e-XXXX-XXXX

Original Article

Indonesia's Defense Diplomacy in Addressing Cyber Threats to National Security: A Study of the Role of the Indonesian National Armed Forces (TNI) in International Cyber Cooperation

Andes Pria Redho Fonda Sebayang[1]✉, Haposan Simatupang[2], Afrizal Hendra[3]
[1,2,3]Universitas Pertahanan RI, Indonesia
Korespondensi Author: andesfonda@gmail.com

Abstrak:

The securitization of cyberspace has positioned cyber threats as a central issue in national defense and international security, prompting states to integrate military capabilities into diplomatic efforts to enhance cyber resilience. This study examines Indonesia's defense diplomacy in addressing cyber threats, with particular attention to the role of the Indonesian National Armed Forces (Tentara Nasional Indonesia – TNI) in international cyber security cooperation. Using a qualitative descriptive case study approach, the research draws on in-depth interviews with key defense and cyber institutions and analysis of relevant policy documents. The findings show that Indonesia's cyber defense diplomacy is conducted through four main mechanisms: defense cooperation, cyber capacity-building, strategic communication, and normative engagement in multilateral forums. Although operational coordination among agencies is relatively effective, fragmented policy alignment limits the development of an integrated national cyber defense framework. TNI plays a significant role through joint cyber exercises, intelligence sharing, capacity development, and active participation in regional platforms such as ADMM-Plus and the ASEAN Cyber Defence Network. This study concludes that stronger institutional integration and standardized interagency mechanisms are essential to enhance Indonesia's cyber resilience and the effectiveness of its defense diplomacy.

Keywords: Defense Diplomacy, Cybersecurity, Military Diplomacy, Interagency,TNI, ASEAN Cyber Cooperation.

Introduction

Cyberspace has emerged as a strategic operational domain equivalent to land, sea, air, and outer space within contemporary security doctrine (Cavelty, 2012). The

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

digitalization of governmental administration, defense command systems, financial services, healthcare networks, transportation management, and public communications has fundamentally transformed national security environments. Cyber incidents—including espionage campaigns, ransomware attacks, data manipulation, disinformation operations, and disruptions to critical infrastructure—are no longer marginal technical problems but constitute strategic threats capable of generating cascading political, economic, and military effects comparable to conventional kinetic operations (Singer & Friedman, 2014). As a result, cybersecurity has become an integral pillar of modern defense doctrines and international security architectures. This transformation is illustrated by NATO's formal recognition of cyberspace as a domain of military operations in 2016, enabling cyberattacks to be treated under collective defense principles similar to other traditional operational domains (NATO, 2016).

Indonesia's vulnerability to cyber threats is magnified by its expansive digital ecosystem and rapid socio-technological integration. With more than 215 million active internet users, the country represents one of the largest digital markets in the world. While this connectivity enhances economic growth and administrative efficiency, it simultaneously expands the national attack surface and exposes systemic governance weaknesses. Recurrent high-profile data breaches affecting government institutions and public databases, coupled with ransomware incidents targeting healthcare facilities and educational institutions, demonstrate persistent vulnerabilities in information security governance. Importantly, these challenges do not result solely from external cyber intrusions, but also from internal governance failures, including insufficient data protection practices, fragmented institutional oversight, limited cyber risk awareness, and uneven enforcement of national standards. Insider misuse, credential leakage, mismanagement of data access, and deficiencies in interagency monitoring repeatedly feature as enabling factors behind major security incidents. Collectively, these patterns underscore that Indonesia's cyber threat environment is a complex blend of transnational digital crime, state-sponsored espionage activities, and domestic governance fragilities that extend beyond purely technological explanations.

In this context, defense diplomacy emerges as a critical non-coercive instrument for addressing the multidimensional and transboundary nature of cybersecurity threats. Cottey and Forster (2004) define defense diplomacy as the use of defense institutions and military resources in non-coercive activities aimed at confidence-building, conflict prevention, and the strengthening of cooperative security mechanisms. Rather than relying on force projection or deterrent postures alone, defense diplomacy enables military actors to function as instruments of strategic engagement, shaping security environments through dialogue, institutional partnerships, and cooperative capacity building. From a military statecraft perspective, defense diplomacy represents an extension of strategic influence beyond combat operations into political and normative spheres, reinforcing national interests through soft power mechanisms (Posen, 1984; Gray, 2010). Within the cyber domain, this approach is particularly salient, as threats transcend borders, attribution remains ambiguous, and collective resilience depends on information sharing, joint training, legal harmonization, and the development of common norms.

