blindness in understanding the national threat landscape. Furthermore, the stagnation of the Cybersecurity and Resilience Bill and the limitations of regional cyber diplomacy highlight the gap between the rhetoric of digital sovereignty and the operational capacity of states. The implications of this research emphasize the urgency of strengthening integrated cybersecurity governance, regulatory reform that balances security and civil rights, and reorienting public-private partnerships as the foundation of cyber resilience.

Corresponding Author:

Muhammad Fawwaz Afif
Padjadjaran University, Indonesia
mfawwazafif@gmail.com

1. INTRODUCTION

Indonesia's digital transformation can no longer be reduced to a mere technocratic process of adopting information technology, but rather constitutes a structural metamorphosis that fundamentally redefines the power relations between the state, the market, and the national security regime (Bagus, 2025). Projections of Indonesia's digital economy as the largest in Southeast Asia, with a Gross Merchandise Value (GMV) reaching hundreds of

billions of dollars, position cyberspace as a strategic national infrastructure on par with the conventional energy and defense sectors (Munandar et al., 2024).

Digitalization has internalized cyber systems into public services, the financial sector, national logistics, and even strategic natural resource-based industries, thus forming a systemic structural dependency (Wibowo, 2024). Consequently, disruption to the digital ecosystem no longer has sectoral implications but has the potential to destabilize national stability as a whole. Therefore, cyberspace must be conceptualized as a domain of state sovereignty that demands a holistic, adaptive, and long-term approach to national security. However, the acceleration of digital connectivity simultaneously expands the national attack surface, exposing it to a spectrum of cyber threats with increasing levels of complexity, sophistication, and strategic motives. The contemporary cyber threat landscape is no longer dominated by small-scale individual crimes, but rather by Advanced Persistent Threats (APTs) that are organized, long-term, and often intertwined with the geopolitical interests of other countries. These attacks are designed not to achieve immediate impact, but rather to systematically infiltrate critical infrastructure, accumulate strategic intelligence, and create space for economic sabotage and political destabilization. This constellation emphasizes the shift in cybersecurity from a purely technical issue to an instrument of power in the global competitive arena. Thus, cyber threats need to be interpreted within the framework of national security and international political economy, rather than being narrowed down to merely technocratic problems.

In a global geopolitical landscape marked by intensifying great power competition, Indonesia's position is increasingly paradoxically strategic and vulnerable (Milia & Attamimi, 2025). Countries with substantial digital economic capacity and strategic resource holdings tend to be prime targets for transnational cyber operations. Indonesia, which occupies a key position in the global supply chain and champions a natural resource-based energy transition agenda, is at the epicenter of this vortex of interests. Cyberattacks against Indonesia not only have the potential to disrupt domestic stability but also have regional and global implications, thus emphasizing that national cybersecurity cannot be separated from international power configurations and transnational strategic economic interests.

Empirically, a structural imbalance is evident between the pace of digitalization in strategic sectors and the readiness of the national cyber resilience system. The downstreaming policy for natural resources, particularly nickel, encourages the development of modern smelters that rely on automation, Industrial Control Systems (ICS), and global connectivity (Koay et al., 2023). This industrial infrastructure serves as the backbone of the national economy, while also creating critical vulnerability to industrial espionage and cyber sabotage. However, the cybersecurity dimension of strategic industries is often perceived as a purely corporate issue, rather than being positioned as an integral part of national security interests.

The reality on the ground also demonstrates the low level of reporting of cyber incidents by the private sector to state authorities. Strategic companies tend to conceal cyber incidents to avoid reputational damage, regulatory sanctions, or negative impacts on stock prices. This situation creates a blind spot in national cyber situational awareness, thereby depriving the state of its ability to respond collectively to threats. This phenomenon highlights the existence of structural problems in the relationship between the state and the private sector that cannot be explained solely through a normative policy approach. Previous studies have shown that national cybersecurity analysis is generally situated within the state's institutional and regulatory framework. Ginanjar (2022) emphasized the urgency of strengthening the National Cyber and Crypto Agency (BSSN) as the central node in national cybersecurity coordination and orchestration. Similarly, Setyawan et al. (2023) positioned regulations, including Presidential Regulation Number 47 of 2023, as the starting point for establishing an integrated national cyber defense system. Both studies contributed significantly to mapping the state's institutional response to the spectrum of cyber threats.

