A Comprehensive Cyber Defense Framework for the Indonesian National Armed Forces: Bridging Governance Gaps for National and ASEAN Cyber Resilience

Timothy Shives and Fibriansyah Fatahillah
Naval Post-graduate School, Monterey, California, USA

timothy.shives@nps.edu
fibriansyah.fatahillah.id@nps.edu

Abstract: Indonesia's National Data Center (*PDN*) was targeted by a ransomware attack on June 20, 2024, paralyzing 210 government agencies, causing manual immigration procedures, and exposing significant weaknesses in Indonesia's cyber governance system. The National Cyber and Crypto Agency (*BSSN*) was mandated under Presidential Regulation 47/2023 to coordinate the response, but the response operation remained disorganized due to various agencies working independently without a unified leadership system, including the Indonesian National Armed Forces (*TNI*) operating independently despite possessing a Cyber Unit (*Satsiber*) with adequate cyber warfare capabilities. The attack on the *PDN* ultimately revealed three governance weaknesses: a lack of a unified command system for conducting national-scale response operations, the separation of military resources from the protection of civilian infrastructure, and a systemic failure to maintain adequate operational readiness. Through a comparative analysis of cyber command models in the United States, Singapore, South Korea, and Australia, combined with an institutional assessment using the McKinsey 7S and NIST frameworks, we propose an integrated defense architecture. The establishment of a Joint Cyber Defense Task Force (JCDTF) operating under a proposed civilian-military organization, the National Cyber Security Coordination Center (NCCC), would create a single command system for crisis response and maintain democratic civilian control through established legal authority, mandatory parliamentary oversight, and limitations on operational areas. This framework would address existing governance weaknesses through democratic cyber governance principles that can also be used by ASEAN countries to address their civil-military integration challenges in handling national-scale cyber incidents.

Keywords: Cyber resilience, Cyber governance, Civil-military relations, Indonesia, ASEAN, Crisis management

1. Introduction

A cyber incident was discovered when immigration officers at Soekarno-Hatta International Airport found their systems encrypted by ransomware upon arriving at the airport at 8:00 AM on June 20, 2024 (Azhar, 2024). The attack, carried out by Brain Cipher, caused 210 government agencies to lose access to critical database systems as it spread through Indonesia's National Data Center (*PDN*) within hours (Antoniuk, 2024). The government refused to pay the $8 million ransom demand but required several weeks to recover their data by performing a manual cloud migration to a commercial cloud service (Karmini, 2024; Nugroho, 2024). The attack revealed that governance weaknesses extended beyond the actual technical intrusion, as various agencies failed to coordinate their response to the cyberattack, there was no single command center, and Indonesia's main defense organization, the Indonesian National Armed Forces (*TNI*), was not included in the national cyber emergency response system (Nugroho, 2024).

This research aims to determine what kind of institutional framework can integrate military cyber operations into Indonesia's defense system while maintaining civilian control over the government. The *PDN* attack provides evidence to support this research by demonstrating specific governance weaknesses that necessitate changes in the current organizational structure. The Indonesian government has introduced a draft Cyber Security and Resilience Bill (*RUU KKS*) intended to create well-defined institutions capable of addressing future cyber challenges, but the bill faces challenges of institutional fragmentation due to the lack of a unified operational body (Lebang, 2025).

We propose a Joint Cyber Defense Task Force (JCDTF) operating within the National Cyber Security Coordination Center (NCCC) as an integrated architecture to address the identified failures. This framework aims to maintain operational efficiency while ensuring democratic oversight through defined legal authority, a civilian-military management system, and programs to develop the technical skills of personnel in the cyber domain.

2. Fragmented Indonesian Cyber Governance

Indonesia's current cybersecurity institutions function as separate entities that appear to compete rather than cooperate. The National Cyber and Crypto Agency (*BSSN*) began operations in 2017 based on Presidential Regulation 47/2023, which established an organization to coordinate activities related to cryptography and cybersecurity, but limited its operational scope to only 400 staff working on policymaking (SSEK Law Firm, 2024).

Meanwhile, the Ministry of Communication and Information (*Kemkomdigi*), as the body operates the government's IT infrastructure through the National Data Center (*PDN*), operates its own security management system without cooperation with *BSSN* (Lebang, 2025). On the other hand, the Indonesian National Police (*Polri*) use its Cyber Crime Unit to conduct investigations into cybercrimes. And the State Intelligence Agency (*BIN*) conducts cyber intelligence operations through its own protected and confidential operational system (IISS, 2021).

