JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i3

Strategic Intelligence Analysis on the Urgency of Establishing a Cyber Force in Indonesia

Suwandi[1*], Suhardi[2], Budi Prasetiyono[3], Dwi Surjatmodjo[4], Yanuar Adi Legowo[5].
[1]National Intelligence College, Bogor, Indonesia, sagsuwandi74@gmail.com
[2]Bandung Institute of Technology, Bandung, Indonesia, suhardi@stei.itb.ac.id
[3]National Intelligence College, Bogor, Indonesia
[4]National Intelligence College, Bogor, Indonesia
[5]National Intelligence College, Bogor, Indonesia

[*]Corresponding Author: sagsuwandi74@gmail.com

Abstract: This article examines the urgency of establishing an Indonesian Cyber Force from a strategic intelligence perspective. Cyber threats against national strategic infrastructure continue to escalate, as reflected in billions of detected cyber traffic anomalies in 2025 and the hacking of the Temporary National Data Center (PDNS) in 2024. This study aims to analyze the institutional, regulatory, and cyber defense capacity gaps Indonesia faces amid increasingly asymmetric and difficult-to-attribute threats. A descriptive-analytical qualitative method with a normative-empirical orientation was applied through policy document analysis, statutory review, and in-depth interviews with expert informants in intelligence, defense, and cybersecurity. The results indicate a strategic gap between the escalation of multidimensional cyber threats and the current institutional readiness of Indonesia's defense. The study concludes that establishing a Cyber Force is a logical consequence of the shifting non-conventional threat paradigm. The primary recommendation is a phased approach starting from the consolidation of a unified cyber command to the evolution into an independent fourth branch within the Indonesian National Armed Forces to ensure digital sovereignty and adaptive national resilience.

Keywords: Strategic Intelligence, Establishing Cyber Force, Cyber Force Indonesia

INTRODUCTION

The development of information and communication technology has transformed cyberspace into a new strategic domain in the global security configuration. Cyberspace is now seen as the fifth domain of warfare after land, sea, air, and space (Darumaya et al., 2023). This transformation has shifted the nature of conflict from conventional to asymmetric and hybrid, where attacks can be launched without the physical presence of military forces. In this context, a country's digital infrastructure becomes a strategic target which, if crippled, can have a systemic impact on political, economic, and national defense stability (Sudiantini et al., 2023). Thus, cybersecurity is no longer merely a technical issue, but has transformed into a strategic national defense issue.

In the context of Indonesia, the acceleration of national digitalization through the transformation of electronic government, the digital economy, and the integration of network-based defense systems has increased exposure to cyber threats. Data from the National Cyber and Crypto Agency (BSSN) shows that from January to July 2025, 3.64 billion cyber traffic anomalies were detected in Indonesian cyberspace (Dhanya, 2025). This figure indicates the high intensity of probing, scanning, and potential attacks on national electronic systems. Conceptually, this condition reflects the existence of systemic vulnerabilities that can be exploited by both state actors and non-state actors, including the Advanced Persistent Threat (APT) group. From a strategic intelligence perspective, the high frequency of attacks is an indicator of the increasing risk of escalating threats to digital sovereignty.

The urgency of strengthening Indonesia's cyber defense has become increasingly apparent after the hacking incident at the Temporary National Data Center (PDNS) in Surabaya in 2024, which involved the Brain Cipher group with LockBit 3.0 ransomware (Dewi, 2025). The attack disrupted public services in hundreds of government agencies and led to the leakage of sensitive data. From a strategic intelligence perspective, this incident reflects a failure in early warning and the resilience of vital information infrastructure. Cyber attacks in this context can no longer be categorized solely as cyber crime, but have entered the spectrum of cyber warfare with implications for national security (Rahmawati, 2017). Therefore, a defense approach is needed that is not only defensive but also has credible deterrence capabilities.

Regulatory structures of the Indonesian National Armed Forces (TNI) have consisted of three branches, as stipulated in Presidential Regulation No. 10 of 2010 on the Organizational Structure of the TNI. However, the enactment of Law No. 3 of 2025 concerning Amendments to Law No. 34 of 2004 concerning the TNI has expanded the military's mandate in countering cyber threats as part of Military Operations Other Than War (Yani et al., 2025). However, the strengthening of this mandate has not been followed by the establishment of an integrated cyber command structure in the form of an independent branch. The absence of such a structure has the potential to cause fragmentation of authority and overlapping functions with civilian institutions such as BSSN (Wisyudha et al., 2025).