Conversely, Septyana et al. (2025) analyzed Indonesia's cybersecurity governance through a state-centric governance approach that emphasizes state dominance in strategic decision-making. However, this study failed to comprehensively elaborate on the dynamics of the relationship between the state and the private sector, the primary managers of critical digital infrastructure. In general, these studies focused on policy and institutional dimensions, without deeply linking them to strategic economic interests and the operational realities of the industry. Based on a literature review, there is a substantial research gap related to the limited analysis of Indonesian cybersecurity from a political economy perspective and the role of the strategic private sector. Existing studies are still dominated by a state-centric approach that positions the state as a sole and rational actor, thus inadequately explaining the failure of cybersecurity collaboration between industrialized countries at the implementation level. Furthermore, the cybersecurity implications of strategic economic policies, such as the downstreaming of natural resources, remain relatively marginalized in academic discourse.

The novelty of this research lies in the integration of the analysis of Indonesian cybersecurity resilience with an international political economy framework and the operational realities of the strategic private sector. Cyber threats are positioned not merely as technical risks, but as arenas for contestation of economic interests and power. By linking Advanced Persistent Threats (APTs), downstreaming policies, and the dynamics of state-industry relations, this research offers a critical perspective rarely explored in Indonesian cybersecurity studies.

In summary, this research aims to analyze Indonesian cybersecurity resilience from a political economy perspective, emphasizing the interaction between the state and the strategic private sector. This aims to identify structural weaknesses and opportunities for strengthening national cybersecurity policies that are more adaptive and long-term.

2. RESEARCH METHODS

This research employs a qualitative approach with a documentary study design and a systematic literature review to gain an in-depth and comprehensive understanding of Indonesia's national cybersecurity dynamics in relation to strategic policies and the global political-economic context (Waruwu et al., 2025). This approach was chosen because it allows researchers to critically examine the relationship between policy texts, security narratives, and empirical practices evolving within an increasingly complex cyber threat landscape.

The research data is sourced from secondary data collected through extensive documentary studies of various credible sources over the period 2020-2025. This period was chosen based on academic considerations that the post-pandemic phase is characterized by a significant escalation of cyber threats, along with the full implementation of the nickel downstreaming policy as a national strategic agenda, and the intensified discussion of the Draft Cyber Security and Resilience Law (RUU KKS). This timeframe is considered to represent a crucial phase in the formation of Indonesia's national cybersecurity architecture.

Data sources include policy and regulatory documents, including the draft Bill on the Protection of Civil Society (KKS), Presidential Regulation No. 47 of 2023 concerning the National Cybersecurity Strategy, the Personal Data Protection Law, and official strategic documents published by the National Cyber and Crypto Agency. Furthermore, this research utilizes technical threat reports from the global cybersecurity industry and leading research institutions such as Mandiant, Google Cloud, Cyfirma, Microsoft, Kaspersky, and Recorded Future, which detail the activities, tactics, and targets of Advanced Persistent Threats (APT) groups in Indonesia and Southeast Asia. Academic literature, including national and international journals discussing cyber diplomacy, the political economy of downstreaming, internet governance, and critical infrastructure risk management, is also used to strengthen the theoretical foundation of the analysis.

Furthermore, research data is also obtained from credible media coverage and reports from civil society organizations such as PBHI, ELSAM, and Lab45, which highlight strategic cyber incidents, including attacks on the National Data Center, as well as controversies over cybersecurity legislation and governance. These sources were used to capture the empirical dimensions and public discourse that developed outside of formal policy documents.

Data analysis was conducted through source triangulation and qualitative content analysis (Khoir & Amaliyah, 2025). Technical information related to attack vectors and APT activity patterns was correlated with strategic political and economic events, such as the implementation of the nickel export ban or the holding of high-level diplomatic meetings in the ASEAN region, to identify interconnections, causal tendencies, and strategic motivations of threat actors. Furthermore, this study applied gap analysis by comparing the normative mandates stipulated in cybersecurity regulations with implementation practices in the field, thus identifying structural and institutional weaknesses in Indonesia's national cybersecurity architecture.

3. RESULT AND ANALYSIS

The political-economic threat of the digital resource curse

One of the key findings of this study is the identification of a structural and systemic causal relationship between national industrial policy and the Advanced Persistent Threats (APT) threat patterns facing Indonesia. In the context of modern cybersecurity, Indonesia is not targeted by incidental attacks, but rather by its strategic position as a key node in the global supply chain for critical minerals. Cyberattacks against Indonesia reflect the dynamics of international geopolitical and economic competition, where the direction of national economic policy implicitly creates incentives for other state actors to conduct offensive cyber operations. This finding aligns with arguments in critical cybersecurity literature that view cyberspace as an extension of the arena for contestation of power and political-economic interests (Najwa, 2024).