TNI maintain their own cyber operations through the *TNI* Cyber Unit (*Satsiber*), established in 2017 to defend military C4ISR networks with approximately 150-200 personnels (IISS, 2021; Priyandita & Lebang, 2025). The military follows a separate command structure because Indonesia placed civilian control over its armed forces after the democratic transition in 1998. This separation between civilian and military organizations supports democratic development, but it creates operational weaknesses when cyberattacks affect both sectors (Putra et al., 2022).

Reflecting on the *PDN* incident, Indonesia is proposing a draft Cybersecurity Bill (*RUU KKS*)in 2025 that would give *BSSN* new powers to control content and manage AI systems as well as conduct criminal investigations, but this would create jurisdictional disputes with *Kemkomdigi* and *Polri*, while the *TNI*'s responsibility to participate in national cyber defense remains unclear (Lebang, 2025). Legislative methods address regulatory issues, but do not solve the problem of how to integrate both civilian and military operations for national-scale cyber crisis response management.

3. Theoretical Framework

Crisis management theory defines a crisis as an urgent threat that endangers the core elements of a system, while leaders must make decisions under conditions of uncertainty and time constraints (Boin et al., 2016). Effective response requires organizations to perform five critical tasks: situational awareness to understand the circumstances, decision-making to choose actions, coordination for alignment among agencies, information dissemination to the public, and learning for the implementation of lessons learned. The *PDN* attack met all the requirements for a crisis, but Indonesia's disorganized governance system made the execution of these tasks difficult.

A governance system composed of many complex elements requires coordination that goes beyond the process of distributing official positions (Peters, 2015). The lead agency model achieves success when organizations understand each other's needs and the coordinator possesses the appropriate knowledge, and there are established relationships between the relevant parties, and all teams have experience with established procedures. Presidential Regulation 47/2023 designated *BSSN* to coordinate cyber-related activities, but the regulation was not accompanied by efforts and processes to create the fundamental elements for *BSSN* to function as a lead agency, leading to a situation where coordination exists only in name, but operations remain separate.

Civil-military integration in the cyber domain faces unique challenges related to translation issues. Boeke (2015) points out that kinetic warfare doctrines fail to translate effectively into cyber operations because these operations operate without clear territory and are difficult to trace to their origins, and do not distinguish between military and civilian targets (Dunn Cavelty, 2014; Rid, 2012). Democratic control systems require civilians to acquire technical capabilities that allow them to conduct successful oversight, rather than allowing the armed forces to operate independently due to information gaps (Feaver, 2005). The Indonesian government faces a dilemma between using its armed forces for national cybersecurity defense and protecting the democratic constitution from erosion that could occur through military expansion into internal surveillance activities.

4. Methodology

This research combines several qualitative research methods, including case study analysis, comparative research, and institutional framework development. The *PDN* attack revealed critical evidence of governance weaknesses requiring fundamental organizational change. The attack timeline and inter-agency response patterns emerged from process tracing that analyzed documents from open sources including government press releases, Indonesian and international media coverage, technical security analyses, and academic commentary. Researchers used various sources to confirm the precise timing of events, where they coded data for timestamps, actor attribution, type of action, and outcomes.

This research evaluates the integration of cyber command through a comparative study of four democratic countries that demonstrate advanced integration models and have strategic importance for Indonesia: the United States, Singapore, South Korea, and Australia. The analysis revealed common operational methods for civilian supremacy but showed two distinct command structures and specific elements that influence the ability to transfer knowledge.

The framework synthesis method applied the McKinsey 7S organizational assessment to identify weaknesses in the Indonesian National Armed Forces' cyber capabilities by analyzing the dimensions of strategy, structure, systems, shared values, skills, staff, and style (Waterman et al., 1980). And the NIST Cybersecurity Framework 2.0 established the operational architecture supporting the proposed institutional design (National Institute of Standards and Technology, 2024). This analysis relies on publicly available data due to a lack of access to classified assessments, internal communications, and complete forensic evidence. The proposed framework requires empirical verification through stakeholder feedback collection, scenario testing, and legal assessment of its compatibility, which should be studied by future researchers.