Based on this background, there is a strategic gap between the escalation of multidimensional cyber threats and the institutional readiness of Indonesia's defense in the cyber domain. Therefore, this study aims to analyze the strategic intelligence urgency of establishing a Cyber Force in Indonesia by examining aspects of threats, regulations, institutional capacity, and military cyber organization models in various countries as comparative material. This analysis is expected to provide conceptual contributions and policy recommendations in formulating an adaptive, integrated, and digitally sovereign national cyber defense design.

METHOD

This study uses a descriptive-analytical qualitative approach with a normative-empirical orientation to analyze the strategic urgency of establishing a Cyber Force in Indonesia. A qualitative approach was chosen because this study aims to gain an in-depth understanding of the dynamics of cyber threats, the construction of defense regulations, and institutional needs from a strategic intelligence perspective, rather than to test quantitative causal relationships (Creswell, 2018). Normatively, this study analyzes national legal and policy documents, particularly Law Number 3 of 2025 concerning the TNI, Presidential Regulation Number 47 of 2023 concerning the National Cyber Security Strategy, and Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure. Empirically, data was obtained through in-depth interviews with expert sources in the fields of intelligence, defense, and cyber security to explore perceptions of the level of threat, capacity gaps, and relevant organizational models. The research was conducted from July 2025 to February 2026.

Data analysis was conducted using an interactive analysis model that included data reduction, data presentation, and systematic conclusion drawing (Miles, Huberman, & Saldaña, 2014). Data from document studies and interviews were coded in a content analysis matrix to identify threat patterns, regulatory dynamics, and institutional needs within a strategic intelligence framework. Conclusions were drawn deductively by integrating empirical findings and intelligence theory, particularly the concept of threat assessment based on the capabilities, intentions, and opportunities of actors (Buzan et al., 1998) to assess the urgency of establishing a Cyber Force as an instrument of national defense. Data validity was maintained through triangulation of sources and methods, as well as confirmation with sources (member checking) to ensure the accuracy of interpretations (Lincoln & Guba, 1985).

RESULTS AND DISCUSSION

The results of the study show that the urgency of establishing a Cyber Force cannot be separated from the paradigm shift in strategic intelligence in facing non-conventional threats. In classical intelligence theory, Sherman Kent defines intelligence as knowledge for policy, namely knowledge that is systematically processed to support high-level decision making (Kent, 1949). Kent emphasized that intelligence is not merely the collection of information, but rather an analytical process aimed at reducing uncertainty in the context of national threats.

The interview findings show that cyber threats to Indonesia are latent, covert, and difficult to attribute quickly. This condition is relevant to the characteristics of modern cyber threats, which often involve state-sponsored actors and operate through Advanced Persistent Threat (APT) schemes. In this context, the eight steps of the analytical process described by Kent, from problem formulation to strategic estimation, are crucial in identifying the intent, capability, and operational patterns of the opponent (Mangio & Wilkinson, 2018).

Scott & Jackson (2004) elaborate that intelligence has three main dimensions: as knowledge, organization, and activity. When applied in the context of establishing a Cyber Force, then:

1. As **knowledge**, the Cyber Force must be able to produce long-term cyber threat assessments;
2. As an **organization**, it requires an integrated command structure;
3. As an **activity**, it must be capable of carrying out both defensive and proactive operations.

Thus, the formation of the Cyber Force is not merely an expansion of the military organization, but rather an epistemological transformation in the way the state understands and responds to digital threats.

Escalation of Cyber Threats

Empirical data shows that the intensity of cyber attacks against Indonesia continues to increase, as reflected in the billions of traffic anomalies detected in the 2025 period (Dhanya, 2025). In addition, the 2024 hacking incident at the Temporary National Data Center (PDNS) exposed the vulnerability of the country's strategic infrastructure (Dewi, 2025). These findings reinforce the argument that cyber threats have gone beyond the category of ordinary digital crime.

Theoretically, Amalia and Atman (2025) emphasize that the core of strategic cyber defense is the ability to attribute. Without credible attribution, countries cannot develop effective deterrence strategies. In many cases, cyber attacks are designed to create ambiguity and plausible deniability, thereby complicating political and military responses.

