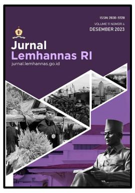

Jurnal Lemhannas RI (JLRI)
E-ISSN : 2830-5728
Vol. 12 No. 4, December 2024: 467-484
DOI: 10.55960/jlri.v12i4.990
https://jurnal.lemhannas.go.id/index.php/jkl

Optimising Multilateral Cooperation in Combating Cybercrime to Enhance National Vigilance

Asep Dicky Lukman W.[1], Rido Hermawan[2*]
[1] Participant, 67th Cohort, Regular Education Programme, Lemhannas R.I. Indonesia
[2] Universitas Hasanuddin, Makassar, Indonesia

*) Corresponding Author: ridohermawan6720@gmail.com

Article Info:

Keywords:
Cybercrime, Cybersecurity Governance, Legal Harmonisation, Multilateral Cooperation, National Vigilance

Article History:
Received : 23-05-2024
Revised : 25-09-2024
Accepted : 30-12-2024

Article DOI :
10.55960/jlri.v12i4.990

Abstract

Purpose: Cybercrime poses an escalating threat to national security, necessitating stronger multilateral cooperation to address cybersecurity governance gaps. This analysis examines how strategic collaboration, legal harmonisation, and intelligence-sharing enhance cyber resilience while identifying key challenges and opportunities in reinforcing national vigilance against cyber threats.

Study Design/Methodology/Approach: A qualitative approach with a comprehensive literature review of primary and secondary sources provides a structured assessment. A SWOT analysis evaluates the strengths, weaknesses, opportunities, and threats in global cybercrime cooperation, while a deductive analytical approach refines cybersecurity models using contemporary empirical data. This methodological framework offers policy insights into the effectiveness of international cyber governance strategies.

Findings: Multilateral cooperation strengthens cyber resilience by facilitating intelligence-sharing, legal alignment, and coordinated cyber defences. Countries with integrated cybersecurity frameworks exhibit stronger defensive capabilities. However, regulatory inconsistencies, trust deficits, and technological gaps hinder collaboration. Addressing these barriers requires harmonised cybersecurity policies, enhanced cyber diplomacy, and joint capacity-building initiatives to improve global cybersecurity governance.

Originality/Value: The analysis advances cybersecurity governance research by integrating SWOT analysis and deductive reasoning to evaluate multilateral strategies. Unlike previous studies that focus on unilateral or regional cybersecurity policies, this research highlights globally adaptive frameworks that reinforce national security. The findings offer concrete policy recommendations for institutions such as ASEAN, ITU, and UNODC to implement harmonised cybersecurity models, ensuring sustainable international cooperation against emerging cyber threats.

How to cite : : Lukman W.A.D. & Hermawan, R. (2024). Optimising Multilateral Cooperation in Combating Cybercrime to Enhance National Vigilance. *Jurnal LemhannasRI, 12*(4), 467-484. https://doi.org/10.55960/jlri.v12i4.990.

INTRODUCTION

State sovereignty remains fundamental in preserving national stability and protecting public interests. The rapid evolution of digital technology has significantly increased the complexity of maintaining sovereignty, particularly as cybercrime has emerged as a transnational threat. These threats target individuals, corporations, critical infrastructure, and government systems, posing substantial risks to national security (Aida, 2021; Ziemke-Dickens & Droogan, 2010). The acceleration of digital transformation has further underscored the urgency of strengthening cybersecurity resilience. The Fifth Geopolitical Era, marked by the digital revolution and the rise of artificial intelligence (AI), has driven profound socio-economic and political changes. However, cybercriminals have also exploited AI to orchestrate more systematic and sophisticated attacks that are increasingly difficult to detect. The Global Risk Report 2024 identifies cybercrime as one of the most pressing global threats over the next decade, primarily due to AI-driven automated security breaches (CNN Indonesia, 2024).

The economic impact of cyberattacks is significant, with the Institute of Internal Auditors (IIA) reporting that global losses from cyber incidents reached USD 8 trillion in 2023, and ransomware attacks are projected to increase financial damages to USD 265 billion by 2031 (Tempo.co, 2022). Despite the global nature of this threat, international cooperation remains hindered by regulatory inconsistencies, policy misalignment, and the reluctance of states to share strategic cybersecurity intelligence (Winarko, H., & Avianto, L., 2024; Cloramidine & Badaruddin, 2023). Indonesia faces severe cybersecurity vulnerabilities, ranking among the lowest three G20 nations on the National Cyber Security Index (NCSI) 2022, with a score of 38.96 out of 100 (Annur, 2022). In 2023, Indonesia recorded an average of 2,200 cyberattacks per minute, highlighting the inadequacy of existing cybersecurity mechanisms (Yonatan, 2023). A stark example is the June 2024 ransomware attack on Indonesia’s National Data Centre (PDN), which disrupted 210 government institutions, including immigration services, law enforcement agencies, and intelligence bodies (CNN Indonesia, 2024). This attack not only crippled public services but also heightened the risk of strategic data leaks, which could be exploited in the global geopolitical landscape.