5. *PDN* Attack: A Governance Crisis

5.1 Timeline and Impact of the Attack

The Brain Cipher ransomware variant, linked to the LockBit family, encrypted the *PDN* system on June 20, 2024, affecting 210 government institutions (Antoniuk, 2024). The sudden shutdown of immigration services forced staff to process passports manually, leading to increasingly long delays at international airports (Reuters, 2024). The government decided to refuse the ransom payment on June 24 after four days of negotiations, but the recovery process faced various challenges that lasted for more than four weeks (Karmini, 2024; Meyer, 2024). Government organizations undertook an emergency cloud migration with a commercial provider because their backup systems were inadequate, resulting in data security threats and exposing their weak crisis recovery capabilities (Nugroho, 2024). Technical analysts indicated that the attackers must have maintained a connection for several days before they activated the encryption, as they needed time to collect data and distribute their ransomware throughout the system infrastructure, proving that the government's monitoring systems failed to detect the breach (Antoniuk, 2024).

5.2 Critical Governance Failures

The first critical governance failure occurred due to the lack of an organized command structure during the incident and system recovery. Although *BSSN* had been designated as the national cyber coordinator, publicly available information indicates that the response system remained uncoordinated and siloed. During the crisis, *BSSN's* role remained largely invisible to the public, in contrast to officials from the Ministry of Communication and Information Technology (*Kemkomdigi*) who received most of the media attention for their work in recovery initiatives (Azhar, 2024). The government took four days to announce its refusal to pay the ransom, indicating that they lacked established policies and protocols for such situations. There is no evidence to suggest that *BSSN* directed inter-agency operations or formed a unified crisis command. The agencies released separate public statements instead of issuing a single message through a coordinated effort, further proving the failure of their coordination system despite having an official framework for collaboration on national cyber issues. *BSSN*, in its position as the official control authority, was deemed lacking in the technical capabilities to direct the handling of the cyber incident, leading several institutions to operate independently because they possessed sufficient resources to manage infrastructure systems (*Kemkodigi*) and conduct investigations (*Polri*).

The second failure was the exclusion of the Indonesian National Armed Forces (*TNI*) from the national response. *TNI* possesses cyber capabilities capable of providing network defense capabilities and forensic analysis and incident response expertise to defend their military C4ISR systems (IISS, 2021). Public records contain no evidence that *TNI* personnel were involved in the *PDN* incident response operations, primarily because the institution operates independently from the democratic changes that occurred after 1998, not due to a lack of capability. Indonesia lacks established legal procedures to allow the military to assist civilian infrastructure during a national cyber emergency. The military's response to and involvement in natural disasters through search and rescue assistance demonstrates an anomaly in the cyber domain, as defense institutions are not involved in protecting national infrastructure. Military technical expertise becomes useless as civilian agencies struggle to recover from such events, illustrating how separate organizational structures lacking operational integration result in additional costs and national-scale effects.

The government failed to achieve operational readiness, leading to a third major failure, where the attacks revealed that the government failed to build adequate protection against its various operational vulnerabilities.

Monitoring systems were unable to identify the attackers, who remained in the system for several days during the reconnaissance phase until end-users reported the problem, rather than the central cybersecurity operations center detecting it. Backup systems failed to function properly, requiring organizations to spend weeks recovering their data instead of using backups for rapid recovery. The ad-hoc approach to commercial cloud migration demonstrated a lack of a disaster recovery plan, and there is no public evidence that previous joint exercises to train inter-agency coordination during cyber crises had a positive effect in accelerating reaction or recovery time from incidents. The recovery period, lasting several weeks, indicates that Indonesia has focused its efforts more on developing regulatory frameworks than on building operational resilience capabilities.

Table 1: International Cyber Command Integration Models

Dimension	United States	Singapore	South Korea	Australia	Indonesia Implication
Command Structure	Unified USCYBERCOM dual-hatted with NSA	Separate military branch (DIS) coordinated with CSA	Military subordinate to NIS oversight	Federated across services with DSPF principles	Unified command reduces fragmentation seen in *PDN* response
Civilian Oversight	Congressional committees plus DoD civilian leadership	Cabinet-level coordination through Total Defence framework	Parliamentary reporting requirements to NIS committees	Defence Minister authority through DSPF	Multiple oversight mechanisms prevent military autonomy
Legal Authority	Title 10 (military) versus Title 50 (intelligence) separation	Defence Act amendments creating DIS statutory basis	National Intelligence Service Act provisions	Defence Act plus DSPF framework	RUU KKS requires explicit *TNI* cyber role authorization
Operational Doctrine	Persistent Engagement and Defend Forward proactive posture	Total Defence integration across domains	Offensive capability development for deterrence	Principles-based mission-adaptive approach	Doctrine development must precede structure creation
Personnel Management	Cyber Mission Force with specialized career tracks	DIS direct recruitment with hybrid civil-military staffing	Military cyber specialist retention programs	Flexible civilian-military teaming arrangements	*TNI* needs dedicated cyber career path preventing rotation losses