The raw ore export ban, fully implemented since 2020, articulates the country's ambition to reposition itself from a mere supplier of raw materials to a strategic actor in the high-value-added industrial ecosystem (Prabowo, 2024). Empirically, this policy has been proven to trigger a surge in foreign direct investment (FDI), particularly from China, in the development of smelters and the electric vehicle battery industry (Matondang et al., 2026). However, this research reveals a paradoxical latent consequence: these economic achievements simultaneously place Indonesia's downstream infrastructure in the focus of foreign cyber intelligence surveillance. Smelters, refining facilities, and the electric vehicle industry's supply chain network are no longer understood merely as means of production but have transformed into strategic assets with high geopolitical value, reflecting both Indonesia's resource sovereignty and its bargaining position in the global contest for critical minerals.

Analysis of threat intelligence reports indicates that state-sponsored APT actors have strong strategic incentives to conduct cyber espionage against the nickel downstream sector (Harahap et al., 2025). From a cybersecurity political economy perspective, this sector functions as a strategic chokepoint that can determine the direction of the distribution of global industrial power (Ambardi et al., 2025). The research findings identify three primary motives for APT operations. First, the hunt for precise, non-public geological reserve data, including the location, quality, and volume of strategic minerals. This data constitutes high-value intelligence that enables competing nations to project global price fluctuations, secure future energy supplies, and develop more aggressive industrial resilience strategies.

Second, this research found strong indications of industrial espionage and intellectual property theft involving advanced refining technologies, particularly High-Pressure Acid Leaching (HPAL). This technology not only represents technical progress but also symbolizes knowledge capital built through costly research and development investments. By infiltrating the digital systems of companies and research institutions, APT actors attempt to replicate this strategic technology without bearing the costs of innovation, thus creating structural distortions in global technological competition.

Third, the research findings reveal the motives for intercepting the strategic communications of state officials directly involved in the formulation and implementation of industrial policies, such as the Ministry of Energy and Mineral Resources, the Coordinating Ministry for Maritime Affairs and Investment, and the Investment Coordinating Board (BKPM). This interception aims to uncover Indonesia's bargaining position before entering the international trade and investment negotiations arena. In cyber diplomacy literature, this kind of practice is understood as a form of cyber-enabled economic statecraft, namely the use of cyber instruments to gain negotiating advantages and structural dominance in the global economic system.

Empirical evidence gathered from threat intelligence reports from 2023 to 2025 confirms the active presence of various APT groups in Indonesia's digital ecosystem, systematically targeting strategic sectors. Mustang Panda, affiliated with China, consistently targets government institutions, the maritime sector, and telecommunications, with a focus on foreign policy espionage and ASEAN geopolitical dynamics (Vice et al., 2024). The Lazarus Group from North Korea demonstrates a pattern of attacks on the financial sector and crypto assets as instruments for state funding and evading international sanctions (Husadi & Idris, 2025). Meanwhile, APT41 (Winnti Group) represents a hybrid form of state espionage and cybercrime, specifically targeting the mining, energy, and technology sectors, including the nickel and critical minerals industries (Nugroho & Rochmadi, 2024).

These findings confirm that the most serious threats to Indonesia's digital sovereignty originate from actors with geopolitical affiliations with Indonesia's major economic partners. This situation creates a structural strategic dilemma, where the development of national technology infrastructure such as 5G networks, industrial area surveillance systems, and cloud computing services relies heavily on hardware and software from the same country as the threat actor's origin.

This dependency creates what this research calls the illusion of digital sovereignty, a situation where formal control over data does not align with substantive control over systems. Despite the implementation of data localization policies, research findings indicate that control over firmware updates, hardware integrity, and core system architecture often falls outside the scope of independent audits by national authorities such as the National Cyber and Cyber Security Agency (BSSN). Critical cybersecurity literature confirms that this situation opens the door to supply chain attacks, where compromise can occur long before the system is operational within the national territory.

In the context of the mining and energy industries, dependence on foreign Operational Technology (OT) systems connected to corporate networks creates existential vulnerabilities. If the control systems of smelters, refining facilities, or smart grids are successfully compromised, foreign actors could potentially possess latent coercive capabilities to cripple national nickel production or trigger energy disruptions in strategic industrial areas within a short time. This capability not only represents a technical threat, but also functions as an instrument of geopolitical pressure that can be activated at any time, thus confirming that the issue of nickel downstream cybersecurity is a fundamental issue that touches the core of Indonesia's economic sovereignty and national security.