Cyber defence diplomacy, therefore, extends the traditional functions of military engagement into strategic communication, multilateral negotiations, joint capacity-building initiatives, and coordinated exercises specifically designed to enhance mutual understanding and operational readiness. In Southeast Asia, these dynamics are evident

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

in platforms such as the ASEAN Defence Ministers' Meeting Plus (ADMM-Plus), the ASEAN Cyber Defence Network (ACDN), and bilateral cyber cooperation agreements involving Indonesia and key regional partners, including Australia, Japan, and South Korea. Through these mechanisms, Indonesian defense diplomacy seeks to bolster technological competencies, forge trust-based partnerships, and embed national cyber defense frameworks within collective security architectures.

Despite steady regulatory advancement, including the enactment of the Electronic Information and Transactions Law, the Personal Data Protection Law, and the institutional establishment of the National Cyber and Crypto Agency (BSSN), Indonesia continues to face implementation challenges. Performance assessments such as the Global Cybersecurity Index (GCI) indicate notable improvements between 2017 and 2020, particularly regarding legal frameworks and organizational measures. However, persistent deficits remain in capacity-building, operational integration, interagency coordination, and the practical effectiveness of international cooperation mechanisms. These shortcomings illustrate a continuing gap between normative expectations (das sollen)—the aspiration for a resilient, integrated national cyber defense posture—and operational realities (das sein) marked by fragmented policy implementation and uneven institutional synchronization.

Within this strategic landscape, the Indonesian National Armed Forces (TNI) constitute a key actor linking defense diplomacy to cyber security governance. Beyond its traditional territorial and maritime defense mandates, TNI has progressively assumed roles in cyber exercises, professional training exchanges, intelligence-sharing programs, and participation in multinational cyber defense initiatives under ASEAN and broader international frameworks. Through institutions such as the TNI Cyber Unit (Satsiber) and the Center for International Cooperation (Puskersin TNI), the military increasingly functions as both an operational security provider and a diplomatic intermediary facilitating cooperative engagements across borders. This dual role positions TNI as a critical bridge between national security objectives and international cyber governance regimes.

Nevertheless, questions persist regarding the coherence of Indonesia's interagency cyber governance architecture and the degree to which defense diplomacy efforts are effectively synchronized with civilian regulatory bodies. Although operational coordination among the Ministry of Defense, TNI units, and BSSN is often functional during training or incident response exercises, sustained policy integration remains limited. Overlapping mandates, fragmented command structures, and the absence of a permanent joint cyber governance forum constrain the development of a unified national posture capable of translating diplomatic gains into comprehensive resilience.

Against this backdrop, this study aims to analyze three interrelated dimensions of Indonesia's cyber defense diplomacy: (1) the forms and implementation of defense diplomacy in countering cyber threats; (2) the effectiveness of interagency coordination mechanisms in international cyber security cooperation; and (3) the contribution of TNI in strengthening Indonesia's cyber defense diplomacy. Accordingly, the central research question guiding this inquiry is: How does defense diplomacy, spearheaded by TNI, function as a strategic instrument to enhance Indonesia's cyber security cooperation and national resilience.

The original contribution of this study lies in its theoretical integration of defense diplomacy and cyber security governance within a middle-power military context. While most prior scholarship treats cyber security predominantly as a civilian-technical or

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

legal-policy domain, and defense diplomacy as belonging mainly to conventional military cooperation frameworks, this research bridges both fields by conceptualizing cyber diplomacy as an emergent form of non-kinetic military statecraft. By incorporating interagency coordination theory and institutional liberalism, this study develops an integrative analytical model explaining how military institutions such as TNI function not only as security operators but also as diplomatic actors shaping transnational cyber cooperation regimes.

