



Building Cyber Confidence: ASEAN's Defence Diplomacy through ADMM-Plus

Dyah Lupita Sari^{1*}, Lu'Lu'ul Aulia Hamidah², Rahma Maulidina³, Khaira Putri Maharani⁴,
Fathania Queen Genisa⁵, Melaty Anggraini⁶, Virginia Ayu Sagita⁷
^{1,2,3,4,5,6,7} UPN Veteran Yogyakarta, Indonesia

Received : September 8, 2026

Revised : September 15, 2026

Accepted : September 16,
2026

Online : October 07, 2026

Abstract

Digital transformation in Southeast Asia has enhanced regional connectivity while creating new vulnerabilities to complex, cross-border cyber threats. This situation has prompted ASEAN to develop cybersecurity cooperation mechanisms, including those within the ASEAN Defence Ministers' Meeting Plus (ADMM-Plus) framework. This study analyzes how the ADMM-Plus, specifically the Experts' Working Group on Cyber Security (EWG-CS), addressed regional cyber threats between 2017 and 2025 through the lens of Confidence-Building Measures (CBMs). Using a qualitative case study approach, the study analyzes secondary data from official ASEAN and ADMM-Plus documents, policy reports, and academic literature, complemented by a semi-structured interview with an official from Indonesia's National Cyber and Crypto Agency (BSSN). The findings show that the EWG-CS operationalizes CBM functions through sustained dialogue, information and knowledge exchange, capacity building, and institutional interaction among ASEAN Member States and Plus Countries. These practices have generated institutional mechanisms and collaborative outputs across three co-chairmanship cycles, including points-of-contact arrangements, technical personnel networking, cyber terminology standardization, cyber exercises, training programs, and the Cyber Security Framework. The BSSN interview further indicates that international cybersecurity cooperation contributes to Indonesia's national cybersecurity by facilitating knowledge transfer, strengthening capacity, expanding institutional networks, and supporting cyber resilience. Rather than directly preventing or responding to cyberattacks, the EWG-CS functions as a defense diplomacy platform that reduces uncertainty, builds trust, and facilitates sustained regional cybersecurity cooperation.

Keywords: *ADMM-Plus, Experts' Working Group on Cyber Security, confidence-building measures, defence diplomacy, cyber security*

INTRODUCTION

Digital transformation in Southeast Asia has unfolded rapidly over the past decade, propelling ASEAN to become one of the regions with the fastest-growing digital economies globally (Sari, 2024). However, this accelerated digitalization has also introduced new vulnerabilities in the form of cross-border, non-traditional cyber threats that no single nation can anticipate or counter in isolation (Lavrova, 2025). Data from various cybersecurity research institutions indicate a significant upward trend in attacks across the region. Figures show that the number of successful cyber intrusions into systems within ASEAN doubled in 2024 compared to 2023. Notably, approximately 67 percent of all incidents recorded over the past two years occurred in 2024 alone, with malware, social engineering, and vulnerability exploitation identified as the most prevalent attack methods targeting organizations and individuals in the region (Lavrova, 2025). Similarly, CYFIRMA (2024) reports a comparable trend across the Asia-Pacific region, identifying system intrusions and ransomware as the primary drivers of data breach incidents, while the manufacturing, government, and financial sectors consistently remain key targets for such attacks (CYFIRMA, 2024).

Copyright Holder:

© Dyah, Lu'Lu'ul, Rahma, Khaira, Fathania, Melaty, & Virginia. (2026)
Corresponding author's email: dyah.lupitasari@upnyk.ac.id

This Article is Licensed Under:



The transboundary nature of cyber threats in the region has been evident since the early years of ASEAN's cyber cooperation. In 2017, several ASEAN nations that play strategic roles in regional defense forums were targeted by cyber campaigns that unfolded almost simultaneously. Reported compromises included Philippine government websites—such as those of the armed forces and the Office of the President—as well as government sites in Laos and Cambodia, and three ASEAN-related portals, including the official ASEAN website (Lassalle et al., 2017). These attacks were attributed to APT32 (also known as OceanLotus), a cyber group suspected of being based in Vietnam and that has conducted cyber espionage operations since at least 2014; its targets have included foreign governments, multinational corporations, journalists, and activists, particularly in Southeast Asia (Lassalle et al., 2017). The fact that APT32's campaign targeted multiple ASEAN countries concurrently—during the same year the EWG-CS concept was agreed upon—underscores that cyber threats in the region are no longer merely technical risks but have become a shared security concern that demands a collective response rather than a purely national approach.