Failure of public-private partnerships in the private sector

National strategic policy documents and the rhetoric of public officials in Indonesia often position the Quad Helix concept of collaboration between government, industry, academia, and civil society as the normative formula for strengthening national cyber resilience (Haryono, 2025). However, the results of this study indicate a substantial gap between the normative framework and empirical practice, particularly in the industrial dimension. Rather than appearing as a strategic partner for the state in strengthening cyber defense, the private sector is faced with structural dysfunction that limits active involvement, openness, and sustainable collaboration. This situation is closely related to the configuration of political-economic incentives that shape the rational

calculations of industry actors in the Indonesian cyber ecosystem, as also highlighted in studies of cybersecurity governance in developing countries.

One of the most consistent findings in this study is the phenomenon of under-reporting of cyber incidents by the private sector, rooted in a trust deficit and a corporate culture (image maintenance). In Indonesian business practices, acknowledging hacking or data breaches is often perceived as a reputational stigma, an indicator of managerial failure, and a direct threat to company value. Fear of falling stock prices, investor withdrawal, and erosion of consumer trust encourages companies to resolve incidents privately, rather than reporting them to state authorities such as the National Cyber and Cyber Security Agency (BSSN) or law enforcement. This phenomenon aligns with international studies showing that without clear incentives and legal protections, the private sector tends to prioritize reputation protection over collective security interests (Sinaroja & Widyoseno, 2024).

This trust deficit is further exacerbated by business actors' perceptions of state capacity. Field findings and a review of policy reports indicate that most industry players doubt the technical capabilities of government institutions to provide a swift, effective, and solution-oriented incident response. Furthermore, there are concerns that sensitive data submitted through reporting mechanisms could potentially be leaked, misused, or become a gateway to further legal issues. The literature on trust in cybersecurity governance confirms that the absence of institutional trust is a major obstacle to public-private collaboration in cybersecurity (Widya et al., 2025).

As a result of this situation, the country experiences what this study calls partial blindness in understanding the national threat landscape. Incident data held by the National Cyber and Cyber Security Agency (BSSN) and related authorities is dominated by attacks on government agencies, while sophisticated attacks on private banks, telecommunications companies, and large e-commerce platforms are often not recorded in the national system. Empirical findings indicate that many incidents are handled behind closed doors through contracts with foreign cybersecurity consultants or, in some cases, through ransom payments without coordination with the state. This situation fundamentally weakens the state's ability to establish an early warning system and share threat intelligence across sectors, as recommended by international best practices (Arbani, 2024).

This structural problem is exacerbated by regulatory uncertainty and the absence of incentive schemes for incident reporting. Unlike the United States, which has a safe harbor mechanism, or the European Union, with its clear and standardized GDPR framework, Indonesia lacks a legal regime that provides adequate certainty and protection for transparent companies. Research findings indicate that companies that report data breaches risk multiple sanctions from various regulators, public opinion pressure, and potential lawsuits, without the guarantee of technical support or sanction mitigation from the state. From an institutional economic perspective, rational business actors tend to view the costs of compliance and the risks of reporting as far greater than the benefits (Siladjaja et al., 2023).

Furthermore, industry evidence suggests that cybersecurity investment in the Indonesian private sector is still positioned as a cost center, rather than a long-term strategic investment. Data from Business Indonesia (2025) noted that the average cybersecurity expenditure per employee in Indonesia is only around USD 18.89, a figure far behind global standards (Paddu, 2024). This situation creates a fragile security ecosystem, particularly among Micro, Small, and Medium Enterprises (MSMEs) integrated into large industrial supply chains. This research found that APT actors often exploit MSMEs as the weakest link through island-hopping techniques, namely hacking small vendors with minimal protection and then infiltrating the networks of large, targeted companies, as also identified in the literature on global supply chain attacks.

The structural vulnerabilities of this industrial sector are further exacerbated by a talent crisis and a human resource capability gap. Indonesia faces a serious shortage of highly specialized cybersecurity experts, such as threat hunters, malware analysts, digital forensic investigators, and security architects. Research findings indicate a war for talent, with the best talent being absorbed by multinational technology companies and the tier-1 banking sector, which can offer competitive remuneration. As a result, other critical infrastructure sectors—such as regional water and electricity utilities, public transportation, hospitals, and local governments—experience acute human resource gaps or limitations.

When facing APT actors manned by foreign military or intelligence units with nearly unlimited resources, this imbalance creates a dangerous capability asymmetry between attackers and defenders. As Prayitno (2025) emphasized, national cyber resilience is determined not only by technology and regulations, but also by the quality of the people who operate these systems. Without structural reforms to the industrial pillars within the Quad Helix, the concept of national cyber collaboration risks remaining an elitist, yet fragile, normative narrative in the face of increasingly aggressive and orchestrated geopolitical cyber threats.