The interview results show a capability gap in distinguishing between criminal incidents and cyber aggression that could potentially be part of foreign military operations. This gap is the rational basis for the formation of a cyber military structure with advanced technical intelligence capabilities.

Regulatory Evolution and Institutional Gaps

Regulatory-wise, the enactment of Law No. 3 of 2025 expands the TNI's mandate in countering cyber threats as part of Non-War Military Operations (Yani et al., 2025). This policy marks the formal recognition that cyber threats are included in the spectrum of national defense. However, the results of the analysis show that the expansion of this mandate has not been followed by adequate organizational restructuring.

Presidential Regulation No. 47 of 2023 on the National Cyber Security Strategy establishes BSSN as the main coordinator of national cyber security. On the other hand, the TNI has a mandate for national defense. This dualism has the potential to cause overlapping authorities if it is not regulated through a clear command mechanism (Wisyudha et al., 2025).

From a strategic intelligence perspective, institutional fragmentation risks causing information stovepiping, which is the obstruction of information flow between institutions. In the context of a cyber crisis, delays in information sharing can exacerbate the impact of attacks. Therefore, the formation of a Cyber Force needs to be designed with the principles of integration and cross-sector coordination.

International Cyber Organization Model

In recent years, the development of global cyber threats has shown a significant escalation, both in the form of digital espionage, sabotage of critical infrastructure, and information operations that affect the political stability of a country (Dong, et al., 2025). This situation has prompted several countries to reorganize their defense structures by incorporating cyber as a strategic component on par with land, sea, and air domains (Ministry of Defense Central Staff, 2012). Therefore, studying cyber organizational models in various countries is important to understand how these countries respond to new threat dynamics in the era of multidomain warfare. Comparative analysis shows that several countries have adopted different cyber organizational models according to their respective strategic contexts, technological maturity levels, and national security needs.

Singapore: Digital and Intelligence Service (DIS)

Singapore is the most relevant model for Indonesia in the region. With the establishment of DIS as the fourth branch of the Singapore Armed Forces in 2022, Singapore has gone beyond the paradigm of conventional cyber command. Through the establishment of the Digital and Intelligence Service, the country has placed cyber operations, digital intelligence, and information operations as an integrated defense system. The DIS is designed to address hybrid threats by combining military intelligence, cyber security, and psychological defense in a chain of command equivalent to the army, navy, and air force (Wikipedia, 2026).

The advantage of the Singapore model lies in the consolidation of human resources. The DIS actively recruiting civilian cyber talent through the “Military Domain Experts Scheme” and special education programs in collaboration with renowned universities (Wikipedia, 2026). For Indonesia, adopting this fourth domain model is seen as an ideal long-term goal, but it requires the readiness of national cyber range infrastructure and a significant budget (Fitri, 2025).

United States: USCYBERCOM Joint Command

The United States (US) has chosen the Unified Combatant Command model through U.S. Cyber Command, which is closely integrated with the technical intelligence agency, the National Security Agency (Fitri, 2025). USCYBERCOM's mission is broad: defend the Department of Defense network (Defend the DoDIN), support regional commands in combat (Support CCDRs), and defend the nation from cyber attacks that have significant consequences (Defend the Nation) (Billingsley, 2023).

The US implements the Defend Forward doctrine, in which cyber forces operate as close as possible to the source of threats on external networks in order to interrupt enemy activities before they successfully penetrate domestic defenses (Billingsley, 2023). This model provides the military with a high degree of flexibility to conduct proactive cyber operations without having to change the existing basic structure of the armed forces (Fitri, 2025).

United Kingdom: National Cyber Force (NCF)

The United Kingdom formed the National Cyber Force as a strategic alliance between the Ministry of Defense and GCHQ (the British signals intelligence agency) (Fitri, 2025). The NCF emphasizes the use of "responsible cyber power" to support diplomatic and national security objectives in an integrated manner (Harknett, et al., 2023). The British model provides lessons on the importance of avoiding sectoral ego among intelligence agencies, with cyber operations carried out jointly by military and civilian experts in a single adaptive joint task (Fitri, 2025).