The escalation of cyber threats on a global scale further reinforces the urgency for enhanced cybersecurity governance. The 2017 WannaCry ransomware attack affected more than 150 countries, causing losses exceeding USD 1 billion, while the NotPetya cyberattack inflicted USD 300 million in damages to Maersk’s logistics operations (Putri, 2021). Similarly, in 2020, the Carbanak and Cobalt hacking groups infiltrated over 100 financial institutions worldwide, a case that was resolved through joint efforts between Europol and the FBI (Rahman, 2020). Despite the necessity for international collaboration in combating transnational cyber threats, efforts remain constrained by fragmented regulations and geopolitical rivalries. The stalled United Nations 2024 cybercrime agreement negotiations underscore the difficulty in achieving global consensus on cybersecurity governance (Chernenko, Demidov, & Lukyanov, 2018).

From a legal perspective, Indonesia's cybersecurity regulatory framework remains inadequate in addressing the complexities of digital threats. The Electronic Information and Transactions (ITE) Law No. 19/2016 and the Personal Data Protection (PDP) Law No. 27/2022 fail to integrate comprehensive cybersecurity strategies within the global digital geopolitical landscape. Furthermore, the National Defence Law No. 3/2002 categorises cybercrime as a non-military threat but lacks a structured response mechanism. Presidential Regulation No. 47/2023 on National Cybersecurity Strategy and Cyber Crisis Management provides a strategic cybersecurity policy framework, yet its implementation remains largely reactive rather than preventive (Ditjen Pothan Kemenhan RI, 2023). Comparatively, Malaysia and Singapore have adopted more structured cybersecurity policies and robust digital defence ecosystems, positioning them ahead of Indonesia in cyber resilience (Lestari & Finaldin, 2022).

At the regional level, ASEAN has initiated cybersecurity collaboration through the ASEAN Regional Forum (ARF) and the development of ASEAN-CERT, a regional cybersecurity response mechanism. Malaysia and Singapore have established advanced cybersecurity ecosystems supported by comprehensive regulations and technological capabilities, whereas Indonesia continues to struggle with regulatory development, technological capacity-building, and cybersecurity workforce limitations (Putri, 2021). The Common Security Concept emphasises that regional cooperation is essential in addressing escalating cyber threats, particularly through regulatory harmonisation and improved multilateral coordination (Vivekanandan, 2016).

Addressing the increasing sophistication of cyber threats requires collective international action, as unilateral approaches remain insufficient in mitigating transnational risks. Without enhanced multilateral cooperation, states remain vulnerable to cyber-enabled disruptions. Given Indonesia’s rapid digitalisation, the country must adopt adaptive and innovative cybersecurity strategies to strengthen its digital defence mechanisms (Cloramidine & Badaruddin, 2023). Cybersecurity is fundamental to safeguarding digital infrastructure and protecting public service systems in the Nusantara Capital City (IKN) development. Strengthening cyber resilience within IKN is vital to mitigating transnational cyber threats and ensuring the security of critical digital assets (Saraswati & Adi, 2022). Doktoralina et al. (2024) highlight that IKN’s smart city transformation requires an integrated cybersecurity approach encompassing data protection, strategic information security, and public engagement to enhance digital resilience. Furthermore, previous studies stress the necessity of digital architecture transformation to strengthen secure data governance in support of national security (Doktoralina, 2023).

Thus, multilateral cooperation in cybersecurity must be optimised to reinforce Indonesia's digital defence mechanisms and enhance resilience against global cyber threats. This study aims to explore optimal strategies for strengthening multilateral cybersecurity cooperation to improve the effectiveness of cybercrime mitigation and enhance national vigilance. The research addresses the following questions:1)What are the barriers and enabling factors in multilateral cybersecurity cooperation?;2) How does multilateral cooperation impact national vigilance?;3)What optimal strategies can enhance the effectiveness of multilateral cybersecurity cooperation in addressing cyber threats?.

Literature Review

Cybersecurity constitutes a strategic pillar of national defence, particularly amid the escalating global threats in the digital domain. Neorealism Theory (Waltz, 1979) posits that states must strengthen their defence capabilities to safeguard stability and national interests (Sabry, 2024). In the cybersecurity context, nations with technological dominance exert control over global security systems, while those reliant on foreign technology remain highly vulnerable to data exploitation and external intervention. Consequently, Indonesia must develop independent cybersecurity capabilities to reduce dependency and enhance competitiveness within the international digital security ecosystem.

International Relations Theory (Bull et al., 1990) asserts that multilateral cooperation and diplomacy serve as primary instruments in fostering global cybersecurity stability. As a rapidly expanding digital economy, Indonesia must strengthen its engagement in forums such as the International Telecommunication Union (ITU) and ASEAN, leveraging strategic partnerships with other nations to bolster its cyber defence capacity.

Collective Security Theory (Gauhar & Palme, 1980) underscores that no state can unilaterally confront cyber threats, making a collective approach essential in mitigating cross-border cyberattacks. At the national level, National Vigilance Theory (Triwidodo et al., 2024) highlights the urgent need for early detection mechanisms and preparedness against strategic threats. In the realm of cybersecurity, Indonesia must adopt adaptive policies, strengthen regulatory frameworks, and enhance inter-agency coordination to ensure effective cyber deterrence.