Regulatory paralysis in the stagnation of the KKS Bill and sectoral egos

The existence of a strong, comprehensive, and legitimate legal framework is a constitutive prerequisite for the development of effective and sustainable national cyber resilience. This research's findings confirm that the

absence of the Cyber Security and Resilience Law (RUU KKS) is not merely a technical legislative issue, but rather a reflection of structural political-legal conflict, where state security interests, civil liberties protection, and institutional rivalries are intertwined. Legal political analysis shows that the RUU KKS is trapped in a complex tug-of-war of interests, resulting in its passage being continually delayed and losing political momentum (Fadilla et al., 2025).

The most consistent opposition to the RUU KKS comes from a coalition of civil society, academics, and digital rights activists, who view the substance of this regulation as rife with a state-centric cybersecurity paradigm. The research findings indicate that articles granting broad authority to the state, particularly the National Cyber and Security Agency (BSSN) and security forces, to filter, intervene, and monitor digital data traffic are perceived as potentially becoming a mass surveillance mechanism that threatens citizens' privacy and freedom of expression. This criticism aligns with global literature, which asserts that the expansion of state cyber authority without democratic oversight risks creating a surveillance state that diminishes digital civil space (Kusumoningtyas, 2023).

Historical trauma from past state surveillance practices has shaped collective memory, making any attempt to centralize information control viewed with deep suspicion. Civil society organizations such as PBHI, ELSAM, and Imparsial have consistently criticized the KKS Bill's approach, which places state security above individual security (human security), while ignoring the principles of privacy by design and due process of law. Research findings indicate that the vague and elastic definition of "cyber threat" has the potential to be interpreted repressively to silence political criticism, digital activism, or oppositional expression in cyberspace. This mobilization of critical discourse has proven effective in hampering the KKS Bill's political legitimacy in parliament, as without public trust and explicit guarantees of human rights protection, cybersecurity legislation struggles to gain adequate social acceptance (Indonesian Legal Aid and Human Rights Association, 2025).

Beyond civil society resistance, this research also found that the legislative deadlock on the KKS Bill was triggered by institutional rivalries and sectoral egos entrenched within the state bureaucracy. Indonesia's cybersecurity governance is currently fragmented among several institutional actors with overlapping mandates. The National Cyber Security Agency (BSSN) is positioned as the national cybersecurity coordinator, while the Ministry of Communication and Digital controls internet infrastructure, ESE, and content blocking policies. Meanwhile, the Indonesian National Police (Polri) has a mandate to enforce cybercrime laws, and the Indonesian National Armed Forces (TNI) has a strategic interest in cyber defense and information operations.

The KKS Bill, which positions the National Cyber Security Agency (BSSN) as the leading sector with broad executive authority, including investigation, prosecution, and asset confiscation, is perceived by other institutions as a threat to their jurisdiction and authority. Research findings indicate that the BSSN's authority to filter "cyber threat" content directly overlaps with the mandate of the Ministry of Communication and Digital Technology, while its investigative authority overlaps with the National Police and the Attorney General's Office. This competition for fiscal resources, political influence, and institutional legitimacy has created a deadlock within the Inter-Ministerial Committee (PAK), resulting in the KKS Bill stalling without substantial progress for years. This phenomenon confirms the theory of institutional rivalry, which states that fragmentation of authority is a major obstacle to national security governance reform (Widodo et al., 2022).

The absence of the KKS Bill directly impacts the state's weak coercive capacity to enforce cybersecurity standards. Research findings indicate that the BSSN lacks the legal capacity to enforce compliance by private Electronic System Operators (PSEs). This institution can only issue recommendatory guidelines and technical standards, without the authority to impose strict administrative or criminal sanctions. As a result, national cybersecurity standards operate within a fragmented voluntary compliance framework, creating structural gaps consistently exploited by cyber threat actors (Najwa, 2024).

As a tactical response to this legislative impasse, the government issued Presidential Regulation Number 47 of 2023 concerning the National Cybersecurity Strategy and Crisis Management. Research findings indicate that this Presidential Regulation does provide a clearer coordination framework for handling cyber incidents and managing crises. However, legally, its status as a presidential regulation presents fundamental limitations. The Presidential Regulation's binding power is internal administrative and relatively weak for the private sector and the wider public. It lacks the capacity to impose criminal sanctions or significant fines, nor does it have the capacity to create economic incentives to encourage voluntary compliance on a national scale.