As a regional organization grounded in the principles of non-interference and consensus, ASEAN has responded to this challenge by using the ASEAN Defence Ministers' Meeting (ADMM) and its expanded counterpart, the ADMM-Plus (Brock, 2024). The ADMM-Plus is unique in that it includes not only the ten ASEAN member states but also eight dialogue partners—the "Plus Countries": Australia, China, India, Japan, New Zealand, the Republic of Korea, Russia, and the United States. This composition makes it a cross-regional cybersecurity forum with a broader scope than forums comprising only ASEAN members. This paper examines how the ADMM-Plus, through its Experts' Working Group on Cyber Security (EWG-CS), has served as an instrument for Confidence-Building Measures (CBMs) in addressing regional cyber threats between 2017 and 2025. Using the CBM concept as an analytical framework, the paper analyzes how the EWG-CS's operational mechanisms—particularly sustained dialogue, information and knowledge exchange, capacity building, and institutional interaction between ASEAN member states and Plus countries—contribute to trust-building and stronger coordination in the face of cross-border cyber threats. Accordingly, this study is guided by the following research question: How does the ADMM-Plus, through the Experts' Working Group on Cyber Security (EWG-CS), function as a confidence-building measure in ASEAN's response to regional cyber threats between 2017 and 2025? The 2017–2025 timeframe is deliberately chosen because, although the concept paper establishing the EWG-CS was agreed upon by ASEAN defence ministers in May 2016, the working group only became operational following its inaugural meeting in Manila in July 2017, marking the start of its first three-year cooperation cycle (Ministry of Defence of the Republic of Indonesia, 2017; Minárik, 2016). This starting point therefore captures the EWG-CS from the moment it began producing verifiable institutional outputs, while the endpoint of 2025 corresponds to the completion of its third co-chairmanship cycle and the ADMM-Plus's fifteenth anniversary, together spanning a sufficiently long period to trace the mechanism's institutional evolution rather than merely its founding moment.

LITERATURE REVIEW

Existing literature on ADMM-Plus and ASEAN cybersecurity underscores the forum's role as an instrument for Confidence-Building Measures (CBMs) within defense diplomacy. Silalahi (2023) demonstrates that the ADMM/ADMM-Plus functions as a CBM mechanism through practical cooperation and interaction among defense institutions—aligning with Tan's (2020) findings that the forum has evolved into a mechanism for regional security multilateralism. Focusing specifically on cyber issues, Shoji (2023), Hoang (2021), and Teo (2023) indicate that the establishment of the Cyber Security Expert Working Group has expanded the ADMM-Plus's role in coordinating and

enhancing regional cybersecurity capacity; meanwhile, [Sianturi \(2021\)](#) examines Indonesia's cyber defense diplomacy within the ADMM-Plus from 2014 to 2019, concluding that this engagement remains in its early stages and has yet to achieve optimal effectiveness. At a more technical level, [Saputri et al. \(2020\)](#) confirm that Indonesia's participation in the ASEAN-Japan Online Cyber Exercise remains focused on personnel capacity building rather than on strategic policy.

Based on this mapping, existing studies fall into three distinct areas of focus. First, research on the ADMM-Plus as a Confidence-Building Measure (CBM) generally centers on defense cooperation and broad regional security dialogue, without explaining how this confidence-building mechanism operates in the face of non-traditional cyber threats ([Silalahi, 2023](#); [Tan, 2020](#)). Second, studies regarding the EWG-CS emphasize institutional coordination and capacity building but have yet to explicitly link these to the framework of defense diplomacy—specifically, how such interactions foster trust among the defense institutions of participating nations ([Shoji, 2023](#); [Hoang, 2021](#); [Teo, 2023](#)). Third, research on Indonesia's involvement tends to be limited to the initial stages of cooperation development or technical implementation aspects, thereby failing to examine the institutional evolution of the EWG-CS across multiple operational cycles ([Sianturi, 2021](#); [Saputri et al., 2020](#)).