Metods

This study employed a qualitative descriptive–exploratory study design aimed at developing an in-depth understanding of Indonesia's defense diplomacy in responding to cyber threats, with particular emphasis on the role of the Indonesian National Armed Forces (TNI) in international cyber security cooperation. A qualitative approach was selected to capture complex institutional processes, perceptions, and strategic interactions that are not readily measurable through quantitative methods (Creswell, 2013). The case study design enabled a contextualized analysis of diplomacy, coordination mechanisms, and military engagement practices across domestic and international settings (Yin, 2018).

Research Scope and Case Selection

Indonesia was selected as the case study based on its status as a middle-power state facing rapidly expanding cyber vulnerabilities while actively participating in multilateral security frameworks. The research focused on national-level governance and diplomatic practices involving defense, cyber policy, and multilateral cooperation between 2017 and 2024, corresponding to key stages of Indonesia's cyber institutional development and increasing participation in ASEAN and international cyber initiatives.

Data Sources

This research utilized both primary and secondary data sources to ensure analytical robustness. Primary data were obtained through semi-structured in-depth interviews with officials and practitioners from key institutions directly involved in cyber governance and defense diplomacy:

1. Directorate of International Defense Cooperation, Ministry of Defense (Ditkersinhan Kemhan);
2. Cyber Defense Center, Ministry of Defense (Pushansiber Kemhan);
3. TNI International Cooperation Center (Puskersin TNI);
4. TNI Cyber Unit (Satsiber TNI);
5. National Cyber and Crypto Agency (BSSN).

Semi-structured interviews were chosen to maintain consistency across respondents while allowing flexibility to explore institution-specific perspectives on coordination mechanisms, diplomatic engagement practices, and cybersecurity capacity-building initiatives (Kvale, 2007). Interview questions were organized around three principal analytical themes: (1) forms of defense diplomacy practiced in cyber cooperation; (2) effectiveness of interagency coordination; and (3) TNI's operational and diplomatic contributions.

Secondary data consisted of official defense and cyber policy documents, Indonesia's National Cyber Security Strategy texts, regulations concerning cyber defense and data protection, ASEAN and ADMM-Plus cyber cooperation agreements, ITU Global

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

Cybersecurity Index (GCI) reports, NATO cyber policy publications, and communiqués from relevant international security forums. Documentary analysis supported the verification and triangulation of interview findings while facilitating contextual interpretation of Indonesia's diplomatic positioning (Bowen, 2009).

Data Analysis

Data analysis followed the interactive model developed by Miles and Huberman (2014), incorporating three analytical stages:

1. Data reduction, which involved coding interview transcripts and policy documents to identify key thematic patterns related to diplomacy practices, coordination challenges, and institutional roles.
2. Data display, whereby matrices and thematic mapping were employed to compare inter-agency perspectives and international engagement activities.
3. Conclusion drawing and verification, achieved through iterative comparison between interview insights and documentary evidence to confirm analytical interpretations and strengthen internal validity.

Validity and Reliability

To enhance research credibility, triangulation was conducted across methods and data sources, comparing interview testimonies with policy documents, international reports, and official statements (Denzin, 2012). Peer debriefing and iterative cross-checking of themes were applied to minimize researcher bias. Confirmability was supported by maintaining structured interview protocols and comprehensive coding trails. Ethical considerations included informed consent, confidentiality assurances, and anonymization of individual respondents to protect institutional sensitivities.

Analytical Framework Application

The theoretical framework integrating defense diplomacy, cybersecurity theory, interagency coordination, and institutional liberalism guided the analytical coding process. Each empirical finding was systematically mapped onto analytical dimensions such as non-coercive military engagement, capacity-building mechanisms, confidence-building measures, policy coordination processes, and institutional participation in multilateral forums. This approach enabled the study to connect empirical observations to conceptual themes and assess how TNI's activities contributed to Indonesia's broader cyber defense diplomacy posture.

Through this methodological design, the study ensured rigorous interpretation of strategic practices linking cyber security governance and military diplomacy, contributing both empirical case analysis and theoretically grounded insight to the scholarship of defense and international security cooperation.

Results

This section presents empirical findings derived from in-depth interviews with key defense and cyber institutions and policy document analysis. Results are organized into four major thematic dimensions corresponding to the analytical framework: (1) defense cooperation mechanisms; (2) cyber capacity-building initiatives; (3) strategic communication and normative engagement; and (4) institutional coordination and governance effectiveness.