Without a strong legal foundation, efforts to enforce cybersecurity standards in critical sectors such as banking, telecommunications, and energy remain reliant on partial and often unsynchronized sectoral regulations. These findings indicate that Presidential Regulation 47/2023 serves more as a temporary administrative solution than a structural instrument capable of holistically building national cyber resilience. In this context, the absence of the KKS Bill is not merely a legal vacuum, but a strategic gap that systematically weakens the state's ability to confront increasingly organized and aggressive geopolitical cyber threats.

The effectiveness of diplomacy and defense between rhetoric and reality

In response to the escalation of increasingly complex cross-border cyber threats, Indonesia has positioned cyber diplomacy as a key pillar of its external defense (Najib & Aidil, 2025). This diplomacy is projected as a normative instrument for building stable, secure, and predictable international cyberspace governance. However, empirical evaluations of the effectiveness of Indonesian cyber diplomacy have yielded ambivalent results. On the one hand, there is recognition of Indonesia's active participation in multilateral forums; on the other hand, such diplomacy has proven to have limited deterrence capacity when faced with the reality of state-sponsored cyber attacks, particularly those carried out by shadowy actors such as Advanced Persistent Threats (APTs).

At the regional level, Indonesia has consistently pushed for the establishment of norms of responsible state behavior in cyberspace through ASEAN and global forums such as the United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG). However, ASEAN's fundamental principle of non-interference has transformed into a strategic paradox in the context of cybersecurity. This principle, originally intended to maintain regional political stability, has instead served as a structural barrier when indications of cyberattacks originate from ASEAN member states themselves or from strategic dialogue partners such as China, the United States, and North Korea. The reluctance to engage in public attribution and open diplomatic confrontation has caused regional response mechanisms to lose their operational effectiveness and become trapped in a normative deadlock.

Regional forums such as the ASEAN Regional Forum (ARF) and the ASEAN Ministerial Conference on Cybersecurity (AMCC) have indeed succeeded in establishing Confidence Building Measures (CBMs), including the creation of emergency contact directories and joint cyber drills. However, these achievements are procedural and symbolic, failing to address the substantive dimensions of establishing collective response mechanisms, joint attribution, or sanctions regimes for cyber norm violations. As Attaqi (2022) notes, ASEAN cyber diplomacy tends to be trapped in a politically safe, technocratic approach, focusing on capacity building while systematically avoiding sensitive issues such as interstate cyber espionage, which is at the heart of the APT threat. Consequently, Indonesia frequently faces aggressive unilateral cyberespionage campaigns without significant regional political and diplomatic support.

These limitations of cyber diplomacy were dramatically exposed in the June 2024 attack by the Brain Cipher ransomware variant of LockBit 3.0 on the Temporary National Data Center (PDNS). This incident crippled not only immigration services but also more than 200 public services across ministries and agencies for weeks. This incident became a critical juncture that exposed structural and systemic weaknesses in Indonesia's national cybersecurity architecture.

First, the attack exposed fundamental failures in the data backup and recovery system. The absence of a mature, tested, and segmented Disaster Recovery Plan resulted in backup data being unavailable offline and even encrypted due to flawed system design. This situation placed the country in a very weak bargaining position, both technically and politically. Second, the ambitious policy of data centralization through the National Data Center was not matched by adequate centralization of security capacity. Instead of strengthening digital resilience, this consolidation created a single point of failure, making it easier for threat actors to cripple hundreds of institutions through a single point of penetration. Third, the slow crisis response, minimal coordination, and opaque public communication exacerbated the social and administrative impacts and eroded public trust in the state.

Furthermore, the PDN incident not only disrupted domestic services but also damaged Indonesia's credibility with global investors and international partners. This incident calls into question the country's readiness to manage strategic data and critical digital infrastructure. Thus, the attack serves as empirical evidence that cyber diplomacy and the rhetoric of "digital sovereignty" have yet to be successfully transformed into robust operational capabilities. This gap between normative ambitions and technical realities underscores that without institutional strengthening, integrated security governance, and political courage in regional fora, Indonesia's cyber diplomacy will remain declarative and unable to prevent attacks that cripple the nation's vital infrastructure.