Looking at these international models, the findings indicate that there are three strategic options for Indonesia, namely a joint command model, a military-civilian collaborative model, and an independent dimension model. These three options are not only related to organizational design but also concern the transformation of defense doctrine, the integration of the national cyber security ecosystem, and the development of sustainable human resource capacity. In the context of Indonesia, with its complex bureaucracy and increasing digital security challenges, the selection of a cyber organization model needs to be carried out gradually and based on comprehensive strategic intelligence analysis.

Synthesis of Expert Views on the Cyber Force

The discourse on the Cyber Force in Indonesia was deepened through an analysis of the views of three key sources with backgrounds in strategic intelligence, defense academia, and operations, namely A.M. Hendropriyono (former Head of BIN), Anton Nugroho (Rector of Unhan RI), and Guruh Prasetyo Putro (Senior Expert at BSSN). All three provide different but complementary insights in formulating national needs.

Strategic Intelligence Perspective A.M. Hendropriyono (BIN)

Jenderal TNI (Purn.) Prof. Dr. A.M. Hendropriyono, S.T., S.H., M.H., former Head of BIN, views the urgency of the Cyber Force as a response to global geopolitical shifts in the Asia and South China Sea regions, which are considered Indonesia's "backyard." Hendropriyono emphasized that future wars will be asymmetric and hybrid wars, where psychological forces will defeat physical forces. He warned that the current attacks of simulacra and hoaxes are a real form of aggression aimed at destroying the rational thinking of society.

For Hendropriyono, the formation of the Cyber Force should not wait until a physical war breaks out. It must become a "Psychological Force" that exists from the central level to the rural level through integration with regional authorities. He highlighted the success of Singapore and China, which are stable because they have cyber armies capable of preventing disinformation attacks. Hendropriyono proposed that the Cyber Force's ammunition should be "information content," and its organization must be integral in order to ward off enemy narratives that enter through mass and digital media.

Academic Perspective Anton Nugroho (Unhan RI)

Rector of the Indonesian Defense University (Unhan RI) Letnan Jenderal TNI (Purn.) Dr. Anton Nugroho, M.M.D.S., M.A., presented empirical data to support the strategic urgency of establishing a Cyber Force. He referred to the PDN 2024 ransomware incident and the

existence of more than 122 million cyber traffic anomalies in just the first eight months of 2024 as evidence that Indonesia's digital infrastructure is very fragile. Anton argues that there is currently a strategic gap between the real threat and the TNI's response capacity, which is still limited to small units such as Satsiber TNI or Pussansiad.

Academically, Anton recommends a realistic, phased approach. Given the constitutional legal obstacles that limit the TNI to three branches, he suggests the formation of a Special Command at the Kotama level under the TNI Commander as a first step (medium term 5-10 years). This unit could later evolve into an independent branch as human resources and infrastructure become available. Anton also emphasized the importance of integrating the Cyber Force with the Sishankamrata doctrine, whereby military cyber forces must be connected with reserve and support components from the civilian sector and the digital defense industry.

Operational Perspective of Guruh Prasetyo Putro (BSSN)

Senior Expert at the National Cyber and Crypto Agency (BSSN), Guruh Prasetyo Putro, S.ST., M.Si (Han) emphasized the need for a clear separation between the realm of national security (civil) and national defense (military). According to Guruh, cyber incidents that have occurred so far can still be handled by civilian agencies such as BSSN, the Police, and Komdigi because they have not yet touched on physical threats to territorial sovereignty. He believes that a Cyber Force is only really needed when physical warfare occurs, where cyber attacks are used to support the crippling of the enemy's radar or communication systems.

However, Guruh provided a recommended structure if a Cyber Force is eventually formed, proposing that it be led by a Chief of Staff of the Cyber Force (KASAS) who would be equivalent to the chiefs of staff of other branches of the military. In an emergency situation, all national cyber capabilities, including BSSN, the National Police, and even the national hacker community, must be under the sole control of KASAS to ensure the effectiveness of counterattacks (offensive). Guruh's emphasis is on a modern “Code Service”; the Cyber Force must focus on securing encrypted traffic and strategic communications behind the scenes of physical warfare.