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

Defense Cooperation

Indonesia's cyber defense diplomacy is primarily implemented through a combination of bilateral security partnerships and multilateral defense platforms. At the bilateral level, formal Memoranda of Understanding (MoUs) and defense cooperation arrangements with countries such as Australia, Japan, South Korea, and Singapore have expanded to include cyber capacity development components alongside conventional military cooperation. Interviews with officials of the Directorate of International Defense Cooperation (Ditkersinhan Kemhan) confirmed that cyber-security cooperation is increasingly embedded into joint training packages, officer exchange programs, and policy-level dialogues focusing on critical infrastructure protection, maritime information systems security, and cyber incident response modeling.

Multilaterally, Indonesia actively engages within the ASEAN Defence Ministers' Meeting Plus (ADMM-Plus) framework. Cybersecurity discussions under the ADMM-Plus Experts' Working Group have progressed from exploratory exchanges into structured table-top exercises simulating cross-border cyber incidents. Interviewees from Puskersin TNI highlighted that these exercises not only enhance technical readiness but also develop shared communication protocols, escalation management procedures, and trust-based intelligence-sharing mechanisms. This finding aligns with defense diplomacy theory emphasizing the creation of confidence-building measures (CBMs) as precursors to cooperative security governance (Cottey & Forster, 2004).

Empirical evidence indicates that Indonesia's participation extends beyond passive engagement. Through the ASEAN Cyber Defence Network (ACDN), TNI has contributed to the co-development of cyber range training modules and scenario simulations aimed at harmonizing cyber operational standards across Southeast Asia. Document analysis suggests that these initiatives aim to build interoperability in detection methodologies, information exchange arrangements, and technical doctrine alignment.

However, results also reveal that the depth of cooperation varies significantly by partner country. Cyber engagements with technologically advanced states tend to emphasize technical knowledge transfer and certification pathways, whereas collaboration with ASEAN peers often centers on joint training and standardized exercises rather than advanced technological exchange. This disparity limits the symmetrical development of collective cyber defense capacity across the region. Nevertheless, Indonesia's defense diplomacy consistently reinforces its diplomatic profile as a proactive middle power in ASEAN cyber security governance, reflecting the strategic utility of military engagement as soft power in shaping regional security norms (Nasserie, 2018).

Capacity Building

The data demonstrate that TNI plays a major role in national cyber capacity building, focusing on human resource development, professional training, and joint exercise participation. Capacity-building programs are largely implemented through three pillars:

1. Personnel exchanges with foreign cyber-defense institutions and defense academies, enabling Indonesian officers to gain exposure to international best practices and emerging cyber warfare doctrine.
2. Professional certification training, conducted in cooperation with national and international training providers, which enhances specialized technical skills in network defense, malware analysis, cyber forensics, and cyber incident containment

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

procedures.

3. Cyber range simulations, carried out under ASEAN and bilateral frameworks, where TNI cyber units jointly conduct live simulation exercises with regional partners to practice scenario response protocols against ransomware attacks, data intrusions, and cyber sabotage operations.

Interviewees within Satsiber TNI emphasized that participation in multinational exercises significantly improved both individual competencies and collective operational awareness. These findings align with cybersecurity theory emphasizing that resilience is built not only on technology but on sustained human capital investment (Singer & Friedman, 2014). Moreover, respondents reported improvements in doctrinal comprehension concerning cyber conflict escalation dynamics and attribution challenges, key components of crisis management frameworks under NATO cyber defense practices (NATO, 2016).

Despite these positive developments, findings also indicate systemic limitations. Capacity-building pipelines remain insufficiently integrated across civilian and military sectors. Training conducted by BSSN, the Ministry of Defense, and TNI operates under largely separate frameworks without standardized national certification pathways or curriculum integration. Officials from BSSN noted that cyber defense training efforts across institutions are often duplicated rather than consolidated, reducing overall efficiency and hindering scalability.

Documentary data further reveal uneven regional participation, where capacity-building benefits are concentrated in central agencies while provincial and sectoral institutions remain weakly developed. This disparity results in fragmented national cyber readiness that undermines comprehensive resilience building. These findings underscore that cyber resilience cannot be achieved through sector-specific initiatives alone but demands integrated, whole-of-government frameworks (ITU, 2012).