4. CONCLUSION

This research finds that cyber threats to Indonesia are not isolated technical phenomena, but rather manifestations of structural and systemic global political-economic dynamics. Indonesia's nickel downstreaming policy and repositioning within the global critical mineral supply chain have paradoxically enhanced its national economic bargaining position, while simultaneously making it a strategic target for state-sponsored cyber espionage operations conducted by Advanced Persistent Threats (APT) actors. These findings teach us that economic transformation based on digital resources and strategic minerals always carries latent security consequences. Cybersecurity, in this context, can no longer be understood as a purely technical domain, but rather as an instrument of power inherent in geopolitical contestation, economic diplomacy, and national sovereignty. From a theoretical perspective, this research reinforces the political economy approach to cybersecurity, which views cyberspace as an arena for conflicting state interests. Practically, these findings provide

an important lesson: the success of national industrial policy must be balanced with a comprehensive, cross-sectoral cyber resilience design oriented toward mitigating long-term strategic risks.

The main strength of this research lies in its ability to integrate political economy analysis, critical cybersecurity, and institutional governance within a single, coherent analytical framework. This research updates the scientific perspective by demonstrating that the failure of public-private collaboration, the regulatory paralysis of the Cybersecurity and Resilience Bill, and the limitations of cyber diplomacy are not separate issues, but rather interconnected within an ecosystem of structural vulnerabilities. Another significant contribution is the introduction of the concepts of the illusion of digital sovereignty and partial state blindness as analytical lenses for understanding the gap between formal and substantive control over strategic digital systems. However, this research has limitations, particularly in its scope, which focuses on the Indonesian context, a specific strategic industrial sector, and a qualitative approach based on open intelligence documents and reports. Therefore, further research with cross-country comparative coverage, a variety of sectors, and quantitative methods or broader industry surveys is needed to obtain a more comprehensive picture. These efforts are expected to provide a more solid empirical foundation for the formulation of adaptive, inclusive, and targeted national cybersecurity policies in the face of increasingly orchestrated geopolitical cyber threats.

5. REFERENCES

[1] Ambardi, K., Widhyharto, D. S., Madya, S. H., & Wibawanto, G. R. (2025). Masyarakat Digital: Teknologi Kekuasaan dan Kekuasaan Teknologi. UGM PRESS.

[2] Arbani, M. (2024). Pentingnya Badan Intelijen Pertahanan dalam Non-Combat Military Mission: Instrumen Perhatian Khusus untuk Peningkatan Kapasitas dan Kapabilitas Pertahanan. Jurnal Syntax Admiration, 5(5), 1876–1891.

[3] Attaqi, M. F. (2022). Implementasi Kebijakan Luar Negeri Indonesia Dalam Menanggulangi Cyber Crime Melalui Kerjasama Dengan Asean Periode 2019-2021. Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial Dan Ilmu ....

[4] Bagus, J. M. (2025). Dari desa ke dunia maya: Evolusi KIM di tengah transformasi digital. Goresan Pena.

[5] Fadilla, D. I., Azhari, A. F., & SH, M. (2025). Analisis Terhadap Perubahan Undang Undang Komisi Pemberantasan Korupsi Dalam Perspektif Politik Hukum. Universitas Muhammadiyah Surakarta.

[6] Ginanjar, Y. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui Badan Siber dan Sandi Negara. Dinamika Global: Jurnal Ilmu Hubungan Internasional, 7(02), 295–316.

[7] Harahap, S. S., Halkis, M., & Sutanto, R. (2025). Advanced Persistent Threat (APT) sebagai Ancaman Perang Siber Asimetris Terhadap Pemerintah Indonesia. Innovative: Journal Of Social Science Research, 5(3), 4465–4485.

[8] Haryono, I. T. (2025). Peran Stakeholder dalam Kolaborasi Pengembangan Teknologi Pertahanan di Indonesia. Indonesia Emas Group.

[9] Husadi, M. A., & Idris, N. I. (2025). Pencurian Cryptocurrency oleh Aktor Negara sebagai Strategi Hybrid Warfare:(Studi Kasus Kelompok Lazarus). Jurnal Ilmu Komunikasi, Administrasi Publik Dan Kebijakan Negara, 2(2), 143–159.

[10] Khoir, M. I., & Amaliyah, S. (2025). SINKRONISASI NILAI KEARIFAN LOKAL PESANTREN: STANDAR AKREDITASI NASIONAL. PARADIGMA: JURNAL PEMIKIRAN DAN PENELITIAN PENDIDIKAN, 11(2), 160–168.

[11] Koay, A. M. Y., Ko, R. K. L., Hettema, H., & Radke, K. (2023). Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. Journal of Intelligent Information Systems, 60(2), 377–405.

[12] Kusumoningtyas, A. A. (2023). Nexus Pengawasan Siber Sebagai Instrumen Keamanan Nasional dan Relevansinya Dengan Demokrasi: Perbandingan Beberapa Negara. Jurnal Adhikari, 2(3), 416–433.