Escalation of Threats and Attribution Challenges

Cyber attacks today are no longer just individual hacking actions (such as “script kiddiess”), but rather well-planned operations with large resources, often sponsored by countries Advanced Persistent Threats (APT). Data shows that today's sophisticated malware is very difficult to track and requires a high level of technical intelligence expertise to attribute. Cyber forces are needed to fill the gap in military capacity to identify whether a disruption to national systems is a common criminal act or the beginning of foreign military aggression (Amalia & Atman, 2025).

The hacking of the Ministry of Defense website in November 2023, which resulted in the leakage of personnel data, shows that even defense institutions are not immune to cyber attacks (Wulandari, et al., 2025). Unpreparedness in facing cyber espionage campaigns can lead to the loss of confidential strategic and intelligence documents, which directly weakens Indonesia's diplomatic bargaining position and combat readiness in the region (Astarini & Rofii, 2021).

Recommendations for the Establishment of a Cyber Force

Based on the above strategic intelligence analysis, the establishment of a Cyber Force in Indonesia cannot be done instantly, but rather through measurable stages to ensure organizational readiness and legal legitimacy.

Phase I: Initiation and Consolidation (1-3 Years)

The initial steps should focus on establishing a TNI Cyber Command (Unified Cyber Command) that integrates existing cyber units in each branch (TNI Cyber Unit, Pussansiad, Pussiberal, Pusiberau) (Fitri, 2025). This unit must be given an operational mandate under the TNI Commander with strategic coordination through the Ministry of Defense in accordance with Law No. 3 of 2025 (Wandi, 2025). In this phase, basic infrastructure development such as a national cyber range for training cyber warfare simulations and secure redundant data centers must be prioritized. In addition, intelligence collaboration with BSSN and BIN must be strengthened through the establishment of a national fusion center for real-time threat information exchange (Fitri, 2025).

Phase II: Development of Active Defense Capabilities (3-7 Years)

The Cyber Force must begin to adopt the doctrine of "Active Defense." This includes threat hunting capabilities (hunting for threats within the network before they attack), cyber deception (the use of trap systems), and sinkholing. The main focus is on protecting National Vital Information Infrastructure (IIVN) that has a direct impact on national defense (Fitri, 2025).

The development of limited cyber counterattack (offensive) capabilities must also begin to be researched, but remain under strict political and international legal supervision (Fitri, 2025). Indonesia needs to be active in international cyber diplomacy to formulate norms of responsible state behavior in cyberspace, while strengthening its bargaining power through respected cyber military capabilities in the ASEAN region (Amalia & Atman, 2025).

Phase III: Evolution into a Fourth Branch (10-15 Years)

In the long term, after the legal framework (including possible further amendments to the constitution or the TNI Law), the availability of competent human resources, and stable budgetary support are achieved, the Cyber Command can be evolved into a Cyber Force as an independent fourth branch. This branch will have a complete structure ranging from a cyber military academy, a branch headquarters, to integrated digital regional units in line with the doctrine of the Universal People's Defense and Security System (Sishankamrata).

CONCLUSION

Analysis Based on the results of strategic intelligence analysis, this study concludes that the urgency of establishing a Cyber Force in Indonesia is a logical consequence of the transformation of the threat environment, which is increasingly digitized, asymmetrical, and difficult to attribute. The escalation of attacks on national strategic infrastructure, including the incident at the Temporary National Data Center (PDNS), shows that cyberspace has become an arena of contestation that directly impacts the stability of the government and the sovereignty of the state. In this context, cyber threats can no longer be positioned as a technical administrative issue, but rather as an integral part of the spectrum of national defense.

An analysis based on the strategic intelligence paradigm as proposed by Kent (1949) shows that a country's response to cyber threats must be based on the ability to produce accurate, integrated, and uncertainty-reducing strategic knowledge. The main challenges faced by Indonesia lie in the gap in attribution capacity, institutional fragmentation between civilian and military actors, and the limited availability of advanced cyber talent. The expansion of the TNI's mandate through Law Number 3 of 2025 has provided a legal basis for military involvement in the cyber domain, but this has not been followed by an organizational design capable of comprehensively integrating cyber defense functions.

International comparative studies show that countries such as the United States, the United Kingdom, and Singapore have adopted military cyber organization models tailored to

their respective strategic needs. These findings indicate that Indonesia has several institutional options, ranging from the formation of a joint cyber command to the evolution towards an independent branch. However, the formation of a Cyber Force should be carried out in stages, taking into account regulatory readiness, civilian supremacy, human resource capacity, and integration with the National Cyber Security Strategy.