6. International Models for Integrated Cyber Command

The comparative analysis shows different methods which allow military cyber operations to function under civilian authority while maintaining democratic oversight. The United States Cyber Command achieves unified command effectiveness through its single authority which controls offensive and defensive operations and intelligence functions while operating under civilian Department of Defense leadership and congressional oversight (US Cyber Command, n.d.). The Digital and Intelligence Service of Singapore operates as a regional military cyber force model which unites with the civilian Cyber Security Agency through Total Defence framework to achieve national defense coordination (Fitriani, 2023; Singapore MINDEF, 2025). The National Intelligence Service of South Korea controls military cyber operations through its oversight system which requires parliamentary disclosure of all activities (Wood, 2024). The Australian Department of Defence (2025) established the Defence Security Principles Framework which uses principles to guide decision-making instead of creating specific rules that allow military operations to adjust while staying within limits set by civilian authorities.

The research reveals multiple recurring patterns which appear throughout all studied cases (Table 1). The four democracies uphold civilian control through separate institutional systems which include US legislative oversight and Singapore and Australia use ministerial control and South Korea depends on intelligence agency coordination (Feaver, 2005). The United States and Singapore operate under unified command systems which differ from Australia's federated system because Indonesia's *TNI* joint command structure appears to support a centralized command structure (Indonesian Ministry of Defence, 2015). The development of operational doctrine before or at the same time as organizational structures proved essential for successful cases which makes Indonesia's current lack of doctrine its most critical problem (Priyandita & Lebang, 2025)

7. Proposed Framework: JCDTF and NCCC

7.1 Diagnostic Assessment of *TNI* Cyber Capabilities

The McKinsey 7S analysis shows that *TNI* cyber mission operations do not align with the current organizational structure because of seven different factors (Table 2). The assessment shows that structural changes by themselves do not solve problems because organizations need to transform their entire strategy and culture and workforce structure.

Table 2: McKinsey 7S Assessment of *TNI* Cyber Readiness

Element	Current Status	Critical Gap
Strategy	Reactive perimeter defense	Lacks Defend Forward or active defense doctrine; focus solely on C4ISR protection (Priyandita & Lebang, 2025)
Structure	Siloed from national governance	Cyber Unit isolated from *BSSN* decision-making; limited integration with civilian intelligence
Systems	Fragmented coordination	No unified incident response platform with civilian CERTs; manual coordination during *PDN* attack
Shared Values	Conventional warfare culture	Institutional prioritization of kinetic operations over digital domain; cyber viewed as support function
Skills	Critical shortages	Deficit in forensic analysts and reverse engineers; reliance on generalist IT staff versus specialists
Staff	Understrength at ~40% manning	Rigid rotation policies prevent specialization retention (Antara News, 2025)
Style	Hierarchical command	Top-down structure slows decision-making speed required for cyber incident response

7.2 National Cybersecurity Coordination Centre (NCCC)

The NCCC would serve as a single operational command center which would handle national cyber emergencies to solve the current problem of insufficient coordination that occurred during the *PDN* attack (Nugroho, 2024). The senior civilian director at *BSSN* or ministerial level would take charge of the operation while deputy directors from *TNI* (JCDTF Commander), *BIN*, *Polri* and *Kemkomdigi* would provide support. The *RUU KKS* amendments through statutory authority would allow crisis management during declared cyber emergencies by controlling member agencies while preserving their regular duties for planning and exercise activities and information exchange (Lebang, 2025).

The NCCC must deliver reports to the National Security Council which should contain quarterly briefings for parliament members together with classified operation information in distinct sections (Wood, 2024). Organizations can protect their operational security through annual public threat assessments which also enable them to share complete information with the public (Australian Department of Defence, 2025). The established framework solves *BSSN*'s present authority-capability problem through its creation of legal command authority which draws operational strength from member agency capabilities (SSEK Law Firm, 2024).