[13] Matondang, K. A., Shafana, A. N., Butarbutar, G., Avrilya, S. Z., & Sidauruk, V. M. (2026). Dampak Transisi Energi Global dan Strategi Kebijakan Ekspor Energi Indonesia Berdaya Saing. RIGGS: Journal of Artificial Intelligence and Digital Business, 4(4), 2377–2384.

[14] Milia, J., & Attamimi, S. (2025). Dinamika Transfigurasi Tata Kelola Global: Posisi Indonesia dalam Restrukturisasi Lanskap Geopolitik Melalui Ekspansi BRICS. Jurnal Ilmiah Hubungan Internasional Fajar, 3(2), 1–9.

[15] MUNANDAR, H., ST, S., & MFM, M. (2024). Optimalisasi Kerja Sama Sektor Keuangan Digital Guna Meningkatkan Ekonomi Makro Dalam Rangka Ketahanan Nasional. Lembaga Ketahanan Nasional Republik Indonesia.

[16] Najib, A., & Aidil, M. (2025). Strategi Diplomasi Indonesia Dalam Memperkuat Kepemimpinan Di ASEAN Pada Era Geopolitik Yang Berubah. Studia: Journal of Humanities and Education Studies, 1(1), 158–171.

[17] Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dan Hukum, 1(2), 8–16.

[18] Nugroho, S., & Rochmadi, T. (2024). Analysis of Information Security Readiness Using the Index KAMI. Decode: Jurnal Pendidikan Teknologi Informasi, 4(3), 881–886.

[19] Paddu, A. H. (2024). Peta Arah Desentralisasi Fiskal Di Indonesia Outlook Ekonomi dan Ketimpangan Wilayah Indonesia. Kini Dan Esok, 23.

[20] Prabowo, H. (2024). Alternatif Penyelesaian Sengketa Larangan Ekspor Nikel Indonesia Di WTO. PROGRESIF: Jurnal Hukum, 18(1), 42–81.

[21] Septyana, D., Azhari, A. A., Hakim, M. I., Alwassi, R. D., & Novianti, S. (2025). Starlink dan Tata Kelola Ruang Antariksa: Analisis Hukum Internasional terhadap Dual-Use dan Dominasi Orbit. Sanskara Hukum Dan HAM, 4(02), 222–233.

[22] Setyawan, H., SIK, M., POLISI, K. B., PERSEORANGAN, K. K. I., & RI, L. (2023). Penguatan Literasi Digital Guna Menjaga Stabilitas Keamanan Menjelang Pemilu Tahun 2024 Dalam Rangka Ketahanan Nasional. Kertas Karya Ilmiah Perseorangan, Jakarta (Id): Lemhanas.

[23] Siladjaja, M., Nugrahanti, T. P., & Madgalena, P. (2023). Teori akuntansi positif: Sebuah tinjauan pada persepsi berbasis rational decision model terhadap informasi akuntansi berkualitas. Mega Press Nusantara.
[24] Sinaroja, A. S., & Widyoseno, V. R. (2024). Korporatisme Negara dan Ekonomi Privatisasi Terhadap Pembangunan Negara dan Kebijakan Publik. Indonesian Journal of Political Studies, 4(1), 76–89.
[25] Vice, R., Simaremare, N. C., & Manalu, S. (2024). Perkembangan Cybercrime: Dampak Terhadap Keamanan dan Ketahanan Nasional serta Pencegahannya. MIMBAR KEADILAN: Jurnal Ilmu Hukum, 71–83.
[26] Waruwu, M., Puat, S. N., Utami, P. R., Yanti, E., & Rusydiana, M. (2025). Metode penelitian kuantitatif: Konsep, jenis, tahapan dan kelebihan. Jurnal Ilmiah Profesi Pendidikan, 10(1), 917–932.
[27] Wibowo, A. (2024). Riset Kelanggengan Bisnis dalam Ekosistem Digital:(Business Sustainability Research in Digital Ecosystems). Penerbit Yayasan Prima Agus Teknik, 1–266.
[28] Widodo, H., Tjahjadi, B., & Basuki, B. (2022). The Role of Innovation Strategy Mediation in Rivalry Relationships with the Organizational Performance. Journal of Accounting Science, 6(2), 167–186.
[29] Widya, T. R., Cahyadi, D., Christanto, D. A., Giantri, L. T., & Hudzaifah, M. (2025). A conceptual hybrid ai-cloud model for government information systems: A structured literature review. Journal of Applied Informatics and Computing, 9(5), 2640–2651.