Strategic Communication and Normative Engagement

Indonesia's defense diplomacy extends beyond technical collaboration into normative and strategic communication activities designed to shape regional cyber governance frameworks. Interview data confirm that Indonesian delegations consistently advocate principles of voluntary restraint, sovereign equality in cyberspace, and international confidence-building measures within ASEAN dialogues, the United Nations Open-Ended Working Group (OEWG), and relevant ITU platforms.

Through these forums, Indonesia seeks to promote norms discouraging offensive cyber operations targeting civilian infrastructure and critical information systems, while endorsing capacity-sharing initiatives to close developmental gaps between ASEAN member states. This diplomatic positioning is indicative of a middle-power strategy emphasizing normative leadership rather than technological dominance (Keohane & Nye, 2011).

TNI's involvement in these dialogues is both direct and symbolic. Senior officers participate as technical advisors within diplomatic delegations or as subject-matter experts in side-event discussions on military cyber doctrine transparency. This engagement contributes to trust-building measures by articulating Indonesia's cyber defense posture as defensive, cooperative, and norm-based. According to interview feedback, military participation enhances the credibility of Indonesian diplomatic narratives because TNI is perceived by regional counterparts as an authoritative operational stakeholder rather than merely a policy observer.

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

Document analysis further shows that Indonesia actively supports the integration of cyber CBMs such as hotline communications, cyber incident notification mechanisms, and transparency exchanges of cyber defense policies among ASEAN defense ministries. These measures directly reflect the objectives of defense diplomacy frameworks designed to prevent escalation and misperceptions (Cottey & Forster, 2004).

Nevertheless, challenges remain. Indonesia's limited ability to offer high-end technological assistance constrains its normative leverage compared to technologically advanced states. While Indonesia contributes diplomatically and institutionally, resource constraints limit its role in advanced cyber tool-sharing networks. Consequently, Indonesia's normative leadership depends heavily on sustained multilateral diplomacy rather than material inducements.

Institutional Coordination

Institutional coordination constitutes the most critical challenge identified by this study. At the operational level, coordination among the Ministry of Defense, TNI cyber units, and BSSN is functional, particularly during multinational exercises and incident response simulations. Cross-agency task forces and ad-hoc working groups enable timely communications and collective response formulation. This operational synchronization reflects the capacity of Indonesian institutions to mobilize when cyber threats require immediate reaction.

However, at the policy and strategic levels, coordination remains fragmented. Overlapping institutional mandates, particularly among BSSN, Kemhan cyber directorates, and military cyber units, produce ambiguous leadership roles in national cyber governance. Interviewees frequently cited the absence of permanent cross-ministerial cyber policy bodies capable of aligning national strategies, allocating resources coherently, and integrating foreign cooperation outputs into domestic policy frameworks.

This finding is consistent with coordination theory which posits that bureaucratic complexity requires formally institutionalized mechanisms rather than ad-hoc cooperation to maintain system coherence (Gulick, 1937; Comfort, 2007). In Indonesia's case, operational coordination does not automatically translate into unified policy coherence or institutional alignment. The absence of standardized joint operating procedures (SOPs) governing international cyber engagements further impedes synchronization, as each agency negotiates foreign partnerships independently.

Moreover, respondents highlighted that lessons learned from international exercises or norms negotiations are not uniformly incorporated into domestic doctrine or regulatory practices. This disconnect limits the strategic utility of defense diplomacy initiatives by preventing international learning processes from producing holistic national resilience improvements.

Synthesis and Theoretical Novelty

The theoretical novelty of this study emerges through its integrative empirical demonstration that cyber diplomacy is not merely a domain of civilian technical governance but constitutes an emergent layer of non-kinetic military statecraft practiced by middle-power defense institutions. While existing literature often conceptualizes cyber security cooperation as civil-regulatory engagement or legal norm-building, findings from Indonesia reveal that military institutions such as TNI operate as hybrid actors embedded within diplomatic networks. They simultaneously perform operational

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

cyber defense roles and diplomatic confidence-building functions that shape transnational cooperation regimes.