7.3 Joint Cyber Defense Task Force (JCDTF)

The JCDTF operates as *TNI*'s primary cyber force which operates through two different command systems: The *TNI* Commander exercises tactical control for military operations, and NCCC maintains operational control for supporting civilian infrastructure (Boeke et al., 2015). The dual subordination system enables organizations to merge their operational capabilities with democratic supervision (Feaver, 2005).

The organizational structure includes three specific elements which follow the US Cyber Mission Force architecture design but maintain proportions suitable for this organization (US Cyber Command, n.d.). The National Defense Teams (NDT) would create fast response systems to assist civilian organizations during major emergencies including the *PDN* attack through NCCC-approved activation for forensic analysis, data recovery and critical infrastructure hardening (Nugroho, 2024). The Combat Support Teams (CST) would unite cyber warfare capabilities with standard *TNI* military operations which would span all three branches of the military including Army and Navy and Air Force (Indonesian Ministry of Defence, 2015). The Force Protection Teams (FPT) would protect *TNI*'s fundamental mission to defend military C4ISR networks through their work of network monitoring and vulnerability testing and threat intelligence gathering and security operation management (IISS, 2021).

The organization will consist of 60% military personnel and 30% civilian technical experts and 10% contractors. The hybrid model solves talent shortages through its ability to create local expertise (Abdurrachman et al., 2024). Personnel management reforms prove essential because they will establish dedicated cyber career paths which extend service periods to 4-5 years instead of typical 2-year assignments to maintain specialized skills and offer 1.5 times standard pay rates to draw candidates and allow civilian experts to join through lateral entry programs and universities can establish recruitment pipelines.

The explicit authorities together with defined limitations serve to stop the expansion of mission scope (Dunn Cavelty, 2014). JCDTF would have complete power to protect *TNI* networks while it would only support civilian infrastructure through *BSSN* Director authorization after receiving a request from NCCC. The organization would perform offensive cyber operations only through presidential authorization which requires National Security Council evaluation (Lebang, 2025). The organization would work with *BIN* to gather intelligence, but *BIN* would keep its main authority to collect intelligence (IISS, 2021). The organization would help *Polri* with technical support during their investigations, but law enforcement agencies would continue to handle all prosecution matters. The established boundaries enforce civilian primacy through direct legal restrictions which replace the need for voluntary self-control (Feaver, 2005).

7.4 Implementation Requirements

The legal system requires RUU KKS to undergo amendments which will establish NCCC as a crisis command center and JCDTF for military network defense and civilian support operations and to create parliamentary oversight systems and prohibit all unauthorized offensive operations (Lebang, 2025). The total budget for five years of implementation needs to be prepared which includes establishment costs for personnel recruitment, training, secure infrastructure, systems, and tools also for annual steady-state operations for personnel, operations, and for modernization. The funding sources for this initiative consist of *TNI* budget reallocation and newly appropriations, international partnerships with US, Australia, South Korea or Singapore and commercial threat intelligence cooperation (Fitriani, 2023).

The NCCC needs to conduct quarterly joint exercises to check its operational readiness because these exercises help assess its coordination systems and create crisis management protocols which determine decision roles and communication methods and set up vital backup systems for infrastructure and continuous improvement through learned lessons. The preparedness investments work to solve the readiness problems which *PDN* attack revealed (Nugroho, 2024).

8. Discussion

8.1 Addressing Democratic Governance Concerns

The military needs to operate within its authorized boundaries because Democratic control mechanisms have created various protective systems. Civilian NCCC director maintains operational authority over JCDTF civilian support missions. The parliamentary oversight committee conducts thorough reviews through its internal technical staff instead of performing typical inspection procedures. The law establishes two types of restrictions which block both home-based surveillance activities and self-operating military attacks. The organization maintains transparency through its annual public reports which show its operational activities and budget usage and capability growth. The protection system for whistleblowers enables staff members to report violations while guaranteeing they will not experience any form of retaliation. The United States and Australia along with other democratic cyber forces operate as international partners which demonstrate their professional military culture through their commitment to civilian control. The system requires structural controls, but these controls do not fully meet all requirements. *TNI* needs professional military education which teaches soldiers about democratic governance through civil-military relations and leadership development that focuses on self-control and responsibility instead of independence. The military should use international exercises to teach its members about democratic values through socialization programs. The process of building civilian capacity stands as an equally important requirement because *BSSN* technical workforce development through training and recruitment and retention practices enables effective oversight instead of information-based rubber-stamping (Aulianisa & Indirwan, 2020). The assessment process receives independent evaluation from technical advisory boards which consist of academic and private sector experts.