Addressing this gap, this study offers a novel contribution by integrating perspectives on Confidence-Building Measures (CBMs) and cybersecurity cooperation to explain how the ADMM-Plus—through its Experts' Working Group on Cyber Security (EWG-CS)—serves a confidence-building function in response to regional cyber threats. Unlike previous studies that position the ADMM-Plus merely as a CBM mechanism within the broader context of defense cooperation, this research identifies and analyzes the specific CBM mechanisms operating within the EWG-CS—particularly sustained dialogue, information and knowledge exchange, capacity building, and inter-institutional interaction and networking. Furthermore, this study expands on research focused on the EWG-CS's inception or early stages by tracing its longitudinal development from 2017 to 2025, thereby examining the sustainability and evolution of the EWG-CS's function as a confidence-building mechanism in the face of cross-border cyber threats. Thus, the study's contribution lies not in claiming that the ADMM-Plus is a CBM, but rather in explaining how—and through which mechanisms—the EWG-CS operationalizes CBM functions within defense diplomacy to address non-traditional security threats at the regional level.

RESEARCH METHOD

This study employs a qualitative case study approach to analyze ASEAN's response to cyber threats through the ADMM-Plus framework during the 2017–2025 period. The research data consist of secondary sources gathered through document analysis—specifically official ASEAN and ADMM-Plus documents such as Joint Declarations, Chairman's Statements, and materials from the Experts' Working Group on Cyber Security (EWG-CS) covering 2017–2025. International journals, books, and policy reports serve as supplementary sources. Data were analyzed qualitatively to identify the evolution of cybersecurity cooperation within the ADMM-Plus framework. The study uses the concept of Confidence-Building Measures (CBMs)—as a component of defense diplomacy—to analyze how ADMM-Plus fosters trust in regional cybersecurity cooperation. From a defense diplomacy perspective, defense relations and instruments are strategically employed to build interstate ties, manage uncertainty, and support shared security interests ([Charillon et al., 2020](#)). A key instrument of defense diplomacy is the use of confidence-building measures (CBMs), which build trust, reduce suspicion, and enhance transparency among nations through sustained communication, information exchange, dialogue, and interaction ([Charillon et al., 2020](#)). Consequently, this study does not treat defense diplomacy as a standalone concept; instead, it focuses its analysis on CBMs as an operational mechanism of defense diplomacy. This framework

is used to identify how mechanisms implemented through the EWG-CS—such as dialogue, information and knowledge exchange, capacity building, and inter-institutional defense interactions—contribute to trust-building and interstate coordination in responding to cyber threats between 2017 and 2025.

For data collection and validation, this study draws on both primary and secondary sources, including official ASEAN and ADMM-Plus documents, EWG-CS publications, government documents and press releases, academic literature, and relevant cybersecurity reports. These sources were systematically reviewed to identify evidence on Indonesia's participation in the EWG-CS, the group's activities and institutional outputs, and the broader implementation of confidence-building measures (CBMs) within the framework of defense diplomacy. In addition to secondary sources, primary data were collected through a semi-structured interview with Arie Setya Dewi, S.ST., S.S., a Senior Policy Analyst at the Directorate of Cybersecurity and Cryptography Strategy, Indonesia's National Cyber and Crypto Agency (BSSN). The interview was conducted on 27 July 2026 to obtain institutional insights into Indonesia's participation in the EWG-CS, particularly aspects of cooperation and institutional engagement that are not fully documented in publicly available sources.

FINDINGS AND DISCUSSION

Cyber Threats as an Emerging Security Issue in ASEAN

Advances in digital technology have become a pivotal force reshaping the security landscape of Southeast Asia. Over the past decade, ASEAN nations have undergone accelerated digital transformation, driven by rising internet use, the growth of the digital economy, the digitization of public services, and greater reliance on information and communication technology (ICT) infrastructure. While this transformation has bolstered regional economic integration, it has also introduced new vulnerabilities to a range of cyber threats. This growing dependence on digital ecosystems has elevated cybersecurity and resilience to a strategic challenge for the Asia-Pacific region ([International Telecommunication Union, 2024](#)). A report by the INTERPOL ASEAN Cybercrime Operations Desk found that in the first half of 2019, the ASEAN region accounted for 7% of global botnet detections and 1.8% of global Command and Control (C&C) servers; the region also saw a 50% increase in banking malware attacks and was the source of over 5% of global Business Email Compromise (BEC) attacks ([INTERPOL, 2020](#)). These figures demonstrate that cyber threats have evolved from mere technical issues into strategic security concerns affecting economic stability, state capacity, and regional security. The escalation of cyber threats is further evidenced by incidents across ASEAN countries. Singapore experienced one of its most significant breaches with the 2018 SingHealth data leak, in which the personal data of approximately 1.5 million patients and the medication details of around 160,000 patients were exposed following a targeted operation against the healthcare sector's information infrastructure ([Committee of Inquiry, 2019](#)). In Indonesia, a 2024 ransomware attack on the Temporary National Data Center (PDNS) highlighted the vulnerability of the nation's digital infrastructure and the resulting impact on public services ([Ministry of Communication and Informatics of the Republic of Indonesia, 2024](#)). Other ASEAN nations—including Malaysia, Thailand, Vietnam, and the Philippines—have similarly faced threats such as malware, phishing, data breaches, and attacks targeting both government and business sectors. These patterns indicate that cyber threats have become a cross-border challenge that cannot be addressed through unilateral action alone.

The borderless nature of cyber threats underscores the urgency of regional security cooperation. Unlike traditional threats with clearly defined geographical boundaries, cyber threats involve actors, infrastructure, and targets that may be located in different regions; consequently, an

effective response requires information sharing, cross-border coordination, and trust-building. Furthermore, the "attribution problem"—where digital obfuscation makes it difficult for states to accurately identify attackers—risks increasing interstate misperceptions (Lee, 2023). Addressing cyber threats therefore requires a combination of technical capacity, security diplomacy, and regional cooperation. In response to the complexity of these threats, ASEAN has begun integrating cybersecurity into its defense cooperation agenda through the ASEAN Defence Ministers' Meeting Plus (ADMM-Plus). This mechanism serves as a platform for ASEAN member states and external partners to strengthen capacity and coordination in addressing non-traditional security issues—particularly through the Experts' Working Group on Cyber Security, which facilitates information exchange, capacity building, joint exercises, and the development of a shared understanding of cyber threats. Thus, the inclusion of cyber threats in the ADMM-Plus agenda demonstrates that ASEAN views cybersecurity as a strategic issue requiring a collective response through defense cooperation and regional security diplomacy.

ASEAN's Response to Cyber Threats through ADMM-Plus

Within the framework of defense diplomacy, confidence-building measures (CBMs) serve as instruments to foster trust, reduce uncertainty and suspicion, and strengthen inter-state relations through sustained communication, information exchange, dialogue, and interaction (Charillon et al., 2020). This study employs CBMs as the primary concept to analyze how cybersecurity cooperation within the ADMM-Plus—specifically through the Experts' Working Group on Cyber Security (EWG-CS)—contributes to building trust and enhancing coordination among nations. Consequently, the study does not focus on defense diplomacy as a standalone concept; instead, it positions CBMs as tools of defense diplomacy used to understand trust-building mechanisms for addressing regional cyber threats. The need for such an instrument is evident from the transboundary nature of cyber threats in the region—exemplified by the 2017 cyberattacks targeting government websites in Laos, Cambodia, and the Philippines (including the Philippine armed forces and presidential office sites, as well as the official ASEAN website). These attacks, which demonstrated the transboundary nature of cyber threats in Southeast Asia, occurred shortly after the ADMM adopted the concept paper establishing the EWG on Cyber Security, based on the Philippines' proposal in May 2016 (Minárik, 2016). Its evolution from 2017 to 2025 can be traced through three cycles of three-year co-chairmanships, yielding concrete outputs that demonstrate the institutionalization of CBMs: during the first cycle (2017–2020), the Philippines and New Zealand produced a Points of Contact and Technical Personnel Directory, a Glossary of Cyber Terminologies, and an EWG-CS portal, all of which were piloted via a Table-Top Exercise in Manila in 2019 (Aurelia & Maheswari, 2024); during the second cycle (2020–2023), Malaysia and the Republic of Korea produced the "CTREX" training program and a Cyber Security Framework (ASEAN Defence Ministers' Meeting, n.d.); meanwhile, the ongoing cycle (2023–2026) continues to strengthen this framework, although details regarding the co-chairs and specific outputs are not fully available in the open sources consulted. This series of outputs demonstrates that the institutionalization of the EWG-CS as a Confidence-Building Measure (CBM) instrument is accompanied by institutional artifacts that are verified and accumulated across cycles, aligning with the concept proposed by Charillon et al. (2020) that CBMs operate through sustained interaction and information exchange rather than as one-off events.