By combining defense diplomacy theory with cybersecurity governance and interagency coordination frameworks, this study advances an analytical model wherein cyber diplomacy becomes a strategic interface linking national military professionalism, international normative advocacy, and institutional capacity-building processes. This empirical integration extends the conventional scope of defense diplomacy literature beyond kinetic domains and maritime or peacekeeping cooperation into the cyber security sphere, thereby contributing novel insight to studies of military soft power and middle-power diplomacy.

Conclusion

This study concludes that Indonesia's defense diplomacy constitutes a strategically significant mechanism for addressing cyber threats and strengthening national cyber security cooperation, particularly through the proactive involvement of the Indonesian National Armed Forces (TNI). Empirical findings demonstrate that defense diplomacy facilitates enhanced cyber capacity-building through joint training programs, multinational simulation exercises, professional exchanges, and increased operational interoperability with regional and international partners. Furthermore, diplomatic engagement in multilateral forums such as ADMM-Plus and the ASEAN Cyber Defence Network has enabled Indonesia to expand its normative influence by promoting confidence-building measures, transparency norms, and cooperative approaches to cyber threat management.

Despite these achievements, the study identifies persistent structural challenges that constrain the overall effectiveness of Indonesia's cyber defense diplomacy. Most notably, deficiencies in policy-level interagency coordination continue to impede the consolidation of international diplomatic outcomes into a coherent national cyber defense architecture. Overlapping institutional mandates among TNI, the Ministry of Defense, BSSN, and other civilian agencies, coupled with the absence of standardized joint operating procedures and permanent cross-ministerial policy synchronization mechanisms, have limited the transformation of cooperation gains into integrated national resilience frameworks.

From a theoretical perspective, this research contributes to defense diplomacy and security studies by conceptualizing cyber diplomacy as an emergent non-kinetic operational layer of military statecraft. The findings affirm that modern armed forces, particularly in middle-power contexts such as Indonesia, increasingly function not only as operational security providers but also as diplomatic actors shaping transnational cyber governance regimes. Consequently, policy reforms emphasizing institutional integration, centralized coordination platforms, and harmonized training systems are essential to maximize the strategic utility of defense diplomacy in enhancing Indonesia's national cyber resilience and sustaining credible regional cyber security cooperation.

Suggestion

Based on the study's empirical findings and theoretical analysis, several policy recommendations are proposed to strengthen the effectiveness of Indonesia's cyber defense diplomacy and enhance national cyber resilience.

First, Indonesia should establish a permanent National Cyber Defense Policy Council integrating the Indonesian National Armed Forces (TNI), the Ministry of

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

Defense, the National Cyber and Crypto Agency (BSSN), and relevant civilian authorities. This institutional platform would facilitate harmonized policy formulation, reduce overlapping mandates, and ensure consistent translation of international cooperation outcomes into domestic cyber governance frameworks.

Second, standardized Joint Cyber Defense Standard Operating Procedures (SOPs) should be developed and implemented across agencies to enhance interoperability, clarify operational roles during cyber incidents, and institutionalize best practices gained through multinational exercises and bilateral cooperation programs.

Third, Indonesia should expand its participation within the ASEAN Cyber Defence Network by promoting more comprehensive multinational exercises that incorporate integrated, whole-of-government cyber incident response simulations. Such exercises would enhance regional interoperability, shared situational awareness, and crisis coordination mechanisms.

Finally, Indonesia should institutionalize cyber attaché positions within defense diplomacy missions abroad. These specialized officers would function as technical-diplomatic liaisons, strengthening international information exchange, coordinating capacity-building initiatives, and reinforcing Indonesia's normative leadership within global cyber security governance forums. Collectively, these policy measures would enhance institutional cohesion, operational readiness, and diplomatic credibility, enabling Indonesia's defense diplomacy to more effectively address transnational cyber threats and contribute to regional cyber stability.

References

Amalia, F. S., Mahroza, J., Halkis, M., Priyanto, P., Purwanto, S., Gunawan, R., ... & David, L. (2024). DIPLOMASI PERTAHANAN INDONESIA-AUSTRALIA UNTUK HUMANITARIAN ASSISTANCE AND DISASTER RELIEF (HADR).

Amrulloh, M. H., Purwanto, S., Hutajulu, B., & Siagian, F. (2025). Strategi Kodam XVII/Cenderawasih dalam Pemenuhan Personel guna Mendukung Kesiapan Operasi di Papua. *Sparta Multidisciplinary Journal,* 1(1), 16-32.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

Cavelty, M. D. (2012). Cyber security and threat politics: US efforts to secure the information age. Routledge.

Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. HarperCollins.

Comfort, L. K. (2007). Crisis management in cyberspace: Information, coordination, and sensemaking in complex operations. Public Organization Review, 7(2), 193–213. https://doi.org/10.1007/s11115-007-0027-5

Cottey, A., & Forster, A. (2004). Reshaping defence diplomacy: New roles for military cooperation and assistance. Oxford University Press.

Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches (3rd ed.). Sage Publications.

Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research*, 6(2), 80–88. https://doi.org/10.1177/1558689812437186

Gulick, L. (1937). Notes on the theory of organization. In L. Gulick & L. Urwick (Eds.), Papers on the science of administration (pp. 1–45). Institute of Public Administration.

Hipdizah, S. A., Sigit Purwanto, S. I. P., Yermia Hendarwoto, S. H., Duarte, R. F., Ferdinan Siagian, S. T., & Han, M. (2025). Buku Ajar Doktrin Militer. Yayasan Putra Adi Dharma.

Hermansah, F., Mahroza, J., Halkis, M., Prakoso, L. Y., Purwanto, S., Sutanto, R., ... & David, L. (2024). DIPLOMASI PERTAHANAN INDONESIA AFGANISTAN

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026

DALAM PENYELESAIAN PERDAMAIAN TAHUN 2018-2023.
International Telecommunication Union (ITU). (2012). Global cybersecurity agenda (GCA): High-level experts group (HLEG) report. ITU Publications.
Keohane, R. O., & Nye, J. S. (2011). Power and interdependence (4th ed.). Longman.
Kvale, S. (2007). Doing interviews. Sage Publications.
Miles, M. B., & Huberman, A. M. (2014). Qualitative data analysis: A methods sourcebook (3rd ed.). Sage Publications.
Nasserie, H. (2018). Defense diplomacy as military soft power: The case of post-Cold War security cooperation. Defense Studies, 18(3), 345–361. https://doi.org/10.1080/14702436.2018.1488822
North Atlantic Treaty Organization (NATO). (2016). Warsaw summit communiqué. NATO Headquarters.
Pajtinka, E. (2016). Military diplomacy and defense diplomacy: A comparative approach. Journal of International Relations, 14(1), 75–92.
Purwanto, S., & Ilhamsyah, I. (2025). Army Human Resources Development Strategy through Human Capital Approach. Indonesian Journal of Social Science and Education (IJOSSE), 1(1), 1-22.
Purwanto, S., Purnomo, M. R., & Budiman, H. (2025). POWER DYNAMICS IN DECISION MAKING: A QUALITATIVE ANALYSIS. POWER, 2(1), 80-86.
Purwanto, S., Basalamah, S., Mallongi, S., & Sukmawati, S. (2020). Effects of Recruitment, Leadership, and Local Culture on Discipline and Performance of Garuda Contingent Soldiers in Lebanon. International Journal of Multicultural and Multireligious Understanding, 7(5), 606-618.
Purwanto, S., & Siagian, F. (2025). Strategic human resources management in the global era: Navigating opportunities and challenges. Centurion MSPD Journal, 1(1).
Purwanto, S., Wibowo, A., & Suharti, T. (2023). The OCB Determinant of Employees in Non-Profit Organization; Leadership Role and Work Engagement. inovator, 12(2), 251-263.
Prasetiawan, H. P., AR, D. D., & Purwanto, S. (2025). THE STRATEGY TO IMPROVE THE CHARACTER OF MILITARY ACADEMY CADETS THROUGH THE ROLE OF MENTORS IN SHAPING PROFESSIONAL OFFICERS TO SUPPORT THE MAIN DUTIES OF THE INDONESIAN ARMY:. Santhet (Jurnal Sejarah Pendidikan Dan Humaniora), 9(6), 2184-2191.
Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
Sigit Purwanto, S. I. P. (2024). Definisi Dan Konsep. Manajemen Sumber Daya Manusia, 1.
Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Sage Publications.

Received: November 14, 2025 – Revised: November 20, 2025 - Accepted: Desember 16, 2025 - Published online: January 30, 2026