Thus, the formation of a Cyber Force is not merely a structural agenda, but part of a broader strategy to strengthen national resilience in the digital age. Its success will largely depend on the state's ability to build coordinated governance, develop sustainable cyber talent, and apply the principle of balance between defensive capabilities and measurable deterrence mechanisms. From a long-term defense perspective, investment in the cyber domain is an investment in the sustainability of Indonesia's digital sovereignty.

REFERENCE

Aji, M. P. (2025). Cybersecurity Politics in Building Cyber Sovereignty in Indonesia Through Strengthening the Role of the National Cyber and Crypto Agency. Society, 13 (2), 1056-1071, 2025. DOI: 10.33019/society.v13i2.960

Amalia, A.F., Atman, W. (2025). Strategi Detterence Siber Indonesia terhadap Ancaman Proxy State Actor. Aliansi : Jurnal Hukum, Pendidikan dan Sosial Humaniora. Volume. 2, Nomor. 4 Juli 2025. DOI: https://doi.org/10.62383/aliansi.v2i4.1116

Astarini, D.R.S., Rofii, M.S. (2021). Siber Intelijen Untuk Keamanan Nasional. Jurnal Renaissance. Vol. 6 No. 01, Mei 2021. https://media.neliti.com/media/publications/483678-none-5fc012c1.pdf

Billingsley, J.L. (2023). Integrated Deterrence and Cyberspace. National Defense University Press, Washington, D.C. https://ndupress.ndu.edu/Portals/68/Documents/strat-monograph/Integrated-Deterrence-and-Cyberspace.pdf

Budiman, M. R. (2016). Optimalisasi Peran Badan Intelijen Negara (BIN) Dalam Mengawal Keamanan Negara Berdasarkan Undang-Undang Nomor 17 Tahun 2011 Tentang Intelijen Negara. Tesis. Universitas Islam Indonesia.

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). SAGE Publications.

Darumaya, B.A., Maarif, S., Toruan, T., Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan, JURNAL KEAMANAN NASIONAL, Vol. IX No. 2 (2023): pp. 299-324

Dhanya, D. (2025, 8 Agustus). Indonesia's BSSN Records 3.64 Billion Cyberattacks in First Half of 2025. Tempo. https://en.tempo.co/read/2037469/indonesias-bssn-records-3-64-billion-cyberattacks-in-first-half-of-2025

Diaz, G. (2005). Methodological Approaches to The Concept of Intelligence Failure. UNISCI Discussion Papers, No. 7, Tahun 2005, pp. 1-16. Universidad Complutense de Madrid, Spanyol. https://www.redalyc.org/pdf/767/76711286004.pdf

Dong, J., Chen, S., Ding, F. et al. (2025). Spatiotemporal characteristics and drivers of global cyber conflicts. Humanit Soc Sci Commun 12, 665. https://doi.org/10.1057/s41599-025-04897-7

Fitri, A. (2025). Peran TNI Dalam Keamanan Siber: Perlukah Pembentukan Angkatan Siber?. Info Singkat. Vol. XVII, No. 15/I/Pusaka/Agustus/2025. https://berkas.dpr.go.id/pusaka/files/info_singkat/Info%20Singkat-XVII-15-I-P3DI-Agustus-2025-1947.pdf

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara. Jurnal Dinamika Global Vol.7 No. 2, Desember 2022. https://doi.org/10.36859/jdg.v7i02.1187

Harknett, R.J., Fischerkeller, M.P., Goldman, E.O. (2023). U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory. Institute for Defense Analyses, Virginia. https://apps.dtic.mil/sti/trecms/pdf/AD1211210.pdf

Hartati, S., Rubiyanto. (2025). Implikasi Uji Materi Undang-Undang No 3 Tahun 2025 Terhadap Prinsip Pemisahan Kekuasaan dan Wewenang Sipil Militer Implications. Jurnal Kolaboratif Sains, Volume 8 No. 10, Oktober 2025. DOI: 10.56338/jks.v8i10.8943.

Indonesia. (2023). Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Lembaran Negara Republik Indonesia Tahun 2023. Jakarta. https://jdih.tanjungpinangkota.go.id/cariprodukhukum/2719

Kent, Sherman. (1949). Strategic Intelligence for American World Policy. Princeton, Princeton University Press, Preface.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Beverly Hills, CA: Sage.