Findings from interviews with the BSSN reinforce the interpretation of Indonesia's level of participation when linked to the aforementioned CBM indicators: international cybersecurity cooperation is regarded by BSSN as a strategic instrument for strengthening Indonesia's national cybersecurity through knowledge and information transfer, capacity building, network expansion, and enhanced cyber resilience. At the regional level, BSSN actively represents Indonesia's position,

facilitates cooperation, and promotes confidence-building measures through ASEAN mechanisms, ASEAN Plus Dialogue Partners, and forums such as the ARF, ADSOM, ADMM, and ADMM-Plus. Knowledge transfer from these cooperative engagements serves as an indicator of capacity building, while the expansion of the national cyber network—through BSSN's engagement in ASEAN Plus Dialogue Partners, ASEAN–Japan Cyber Security Cooperation, ARF, ADMM-Plus, the UN Permanent Global Mechanism on ICT Security, and the BRICS Working Group on ICT Security, as well as bilateral cooperation with partner countries—reflects recurring communication extending to cyber forums beyond the ADMM-Plus (BSSN, personal communication, July 27, 2026). Nevertheless, the effectiveness of the EWG-CS is constrained by structural limitations stemming from ASEAN's consensus-based and non-interventionist nature: a [Tsjeung study \(2023\)](#) indicates that geopolitical friction among dialogue partners—such as the 2021 Myanmar coup and Russia's 2022 invasion of Ukraine—can spill over into ADMM-Plus EWG mechanisms; meanwhile, the forum's emphasis on dialogue rather than legally binding regulations limits its enforcement power in fostering collective compliance, and the disparity in technical capacity among member states is evident in the surge of ransomware incidents across the region during 2023–2024 ([Lavrova, 2025](#); [CYFIRMA, 2024](#)). Overall, the trajectory of the EWG-CS from 2017 to 2025 confirms that ASEAN's response to cyber threats via the ADMM-Plus operates primarily at the level of confidence-building and fostering mutual understanding among defense institutions, rather than through direct technical enforcement; its long-term effectiveness depends on the extent to which ASEAN and its dialogue partners can sustain this communication amidst capacity gaps and shifting geopolitical dynamics.

EWG-CS as a Confidence-Building Mechanism within ADMM-Plus

From the perspective of defense diplomacy, the confidence-building efforts of the ADMM-Plus can be viewed as a mechanism to foster communication and mutual understanding in the face of cross-border cyber threats. This characteristic is evident in the 2017 cyberattacks that targeted various government websites in Laos, Cambodia, and the Philippines—including those of the armed forces and the Philippine Office of the President ([Lassalle et al., 2017](#)). Such cases demonstrate that cyber threats can span multiple countries within the region, creating a need for cross-border communication and cooperation. In this context, the establishment of the ADMM-Plus Experts' Working Group on Cyber Security (EWG-CS) provides a cooperative framework for ASEAN and Plus countries through meetings, information and expert exchanges, and the development of cooperative mechanisms between defense and military institutions. The implementation of confidence-building is further demonstrated by the sustained communication facilitated by the EWG-CS. This forum was established not merely to respond to cyber threats affecting member states, but also to serve as a space for defense agencies to engage in ongoing communication. For instance, the inaugural EWG-CS meeting held in Manila in July 2017 brought together ASEAN nations and the eight Plus countries to discuss cybersecurity cooperation ([Ministry of Defence of the Republic of Indonesia, 2017](#)). This collaboration subsequently yielded mechanisms and outputs such as Points of Contact (POCs), the development of online platforms for information and policy exchange, the conduct of multilateral training and exercises, and the establishment of cybersecurity centers ([ASEAN Regional Forum, 2018](#)). These activities operate within the broader ADMM context, serving as a platform to enhance Confidence-Building Measures through dialogue and practical cooperation. Consequently, when viewed alongside the cyberattacks of that same year, the EWG-CS functions not as a direct incident response mechanism, but rather as an effort to establish defense communication channels both prior to and during the emergence of threats. This is significant because the EWG-CS framework itself prioritizes raising awareness, exchanging information and expertise, and developing cooperative solutions as its primary objectives ([Aurelia & Maheswari,](#)

2024). Thus, the EWG-CS demonstrates that defense diplomacy within ADMM-Plus cybersecurity cooperation operates primarily through confidence-building, communication, and mutual understanding, rather than through direct military responses to attacks. In other words, instances of cyberattacks provide the context highlighting the need for such cooperation, while the EWG-CS offers the institutional mechanisms to build confidence and collective capacity in addressing transnational threats.

CONCLUSIONS

This study demonstrates that ASEAN's response to cyber threats through the ADMM-Plus during 2017–2025 constitutes a Confidence-Building Measure (CBM) integral to regional defense diplomacy. The research findings indicate that the ADMM-Plus Expert Working Group on Cyber Security (EWG-CS) strengthens regional cybersecurity cooperation through CBM mechanisms—evidenced by sustained dialogue, information exchange, capacity building, and institutional interaction among ASEAN member states and dialogue partners. However, the study does not present the EWG-CS as a direct mechanism for preventing or responding to cyberattacks; rather, it serves as a defense diplomacy platform that fosters trust, reduces uncertainty, and develops cooperative practices to address cross-border cyber threats. Theoretically, this study contributes to defense diplomacy by showing that CBMs apply not only to conventional military security but also to non-traditional security issues through knowledge exchange, professional networking, and sustained institutional engagement. Practically, the study highlights the importance of strengthening coordination between defense institutions and national cybersecurity agencies, developing clearer evaluation mechanisms for EWG-CS programs, and narrowing the cyber capacity gap among participating nations to enhance the effectiveness of regional cooperation. Further research could examine the empirical effectiveness of EWG-CS programs and analyze how domestic capacities and geopolitical dynamics influence the evolution of ASEAN cybersecurity cooperation.

LIMITATIONS & FURTHER RESEARCH

This study has several limitations that should be acknowledged. First, the primary data collection relies on a single interview with one BSSN official; while this provides valuable firsthand insight into Indonesia's participation, it cannot capture the full diversity of experiences among the eighteen ADMM-Plus member and dialogue-partner states, and the findings drawn from this interview should therefore be read as illustrative of the Indonesian case rather than generalizable across the forum. Second, the analysis relies substantially on publicly available secondary documents; details regarding the co-chairs and specific outputs of the ongoing 2023–2026 cycle was not fully accessible through open sources at the time of writing, which constrains the completeness of the study's most recent chronological coverage. Third, as a qualitative case study grounded in document analysis and a single interview, this research does not empirically measure the operational effectiveness of EWG-CS programs in preventing or mitigating actual cyberattacks; it instead traces the mechanism's institutional and confidence-building function. Future research could address these limitations by incorporating interviews with officials from multiple ADMM-Plus member and dialogue-partner states, accessing restricted internal ADMM-Plus documentation where possible, and employing mixed methods to empirically assess the EWG-CS's operational outcomes.

REFERENCES

ASEAN Defence Ministers' Meeting. (n.d.). *About the ASEAN Defence Ministers' Meeting Plus (2)*. <https://admm.asean.org/index.php/about-admm/2-uncategorised/518-admm-plus-2.html>

- ASEAN Regional Forum. (2018). *ASEAN Regional Forum 2018*. National Cyber Security Agency Malaysia. <https://www.nacsa.gov.my/arf.php>
- Aurelia, A., & Maheswari, A. E. S. (2024). Analysis of the implementation of the “ASEAN Cyber Security Framework” in Singapore in 2020. *Journal of Social and Economics Research*, 6(1), 2168–2179. <https://idm.or.id/JSER/index.php/JSER>
- Brock, J. (2024, July 16). *ASEAN's cyber initiatives: A select list*. Center for Strategic and International Studies. <https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list>
- Charillon, F., Balzacq, T., & Ramel, F. (2020). Defense diplomacy. In T. Balzacq, F. Charillon, & F. Ramel (Eds.), *Global diplomacy: An introduction to theory and practice* (pp. 267–278). Springer. https://doi.org/10.1007/978-3-030-28786-3_19
- Committee of Inquiry. (2019, January 10). *Public report of the Committee of Inquiry into the cyber attack on Singapore Health Services Private Limited's patient database on or around 27 June 2018*. Government of Singapore. <https://file.go.gov.sg/singhealthcoi.pdf>
- CYFIRMA. (2024, September 26). *The changing cyber threat landscape: Asia-Pacific (APAC) region—Volume 3*. <https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-asia-pacific-apac-region-volume-3/>
- Hoang, T. H. (2021, February 10). *Repositioning the ADMM-Plus in a contested region* (ISEAS Perspective No. 13). ISEAS-Yusof Ishak Institute. <https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/iseas-2021-13-repositioning-the-admm-plus-in-a-contested-region-hoang-by-thi-ha/>
- International Telecommunication Union. (2024). *Global cybersecurity index 2024*. <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>
- INTERPOL. (2020). *ASEAN cyberthreat assessment 2020*. <https://www.interpol.int/en/Media/Documents/Publications/ASEAN-Cyberthreat-Assessment-2020>
- Lassalle, D., Koessel, S., & Adair, S. (2017, November 6). *OceanLotus blossoms: Mass digital surveillance and attacks targeting ASEAN, Asian nations, the media, human rights groups, and civil society*. Volexity. <https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/>
- Lavrova, D. (2025, March 20). *Cybersecurity threatscape in Southeast Asia*. Positive Technologies. <https://positechglobal.com/en/research/analytics/cybersecurity-threatscape-in-southeast-asia/>
- Lee, H. (2023). Public attribution in the US government: Implications for diplomacy and norms in cyberspace. *Policy Design and Practice*, 6(2), 198–216. <https://doi.org/10.1080/25741292.2023.2199964>
- Minárik, T. (2016, October 31). *ASEAN to focus on cybersecurity capacity- and confidence-building in 2017*. NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoe.org/incyber-articles/asean-to-focus-on-cybersecurity-capacity-and-confidence-building-in-2017/>
- Ministry of Communication and Informatics of the Republic of Indonesia. (2024, June 24). *BSSN identifikasi Pusat Data Nasional Sementara diserang ransomware*. <https://www.komdigi.go.id/berita/pengumuman/detail/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware>
- Ministry of Defence of the Republic of Indonesia. (2017, July 19). *1st ADMM-Plus Experts' Working Group on Cyber Security July 2017 digelar di Filipina*. <https://www.kemhan.go.id/bikintelhan/2017/07/19/1st-admm-plus-experts-working-group-on-cyber-security-july-2017-di-gelar-di-filipina.html>

- Saputri, D. P., Surryanto, D. W., & Risman, H. (2020). The Indonesian cyber diplomacy: ASEAN-Japan online cyber exercise. *Technium Social Sciences Journal*, 9, 453–464. <https://doi.org/10.47577/tssj.v9i1.911>
- Sari, M. N. (2024). Cybercrime in Association of Southeast Asian Nations: Regional effort and its effectiveness. *Journal of Information Policy*, 14, 568–598. <https://doi.org/10.5325/jinfopoli.14.2024.0016>
- Shoji, T. (2023). ASEAN political security community: Development of multilateral cooperative frameworks and further challenges. *Security & Strategy*, 3. <https://www.nids.mod.go.jp/english/publication/security/pdf/2023/01/09.pdf>
- Sianturi, S. M. (2021). Indonesian defense diplomacy in achieving cyber security through ADMM-Plus 2014–2019. *LITERATUS*, 3(2), 152–158. <https://doi.org/10.37010/lit.v3i2.300>
- Silalahi, A. E. (2023). ADMM/ADMM-Plus as CBM through non-traditional issues (ASEAN). *International Journal of Humanities Education and Social Sciences*, 2(6), 1819–1833. <https://doi.org/10.55227/ijhess.v2i6.460>
- Tan, S. S. (2020). Is ASEAN finally getting multilateralism right? From ARF to ADMM+. *Asian Studies Review*, 44(1), 28–43. <https://doi.org/10.1080/10357823.2019.1691502>
- Teo, S. (2023, May 8). *The future of the ADMM-Plus in the Indo-Pacific*. Institute for Security & Development Policy. <https://www.isdp.eu/publication/the-future-of-the-admm-plus-in-the-indo-pacific/>
- Tsjeng, Z. H. (2023, December 13). *ASEAN Defence Ministers' Meeting-Plus: Divisions amid functional cooperation?* RSIS Commentary. <https://rsis.edu.sg/rsis-publication/idss/ip23088-asean-defence-ministers-meeting-plus-functional-cooperation/>