8.2 Limitations and Future Research

The framework solves governance deficiencies which researchers discovered through their analysis of *PDN* attack data and their comparison of different systems but needs testing in real-world settings. The research

agenda for future development needs to conduct semi-structured interviews with *TNI*, *BSSN*, BIN and Polri officials which will help assess framework usability and identify barriers to execution. The operational readiness assessment needed by conduct tabletop exercises which will stress test the NCCC coordination on crisis to verify system performance before deploying the full system. The legal assessment of constitutional compatibility with public law evaluation of dual-reporting military structures would protect democratic legitimacy. The analysis of political economy would help identify which organizations oppose authority consolidation and what motivates them to change their opposition which would guide the implementation process.

The framework also needs political support to achieve long-term success because its success requires continuous implementation after the initial establishment of its structural components. The democratic institutions of Indonesia need to maintain their focus on civilian oversight because military autonomy becomes more attractive because of technical difficulties. The analysis of regional effects needs to evaluate ASEAN norms which include non-interference so Indonesia should maintain transparency through its participation in the ASEAN Defence Ministers' Meeting (ADMM) cyber working group, its conduct of defensive military exercises and voluntary assessment programs instead of forcing integration models on neighboring countries with different political structures.

9. Conclusion

The June 2024 *PDN* ransomware attack revealed three core weaknesses in Indonesia's cyber defense governance system because the country operated without a single command center despite creating coordination protocols and because it did not combine military assets with civilian infrastructure protection and because its operational readiness remained insufficient. The institutions failed to stop these disasters because they dedicated their efforts to managing regulations instead of creating proper crisis management infrastructure. The US, Singapore, South Korea and Australia have different models which could prove that within democracies system they can merge their military cyber forces into their existing structures while keeping civilian control. The JCDTF/NCCC framework which the authors propose implements these principles into Indonesia's current institutional framework by having NCCC lead operations under civilian control while JCDTF reports to both organizations. The operationalization of democratic accountability depends on four elements which include explicit legal authorities and parliamentary oversight and prohibited capabilities and civilian technical capacity building.

The research evaluates *PDN* governance failures through complete assessment while it evaluates different integration frameworks to develop specific organizational designs which fix the identified weaknesses. The framework requires empirical testing through stakeholder participation and scenario-based evaluation to confirm its design methodology which derives from theoretical concepts. The success of implementation depends on continuous political support which must focus on developing capabilities and maintaining democratic monitoring systems.

The institutional framework of Indonesia needs to establish a system which unites operational performance with public oversight for digital sovereignty protection. The *PDN* attack created an opportunity for Indonesia to use for protecting its national cyber security systems while showing democratic leadership in ASEAN's digital transformation process. The dialogue needs to move away from emergency response work toward building permanent institutions.

Acknowledgements

The authors express sincere gratitude to the Naval Postgraduate School for academic guidance and resources, and to LPDP for sponsorship.

Ethics Declaration: This research was conducted using publicly available data, including government reports, academic papers, and news articles. As such, it did not involve human subjects or confidential data, and formal ethical clearance was not required.

AI Declaration: Open-source artificial intelligence tools were used solely for proofreading and citation formatting. All analysis, arguments, and conclusions presented in this paper are the original work of the authors or are derived from appropriately cited sources.

References

Abdurrachman, F., Suharjo, B., & Biantoro, Y. (2024). Building The TNI's Defense Posture In Cyberspace: Strategies For Dealing With Cyber Warfare In The Digital Era. IJPSAT, 48(1), 451–461.