Lim, K. (2016). Big Data and Strategic Intelligence. Intelligence and National Security, 31(4), 619–635. https://doi.org/10.1080/02684527.2015.1062321

Mangio, C.A., & Wilkinson, B.J. (2018). Intelligence Analysis: Once Againlocked. Oxford Research Encyclopedia of International Studies. https://doi.org/10.1093/acrefore/9780190846626.013.451

Miles, M.B., Huberman, A.M. and Saldana, J. (2014) Qualitative Data Analysis: A Methods Sourcebook. Sage, London.

MKRI. (2025). Permohonan Pengujian Formil dan Materiil atas Undang-Undang Nomor 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia. https://www.mkri.id/public/filepermohonan/Permohonan_4309_8284_Permohonan_redact.pdf

Salim, B. (2025). Undang Undang Nomor 3 Tahun 2025 Revisi Undang Undang Nomor 34 Tahun 2004 Tentang Tentara Nasional Indonesia Dalam Pendekatan Interdisipliner. Jurnal Multidisiplin Ilmu Akademik. Vol.2, No.4 Agustus 2025. DOI: https://doi.org/10.61722/jmia.v2i4.6710

Samad, M. Y. & Persadha, P. D. (2022). Pendekatan Intelijen Strategis Sebagai Upaya Memberikan Perlindungan di Ruang Siber Dalam Konteks Kebebasan Menyatakan Pendapat. https://jurnal.dpr.go.id/index.php/kajian/article/download/3588/1071

Scott, L. & Jackson, P. (2004). The Study of Intelligence in Theory and Practice. Intelligence & National Security. 19:2, 139-169, DOI: 10.1080/0268452042000302930

Sefiana, A.P. (2026, 28 Januari). Serangan Siber Indonesia dan Ancaman "Digital Pearl Harbor", Saat Negara Bisa Lumpuh Tanpa Perang dan Tanpa Satu Peluru Ditembakkan. Jawapos. https://trenggaleknjenggelek.jawapos.com/hukum-kriminal/2597112013/serangan-siber-indonesia-dan-ancaman-digital-pearl-harbor-saat-negara-bisa-lumpuh-tanpa-perang-dan-tanpa-satu-peluru-ditembakkan

Sudiantini, D., Ayu, M.P., Aswan, M.C.A.S., Prastuti, M.A., Apriliya, M. (2023). Transformasi Digital : Dampak, Tantangan, Dan Peluang Untuk Pertumbuhan Ekonomi Digital. Trending: Jurnal Ekonomi, Akuntansi dan Manajemen. Vol.1, No.3 Juli 2023. https://doi.org/10.30640/trending.v1i3.1115

The ministry of Defense Central Staff. (2012). THE DEFENCE CYBER STRATEGY. Netherlands Ministry of Defence. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Netherlands_2012_NDL-Cyber_StrategyEng.pdf

Wandi. (2025, 20 Maret). Revisi UU TNI 2025: Siap Hadapi Ancaman Siber, Usia Pensiun Perwira Tinggi Naik Jadi 65 Tahun, diakses Februari 22, 2026, https://infopublik.id/kategori/nasional-politik-hukum/910732/revisi-uu-tni-2025-siap-hadapi-ancaman-siber-usia-pensiun-perwira-tinggi-naik-jadi-65-tahun

Wikipedia. (2026, January 17). Digital and Intelligence Service. Wikipedia. https://en.wikipedia.org/wiki/Digital_and_Intelligence_Service

Wulandari, R., Priyanto, Hendra, A. (2025). The Indonesia's Cyber Security Strategy in the Face of Evolving Modern Warfare Threats. Formosa Journal of Applied Sciences (FJAS). Vol. 4, No.2 2025: 615-626. DOI: https://doi.org/10.55927/fjas.v4i2.5

Yaputra, H., Izzuddin, H., Yusrial, M. R. (2025, 25 Maret). Kontroversi Pelibatan Tentara Hadapi Ancaman Siber dalam UU TNI. Diakses Februari 22, 2026, https://www.tempo.co/politik/kontroversi-pelibatan-tentara-hadapi-ancaman-siber-dalam-uu-tni-1224841