Grounded in these theoretical perspectives, this study emphasises the critical role of comprehensive cybersecurity regulations and international cooperation in establishing a resilient and adaptive cyber defence system capable of addressing the challenges of the digital era.

Inhibiting and Supporting Factors in Multilateral Cybersecurity Cooperation

The primary inhibiting factor in multilateral cooperation on cybersecurity is the disparity in policies and regulations among nations. To date, no binding global agreement has been established regarding international cybersecurity standards. Although the United Nations General Assembly adopted Resolution No. 74 in 2019 to initiate an international convention on cybercrime, this agreement has yet to achieve global consensus as of the 2024 UN Assembly. Consequently, cyber diplomacy efforts are frequently hindered by national political and economic interests. Furthermore, reliance on foreign technology and low digital literacy levels in certain nations, including Indonesia, pose additional challenges to effective cooperation. Data indicate that Indonesia’s digital literacy rate stands at 62%, the lowest among ASEAN countries.

Conversely, supporting factors include various ongoing multilateral cooperation initiatives, such as the ASEAN Regional Forum (ARF) on Cybersecurity Initiatives, which aims to enhance cybersecurity capacity across Southeast Asia. Additionally, Indonesia has established collaborations with Japan, Australia, the United Kingdom, and the United States to strengthen digital forensics, enhance cybersecurity capabilities, and develop national cybersecurity policies. However, the effectiveness of these partnerships remains contingent on regulatory harmonisation at both domestic and international levels. Divergent standards and policies among nations frequently present barriers to the implementation of joint cybersecurity programmes.

The Impact of Multilateral Cooperation on National Vigilance

Multilateral cooperation in cybersecurity significantly contributes to enhancing national vigilance by strengthening digital defence capabilities and mitigating cyberattack risks. According to National Vigilance Theory, every state bears the responsibility of safeguarding its strategic infrastructure, including government information systems and citizens’ personal data. Indonesia has witnessed a substantial increase in awareness regarding the importance of cybersecurity, particularly following the cyberattack on the National Data Centre (PDN) in June 2024, which disrupted over 210 government institutions. This incident served as a turning point for the government, accelerating the implementation of national cybersecurity strategies through enhanced cooperation with partner nations.

However, challenges persist, particularly in the integration of national policies with international mechanisms. Indonesia continues to face regulatory constraints, as its domestic cybersecurity laws remain misaligned with international standards. Law No. 19/2016 and Law No. 27/2022 have yet to fully accommodate cross-border data protection and coordinated international cybercrime investigations. Resolving these shortcomings is fundamental to ensuring Indonesia's cybersecurity policies align with global best practices, thereby maximising the effectiveness of multilateral cybersecurity cooperation (Sarjito, A., 2024).

Optimal Strategies for Enhancing the Effectiveness of Multilateral Cooperation in Addressing Cyber Threats

Enhancing the effectiveness of multilateral cooperation in combating cyber threats requires a set of integrated strategies. One of the key measures is regulatory harmonisation and the strengthening of national cybersecurity policies. Domestic regulations must align with international standards to ensure that multilateral cooperation operates more effectively. Presidential Regulation (PERPRES) No. 47 of 2023 on the National Cybersecurity Strategy has served as an initial step in establishing a cyber defence framework. However, a comprehensive Cybersecurity Law is still needed. In comparison to Malaysia and Singapore, which have more advanced cybersecurity regulations, Indonesia must urgently strengthen its domestic regulatory framework to ensure the effectiveness of its international cooperation efforts.

Additionally, enhancing technological capacity and human resources is a critical factor in strengthening national cybersecurity. International cooperation should prioritise technology transfer and capacity-building initiatives for cybersecurity professionals. Indonesia continues to face a digital skills gap, necessitating more extensive training programmes and cybersecurity certification initiatives in collaboration with developed nations. Furthermore, strengthening the role of the National Cyber and Crypto Agency (BSSN) as the primary institution for national cybersecurity should be prioritised as part of Indonesia's digital defence strategy.

To enhance Indonesia's global standing, cyber diplomacy in international forums must be strengthened. Indonesia must actively contribute to cybersecurity negotiations in key global platforms, such as the G20, ASEAN, and the United Nations. Greater participation in international forums would reinforce Indonesia's position in discussions on global cybersecurity policies. Additionally, this diplomatic effort must be supported by cross-ministerial coordination and increased representation in international cybersecurity initiatives.

Moreover, strengthening cybersecurity infrastructure and crisis management is a key determinant of element of Indonesia's cybersecurity optimisation strategy. The national cybersecurity infrastructure must be reinforced to withstand increasingly sophisticated cyberattacks. PERPRES/47/2023 outlines cyber crisis management measures, but its implementation requires support from multiple stakeholders. Consequently, collaboration with the private sector and academia in the development of digital security technologies is a key factor in enhancing the effectiveness of the national cybersecurity system. By implementing these measures, Indonesia can enhance its digital resilience and improve its cyber deterrence capabilities against global cyber threats.

METHODS

This study adopts a qualitative research method with a descriptive-analytical approach, focusing on a comprehensive literature review. This approach enables an in-depth examination of multilateral cooperation in cybersecurity by assessing policies, regulations, and international best practices. The research primarily relies on secondary data from authoritative sources, including reports from international organisations, peer-reviewed academic journals, policy documents, and official government publications.

To systematically assess the effectiveness of multilateral cooperation in addressing cyber threats, this study integrates a SWOT analysis to identify strengths, weaknesses, opportunities, and threats associated with international cybersecurity collaboration. This structured evaluation ensures a comprehensive analysis of policy measures and regulatory effectiveness. Additionally, the research applies a deductive analytical approach, aligning existing theoretical models with empirical findings. This systematic method enhances analytical validity and reliability, ensuring that the findings provide actionable policy recommendations for Indonesia's cybersecurity governance. The following table 1 presents the operational definitions of key variables examined in this study:

Table 1. Operational Definitions of Key Variables

Research Variables	Operational Definition	Indicators	Research Process
Optimisation	Strengthening the effectiveness of multilateral cooperation in cybersecurity.	Efficiency of collaboration, enhancement of digital resilience, effectiveness of policy strategies.	Evaluation of regulatory frameworks and comparative analysis with other nations.
Multilateral Cooperation	International diplomatic relations involving multiple states to address global security challenges.	Participation in international forums, cybersecurity agreements, policy coordination across states.	Policy analysis and assessment of cybersecurity diplomacy.

Cybersecurity	The digital domain encompassing computer systems, networks, and information technology.	Frequency of cyberattacks, resilience of digital infrastructure, compliance with global security standards.	Collection of empirical data from cybersecurity reports and policy reviews.
National Vigilance	The state's preparedness to detect and prevent threats to national stability.	Cyber defence policies, digital literacy initiatives, cybersecurity incident response mechanisms.	Analysis of cyber threat trends and assessment of national regulatory preparedness.
Ransomware	Malware that encrypts or locks systems until a ransom is paid.	Number of ransomware attacks, economic consequences, mitigation strategies implemented.	Case study analysis of ransomware incidents and evaluation of government response policies.

Source: Author (2024)

To enhance data reliability, this study follows a systematic approach by consulting credible sources, including official documents from international institutions such as the International Telecommunication Union (ITU), reports from the Cybersecurity & Infrastructure Security Agency (CISA), and peer-reviewed research on cybersecurity governance. This structured methodology reinforces the analytical depth of the study, ensuring robust insights for policy development in Indonesia's cybersecurity landscape. The research follows the conceptual framework illustrated in Figure 1, which consists of three key analytical stages:

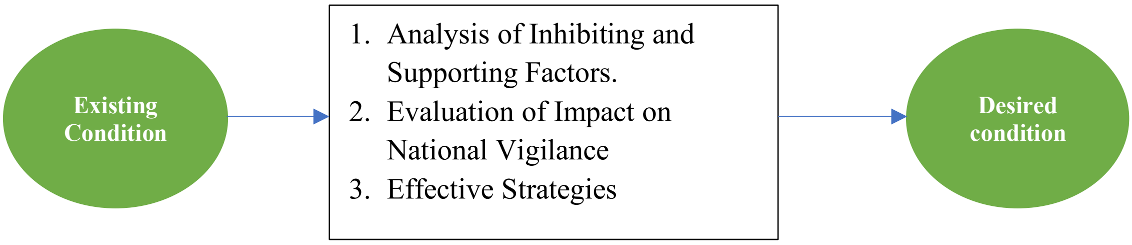
Existing Condition
1. Analysis of Inhibiting and Supporting Factors.
2. Evaluation of Impact on National Vigilance
3. Effective Strategies
Desired condition

Figure 1: Framework for Cybersecurity and Multilateral Cooperation

Stage 1: Problem Identification

This stage examines major cybersecurity threats, including ransomware attacks and transnational cyber risks, which threaten national sovereignty and cybersecurity preparedness. A key challenge in strengthening multilateral cybersecurity cooperation is the lack of comprehensive cybersecurity legislation, particularly the absence of a dedicated Cybersecurity Law, which is essential for establishing a robust legal foundation for cyber diplomacy.

Stage 2: Analysis of Supporting and Hindering Factors

This stage evaluates the barriers and facilitators of multilateral cooperation in cybersecurity. Key obstacles include regulatory misalignment, lack of coordination among stakeholders, and a shortage of cybersecurity expertise. Conversely, supporting factors include existing international agreements with ASEAN, G20, and the United Nations, along with increased governmental commitment to digital security.

Stage 3: Evaluation of Impact on National Vigilance

The final stage analyses how multilateral cooperation strengthens national vigilance against cyber threats that jeopardise economic security, critical digital infrastructure, political stability, and international relations. The analysis underscores how global collaboration enhances national cybersecurity frameworks and builds resilience against emerging cyber threats.

This methodological approach ensures a systematic and structured analysis of cybersecurity governance, providing policy-driven insights to enhance multilateral cooperation and reinforce national cybersecurity resilience.

RESULT AND DISCUSSION

The Impact of Multilateral Cooperation on National Vigilance

Multilateral cybersecurity cooperation significantly enhances national vigilance, particularly in human resource development, technology transfer, and cyber diplomacy. Engagement in international forums such as ITU and ARF enables Indonesia to access advanced security technologies while fostering capacity-building initiatives through joint training programmes and cross-border intelligence-sharing mechanisms.

However, the success of multilateral cooperation depends on regulatory alignment with international cybersecurity standards. Comparative studies show that Singapore and Japan have adopted progressive cybersecurity regulations, ensuring greater policy coordination and incident response preparedness. Meanwhile, Indonesia continues to grapple with fragmented policies and institutional inefficiencies, limiting the full potential of international partnerships.

From a public policy perspective, cybersecurity governance must be dynamic and adaptable to evolving technological threats (Safitra et al., 2023; Zaydi, 2024). The National Cyber and Crypto Agency (BSSN) is central to the integration of multilateral cybersecurity strategies into national policies. However, Indonesia remains heavily dependent on foreign cooperation to enhance cyber resilience. While international partnerships offer strategic advantages, self-reliance in cybersecurity governance must be prioritised to reduce long-term security risks.

Collective Security Theory emphasises that cyber threats cannot be mitigated through unilateral actions. Indonesia's engagement in multilateral forums reflects this strategic approach, where global cybersecurity is perceived as a shared responsibility. However, to optimise these collaborations, Indonesia must ensure adaptive policymaking that aligns with rapidly evolving digital threats.

Comparative Analysis of Indonesia's Cybersecurity Landscape

Neorealism Theory (Waltz, 1979) explains how technological superiority determines state power in global security structures. In cybersecurity, technologically advanced nations dominate international cyber governance, while less technologically independent states remain vulnerable to digital exploitation. Indonesia's heavy reliance on foreign digital infrastructure increases the risks of cyber espionage, data breaches, and strategic vulnerabilities.

A major regulatory shortfall in Indonesia's cybersecurity governance is the absence of a dedicated Cybersecurity Law. Existing regulations, such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP), fail to establish clear mechanisms for critical infrastructure protection or cross-border cybersecurity collaboration. Comparatively, Malaysia and Singapore have implemented more structured cybersecurity laws, enabling a more integrated response to cyber threats. To narrow this disparity, Indonesia must accelerate legislative efforts to introduce comprehensive cybersecurity policies that align with global cybersecurity frameworks.

Another critical challenge is the shortage of skilled cybersecurity professionals. Data from Indonesia's Ministry of Communication and Informatics indicate that 600,000 cybersecurity experts are needed annually, yet graduate output remains insufficient. The National Cyber and Crypto Agency (BSSN) remains integral to national cybersecurity management; however, limited human resource capacity hinders the agency's operational effectiveness. Compared to Singapore and Japan, which prioritise cybersecurity workforce development through education and industry partnerships, Indonesia must enhance academic collaboration and vocational training to meet growing cybersecurity demands.

Moreover, foreign technology dependency further weakens Indonesia's cyber resilience. Neorealism Theory asserts that technological disparities allow dominant nations to exert control over weaker states, influencing cybersecurity architectures and policy-making processes. Strengthening technological autonomy by investing in domestic cybersecurity research and development (R&D) is essential to mitigating foreign dependency risks and enhancing national strategic positioning in global cybersecurity governance..

The Impact of Multilateral Cooperation on National Vigilance

Multilateral cooperation is instrumental in reinforcing national vigilance by improving human resource capacity, facilitating technology transfer, and advancing cyber diplomacy. Active participation in international cybersecurity forums, including the International Telecommunication Union (ITU) and the ASEAN Regional Forum (ARF), provides Indonesia with access to advanced digital security technologies and facilitates capacity-building initiatives through training and knowledge exchange programmes. This engagement supports Indonesia's efforts to bridge technological gaps and improve cyber resilience against evolving threats.

Beyond capacity-building, collaborative mechanisms improve the early detection and prevention of organised cyber threats. Through structured information-sharing systems and intergovernmental coordination, Indonesia can enhance threat anticipation capabilities and implement proactive mitigation strategies. However, the effectiveness of these initiatives depends on the alignment of national regulations with global cybersecurity standards and the government's commitment to adaptive policy implementation. The National Cyber and Crypto Agency (BSSN), as Indonesia's leading body in cybersecurity governance, serves a key function in fortifying digital defence strategies. However, regulatory gaps, fragmented institutional coordination, and heavy reliance on foreign partnerships continue to undermine national cyber resilience. While international cooperation remains essential, Indonesia must prioritise self-reliance in cybersecurity governance by developing indigenous technologies, strengthening regulatory enforcement, and improving human capital.

From the perspective of Collective Security Theory, cyber threats are transnational in nature, requiring integrated global response mechanisms rather than unilateral action. Indonesia's participation in multilateral cybersecurity frameworks reinforces this principle by promoting collective digital resilience as a shared responsibility. However, to maximise the benefits of international collaboration, Indonesia must enhance regulatory flexibility, improve institutional coordination, and adopt strategic cybersecurity policies that align with the rapidly evolving digital threat landscape.

Regulatory and Strategic Gaps in Indonesia's Cybersecurity Governance

Cybersecurity regulations must be dynamic and adaptable to keep pace with rapid technological advancements and the growing complexity of cyber threats (Safitra, Lubis, & Fakhrurroja, 2023; Zaydi, 2024). Comparative studies indicate that Singapore and

Japan have implemented progressive cybersecurity models, featuring robust regulatory frameworks, strict enforcement mechanisms, and well-coordinated cyber defence strategies. In contrast, Indonesia continues to grapple with fragmented cybersecurity policies, hampering policy effectiveness and cross-sectoral collaboration. Despite recent regulatory advancements, Indonesia's cybersecurity framework remains inadequate in addressing cross-border cyber threats and requires stronger integration with international cybersecurity norms.

To enhance multilateral cooperation effectiveness, Indonesia must strengthen cross-sectoral coordination, involving academia, industry, and government agencies in developing a comprehensive digital security ecosystem. Public-private partnerships must also be reinforced, particularly in early detection systems, cyber threat intelligence-sharing, and technological innovation. Furthermore, reducing dependence on foreign cybersecurity solutions is essential to safeguarding national digital sovereignty. Indonesia should prioritise domestic cybersecurity industry development and increase investment in cybersecurity research, indigenous software development, and digital defence innovation.

Optimising Multilateral Cooperation through a Strategic Approach

To identify the most effective strategies for improving multilateral cybersecurity cooperation, a SWOT analysis assesses Indonesia's strengths, weaknesses, opportunities, and threats in digital defence. Table 2 provides an overview of the key internal and external factors influencing Indonesia's cybersecurity governance.

Table 2. SWOT Analysis of Multilateral Cooperation in Cybersecurity

INTERNAL	EKSTERNAL
STRENGTHS	**OPPORTUNITIES**
1) Active participation in multilateral cybersecurity forums, such as the ITU and ARF, fostering cyber diplomacy and technological collaboration 2) The existence of the National Cyber and Crypto Agency (BSSN), which serves as Indonesia's primary cybersecurity institution. 3) Strategic partnerships with major cybersecurity actors, including the United States, the United Kingdom, and Australia, to advance human resource capacity.	1) Escalating complexity and sophistication of cyber threats, making detection and prevention increasingly challenging. 2) Advancements in cybersecurity technologies that can be leveraged for strengthening Indonesia's cyber defence capabilities. 3) Increased access to training programmes, technical cooperation, and knowledge exchange initiatives from global cybersecurity leaders.

E-ISSN: 2830-5728

INTERNAL	EKSTERNAL
WEAKNESS	**THREATH**
1) Lack of a comprehensive Cybersecurity Law, resulting in legal ambiguity and policy fragmentation. 2) The demand for cybersecurity professionals in Indonesia stands at 600,000 per year, yet the available workforce remains significantly below the required level, highlighting an urgent need for capacity-building efforts. 3) Weak inter-agency coordination between government bodies, the private sector, and cybersecurity stakeholders, impeding effective threat response mechanisms.	1) Escalating complexity and sophistication of cyber threats, making detection and prevention increasingly challenging. 2) Over-reliance on foreign cybersecurity technology, increasing data security risks and potential external influence. 3) Regulatory inconsistencies between Indonesia and international partners, complicating policy harmonisation and multilateral cybersecurity cooperation.

Source: Processed by the author (2024)

Strategic Policy Recommendations for Strengthening Cybersecurity Cooperation

Given the findings of the SWOT analysis, Indonesia must adopt a series of strategic measures to optimise multilateral cybersecurity cooperation and enhance national vigilance against digital threats.

The first critical step is to enact a comprehensive Cybersecurity Law. Establishing a clear legal framework will provide the foundation for cross-border cyber defence cooperation and facilitate the mitigation of digital threats. With such legislation in place, international coordination in combating cybercrime can be better structured, while law enforcement against cross-border cyberattacks can become more effective.

In addition to regulatory aspects, strengthening human resource capacity in cybersecurity is essential to improving national digital resilience. Indonesia must forge strategic partnerships with leading cybersecurity technology providers, academic institutions, and international allies to develop a highly skilled cybersecurity workforce. This effort should include intensive training, certification programmes, and expert exchanges to ensure that Indonesia has professionals capable of addressing global cyber threats.

Furthermore, enhancing inter-agency coordination is crucial to strengthening the national cybersecurity system. Currently, coordination between government institutions, private-sector stakeholders, and cybersecurity experts remains inadequate, leading to slow responses to cyber incidents. To address this, an integrated mechanism must be established to enable real-time information sharing among relevant institutions. The implementation of artificial intelligence (AI)-driven systems and advanced analytics can accelerate early detection and response to evolving cyber threats.

Another strategic priority is to reduce reliance on foreign cybersecurity technology. At present, Indonesia depends significantly on foreign software and infrastructure, increasing the risk of strategic data breaches. To mitigate this, the government must encourage the development of a domestic cybersecurity industry by increasing investment in research and development (R&D) in digital security. Supporting cybersecurity start-ups and providing incentives for local industries will be key in fostering a self-sufficient and highly competitive national cybersecurity ecosystem.

Finally, expanding cyber diplomacy efforts in international forums is essential. Indonesia must take a more active role in global cybersecurity negotiations and advocate for stronger multilateral cooperation mechanisms. Participation in organisations such as the International Telecommunication Union (ITU), ASEAN Cybersecurity Cooperation, and other global cybersecurity forums will enhance Indonesia’s role in shaping international cybersecurity standards. Moreover, regulatory harmonisation with global cybersecurity standards must be pursued to ensure Indonesia’s adaptability to international policy changes and to strengthen collective digital resilience.

By implementing these measures, Indonesia can maximise the benefits of multilateral cooperation, strengthen its national cybersecurity infrastructure, and enhance resilience against increasingly complex threats in the digital transformation era. A well-structured and cross-sectoral policy approach will be key to establishing a robust and sustainable cybersecurity system.

CONCLUSION

This study confirms that multilateral cooperation in cybersecurity is essential for Indonesia in addressing complex and transnational cyber threats. However, regulatory deficiencies, a shortage of cybersecurity professionals, and reliance on foreign technology remain key challenges. Additionally, policy inconsistencies and geopolitical tensions hinder international cybersecurity harmonisation. Despite these obstacles, Indonesia’s engagement in global forums such as the International Telecommunication Union (ITU), the ASEAN Regional Forum (ARF), and the ASEAN Political-Security Community (APSC) offers opportunities to enhance human resource capacity, adopt advanced cybersecurity technologies, and strengthen collective security mechanisms. The effectiveness of these cooperative efforts depends on comprehensive national policy reforms, institutional capacity-building, and increased investment in cybersecurity infrastructure to reduce external dependency. The government must prioritise the enactment of a comprehensive Cybersecurity Law, improve cross-sectoral coordination among key institutions, and advance regional regulatory harmonisation within ASEAN to establish an integrated cybersecurity response mechanism. Strengthening collaboration with INTERPOL, UNODC, and ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) will enhance cybercrime prevention frameworks and digital forensic capabilities.

Long-term policies should focus on expanding cybersecurity investment, fostering domestic innovation, and reducing dependency on foreign technologies. Establishing a national cybersecurity task force, modelled after Singapore's Cyber Security Agency (CSA) and Japan's National Centre of Incident Readiness and Strategy for Cybersecurity (NISC), would improve cyber incident response and crisis management. Future research should explore case studies from leading cybersecurity nations, apply quantitative risk assessments, and analyse geopolitical risks and foreign technology dependency to guide Indonesia's cybersecurity strategy and digital sovereignty efforts. Strengthening multilateral cooperation while enhancing national cybersecurity autonomy will enable Indonesia to develop a resilient and adaptive digital security framework in response to evolving global cyber threats.

REFERENCE

Aida, A. N. (2021). *Kondisi keamanan siber Indonesia. Budget Issue Brief Politik dan Keamanan, 7*(12), 1-2. Retrieved from https://berkas.dpr.go.id/pa3kn/analisis-tematik-apbn/public-file/bib-public-65.pdf

Annur, C. M. (2022). Indeks keamanan siber Indonesia peringkat ke-3 terendah di antara negara G20. *Databoks Katadata.* Retrieved from https://databoks.katadata.co.id

Bull, H., Kingsbury, B., & Roberts, A. (1990). *Hugo Grotius and international relations*. Retrieved from https://books.google.co.id/books?id=KwhREAAAQBAJ

Chernenko, E., Demidov, O., & Lukyanov, F. (2018). *Increasing international cooperation cybersecurity and adapting cyber norms.* Retrieved from https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

Cloramidine, F., & Badaruddin, M. (2023). Mengukur keamanan siber Indonesia melalui indikator pilar kerja sama dalam Global Cybersecurity Index (GCI). *Populis: Jurnal Sosial dan Humaniora, 8*(1), 57-73. Retrieved from https://journal.unas.ac.id/populis/article/view/1957

CNN Indonesia. (2024). Infografis: Ancaman global 10 tahun ke depan. *CNN Indonesia.* Retrieved from https://www.cnnindonesia.com/teknologi/20240129094459-188-1055577/infografis-ancaman-global-10-tahun-ke-depan

Direktorat Jenderal Potensi Pertahanan, Kementerian Pertahanan Republik Indonesia. (2023). *Perlunya pembangunan sistem pertahanan siber (Cyber Defense) yang tangguh bagi Indonesia.* Kementerian Pertahanan RI. Retrieved from https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber%20Defence.pdf

Doktoralina, C. M. (2023). Optimasi konsep satu data arsitektur digital: Suatu kerangka konsep analisis ketahanan nasional. *Jurnal Lemhannas RI, 11*(3), 202-210. https://doi.org/10.55960/jlri.v11i3.480

Doktoralina, C. M., Nugroho, L., Putra, Y. M., & Prabantoro, A. M. P. (2024). Framing smart city in Indonesia's new capital: Integrating technology, culture, and public participation. *Business, Management & Accounting Journal (BISMA), 1*(2), 92-99. https://doi.org/10.70550

Fanasafa, I. (2022). Jenis kejahatan siber serta cara pencegahannya. *Direktorat Jenderal Kekayaan Negara, Kementerian Keuangan Republik Indonesia.* Retrieved from https://www.djkn.kemenkeu.go.id/artikel/baca/15712/Kenali-Dunia-SiberWaspadai-Kejahatannya-Bagian-I.html

Gauhar, A., & Palme, O. (1980). Olof Palme. *Third World Quarterly, 2*(4), 633-647. https://www.jstor.org/stable/3990868

Kinne, B. J. (2018). Defense cooperation agreements and the emergence of a global security network. *International Organization, 72*(4), 799-837. https://doi.org/10.1017/S0020818318000218

Kementerian Luar Negeri Republik Indonesia. (2022). *Kerja sama multilateral Indonesia dalam bidang keamanan siber dan diplomasi digital.* Retrieved from https://kemlu.go.id/portal/id/read/89/halaman_list_lainnya/kejahatan-lintas-negara

Lestari, M., & Finaldin, T. (2022). Kerja sama antara Indonesia dan negara-negara di Asia Tenggara melalui ASEAN Regional Forum dalam bidang keamanan siber. *Global Mind, 4*(2), 27-42. https://doi.org/10.53675/jgm.v4i2.987

Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Retrieved from https://peraturan.bpk.go.id/Details/255542/perpres-no-47-tahun-2023

Putri, K. V. K. (2021). Kerja sama Indonesia dengan ASEAN mengenai cyber security dan cyber resilience dalam mengatasi cyber crime. *Jurnal Hukum Lex Generalis, 2*(7), 542-554. https://doi.org/10.56370/jhlg.v2i7.90

Rahman, L. L. A. (2020). Implikasi diplomasi pertahanan terhadap keamanan siber dalam konteks politik keamanan. *Jurnal Diplomasi Pertahanan, 6*(2), 1-93. https://doi.org/10.33172/jdp.v6i2.654

Sabry, F. (2024). *Neorealism in international relations: Understanding power and conflict in a changing world.* One Billion Knowledgeable. Retrieved from https://books.google.co.id/books?id=eVIZEQAAQBAJ

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), 13369. https://doi.org/10.3390/su151813369

Saraswati, M. K., & Adi, E. A. W. (2022). Pemindahan Ibu Kota Negara ke Provinsi Kalimantan Timur berdasarkan analisis SWOT. *Oratio Journal*. Retrieved from https://ejurnal.ubk.ac.id/index.php/oratio/article/view/163

Sarjito, A. (2024). Technological pride and national resilience: How innovation shapes stability and security. *Jurnal Lemhannas RI, 12*(3), 277-298. https://doi.org/10.55960/jlri.v12i3.940

Tempo.co. (2022). Kerugian akibat kejahatan siber diperkirakan capai ratusan ribu triliun rupiah. *Tempo.co.* Retrieved from https://www.tempo.co/read/1587273/kerugian-akibat-kejahatan-siber-diperkirakan-capai-ratusan-ribu-triliun-rupiah

Triwidodo, I., Hasyim, M., Fuddin, A. H., Gutomo, Wingarta, I. P. S., & Chasib, A. (2024). *Bahan ajar: Kewaspadaan nasional* (Direktorat Materi dan Penilaian Peserta Kedeputian Bidang Pendidikan Pimpinan Tingkat Nasional, Ed.). Lemhannas Press.

Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara. Retrieved from https://peraturan.bpk.go.id/Details/44421/uu-no-3-tahun-2002

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Retrieved from https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Retrieved from https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Undang-Undang Republik Indonesia Nomor 24 Tahun 2000 tentang Perjanjian Internasional. Retrieved from https://peraturan.bpk.go.id/Details/44991/uu-no-24-tahun-2000

Undang-Undang Republik Indonesia Nomor 37 Tahun 1999 tentang Hubungan Luar Negeri. Retrieved from https://peraturan.bpk.go.id/Details/45358/uu-no-37-tahun-1999

Vivekanandan, B. (2016). Olof Palme. In *Global visions of Olof Palme, Bruno Kreisky and Willy Brandt* (pp. 27-45). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-33711-1_2

Winarko, H., & Avianto, L. (2024). Strengthening digital transformation of mass media for national resilience. *Jurnal Lemhannas RI, 12*(1), 109-116. https://doi.org/10.55960/jlri.v12i2.559

Yonatan, A. Z. (2023). *10 negara kontributor serangan siber Indonesia terbesar 2023.* Retrieved from https://data.goodstats.id/statistic/10-negara-kontributor-serangan-siber-indonesia-terbesar-2023-ro05C

Zaydi, M. (2024). *A new framework for agile cybersecurity risk management.* In *Agile security in the digital era: Challenges and cybersecurity trends* (p. 19). Retrieved from https://books.google.co.id/books?id=NaM2EQAAQBAJ

Ziemke-Dickens, C., & Droogan, J. (2010). *Asian transnational security challenges: Emerging trends, regional visions.* Macquarie University, Centre for Policing, Intelligence and Counter Terrorism (PICT) [in association with] The Council for Asian Transnational Threat Research (CATR).