Antara News. (2025, February 3). TNI to continue cyber defense training for soldiers. https://en.antaranews.com/news/343530/tni-to-continue-cyber-defense-training-for-soldiers
Antoniuk, D. (2024, June 24). Indonesia's national data center encrypted with LockBit ransomware variant. The Record. https://therecord.media/indonesia-national-data-centre-hacked
Aulianisa, S. S., & Indirwan, I. (2020). Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia. Lex Scientia Law Review, 4(1), 33–48. https://doi.org/10.15294/lesrev.v4i1.38197
Australian Department of Defence. (2025, May 30). Defence Security Principles Framework | Defence. https://www.defence.gov.au/business-industry/industry-governance/defence-security-principles-framework
Azhar, M. (2024, June 25). Cyberattack on Indonesia's national data centre paralyses government services [Online post]. GovInsider. https://govinsider.asia/intl-en/article/cyberattack-on-indonesias-national-data-centre-paralyses-government-services
Boeke, S., Heinl, C. H., & Veenendaal, M. A. (2015). Civil-military relations and international military cooperation in cyber security: Common challenges & state practices across Asia and Europe. 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 69–80. https://doi.org/10.1109/CYCON.2015.7158469
Boin, A., 'T Hart, P., Stern, E., & Sundelius, B. (2016). The Politics of Crisis Management: Public Leadership under Pressure (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316339756
Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Science and Engineering Ethics, 20(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y
Feaver, P. (2005). Armed servants: Agency, oversight, and civil-military relations (1. paperpack ed). Harvard Univ. Press.
Fitriani. (2023, September 5). New structures for ASEAN cyber defence and information sharing [Online post]. IISS. https://www.iiss.org/online-analysis/online-analysis/2023/09/new-structures-for-asean-cyber-defence-and-information-sharing/
IISS. (2021). Cyber Capabilities and National Power—Indonesia (pp. 143–151). International Institute for Strategic Studies.
Indonesian Ministry of Defence. (2015). Indonesian Defence White Paper 2015 (Third). Defence Ministry of the Republic of Indonesia. https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf
Karmini, N. (2024, June 24). Indonesia won't pay an $8 million ransom after a cyberattack compromised its national data center. AP News. https://apnews.com/article/indonesia-ransomware-attack-national-data-center-213c14c6cc69d7b66815e58478f64cee
Lebang, C. G. (2025, March 18). Indonesia's Cyber Security and Resilience Bill: Strengthening Governance or Expanding Institutional Rivalries? Https://Www.Lab45.Id/. https://www.lab45.id/detail/298/indonesia-rsquo-s-cyber-security-and-resilience-bill-strengthening-governance-or-expanding-institutional-rivalries
Meyer, C. (2024, June 26). Indonesia Refuses to Pay $8M Ransom in Data Center Cyberattack [Online post]. ASIS International. https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2024/june/indonesia-ransomware/
National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (No. NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
Nugroho, Y. (2024, August 8). Indonesia's National Data Centre Ransomware Attack: A Digital Governance Failure? FULCRUM. https://fulcrum.sg/indonesias-national-data-centre-ransomware-attack-a-digital-governance-failure/
Peters, B. G. (2015). Pursuing Horizontal Management: The Politics of Public Sector Coordination. University Press of Kansas. https://doi.org/10.1353/book46028
Priyandita, G., & Lebang, C. G. (2025, April 10). Indonesia's cyber soldiers: Armed without a compass. The Strategist. https://www.aspistrategist.org.au/indonesias-cyber-soldiers-armed-without-a-compass/
Putra, T. M., Midhio, I. W., & D.A.R, D. (2022). The Challenges of Civil-Military Cooperation in The Face of Cyber Threats in Indonesia. International Journal of Research and Innovation in Social Science, 06(02), 471–474. https://doi.org/10.47772/IJRISS.2022.6221
Reuters. (2024, June 24). Cyber attack compromised Indonesia data centre, ransom sought. https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/
Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939
Singapore MINDEF. (2025, July 27). Cyber Defence. Ministry of Defence. https://www.mindef.gov.sg/defence-matters/defence-topics/cyber-defence/
SSEK Law Firm. (2024, May 20). Fortifying Indonesia's Cyber Defenses: New Regulations for National Security and Crisis Management. SSEK Law Firm. https://ssek.com/blog/fortifying-indonesias-cyber-defenses-new-regulations-for-national-security-and-crisis-management/
US Cyber Command. (n.d.). US Cyber Command History. Retrieved December 8, 2025, from https://www.cybercom.mil/About/History/
Waterman, R. H., Peters, T. J., & Phillips, J. R. (1980). Structure is not organization. Business Horizons, 23(3), 14–26. https://doi.org/10.1016/0007-6813(80)90027-0
Wood, N. (2024, August 2). South Korea's 2024 Cyber Strategy: A Primer | Strategic Technologies Blog | CSIS [Online post]. CSIS. https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer