https://nawalaeducation.com/index.php/SG/index
Volume 1 Nomor 2, November 2024
E-ISSN : 3047-9339
DOI : https://doi.org/10.62872/rw69zn27

National Security Strategies Amidst Increasing Global Cyber Threats: A Multilateral Approach

Loso Judianto
IPOSS Jakarta, Indonesia
e-mail: losojudijantobumn@gmail.com

INFO ARTIKEL

Entered
October 10, 2024
Revised
November 11, 2024
Accepted
November 20,2024
Published
November 30, 2024

Keywords:
Cyber Threats, National Security, Multilateral Cooperation, Security Strategy, Information Technology

ABSTRAK

In today's digital age, the development of information technology has a significant impact on various sectors, including the economy, politics and security. While technology provides opportunities for efficiency and innovation, it also introduces increasingly complex cyber threats. Cyberattacks now target not only individuals, but also large institutions, multinational corporations and governments, resulting in economic losses and threatening the socio-political stability of a country. Indonesia, like many other countries, faces growing cyber threats, including e-HAC data leaks and ransomware attacks. These threats require a multilateral approach due to their cross-border nature and the involvement of highly capable actors, whether individuals, criminal groups or specific states. This research aims to explore national security strategies in dealing with global cyber threats through a multilateral approach. The main focus is to identify how international cooperation can improve the effectiveness of a country's cybersecurity and analyze the challenges in implementing this strategy. Using a qualitative approach and descriptive-analytical design, this research collected secondary data from official documents, reports of international organizations, as well as relevant journal articles. The results of this research are expected to provide useful recommendations for policymakers in formulating national security strategies that are more resilient and responsive to evolving cyber threats.

INTRODUCTION

In today's digital era, the transformation of information technology has brought significant changes in various aspects of life, from economics, politics, to security. The widespread use of technology creates great opportunities for efficiency and innovation, but also opens up space for ever-evolving cyber threats. Cyberattacks now target not only individuals, but also large institutions, multinational companies, and governments. This results in losses that are not only economic but also affect the social and political stability of a country. This phenomenon can be seen from the increase in cyberattacks in various parts of the world. The United States, for example, experienced an attack on the Colonial Pipeline network in 2021, which caused serious disruptions in energy supply in the eastern region of the country (U.S Department of Homeland Security; Kilovaty, 2023). The UK faced a critical situation when the WannaCry ransomware attacked its national

health system (NHS) in 2017, disrupting public health services (Wardle, 2017). In Asia, Singapore fell victim to a large-scale data hack in 2018, where the personal information of more than 1.5 million citizens, including the Prime Minister's medical data, was stolen by cybercriminals (Tham, 2018).

Indonesia is not immune to this threat either. Several significant cyberattack incidents have occurred, one of which was the data leak from the e-HAC (Electronic Health Alert Card) system in 2022 involving the personal data of millions of citizens (Sari, 2022). In addition, sensitive government data, such as diplomatic documents and civil registration information, were also reportedly leaked and traded on digital black markets. These incidents point to gaps in the national digital infrastructure that require serious attention to prevent further losses in the future. These attacks are characterized as cross-border and involve highly capable actors, whether individuals, international criminal groups or specific states. These organized attacks are often difficult for a single country to track and counter, requiring international cooperation. This requires countries to not only develop comprehensive national cybersecurity strategies, but also build stronger multilateral cooperation to address increasingly complex global threats (Badan Siber dan Sandi Negara, 2023).

Previous research has discussed the importance of a multilateral approach in addressing global cyber threats. Nye (2017) highlighted that international collaboration is key in building effective cybersecurity. Dunn Cavelty (2018) underlined the need for strategies that focus not only on prevention but also adaptive response to attacks. Other research identifies the role of multilateral organizations, such as the United Nations (UN), NATO and ASEAN, in encouraging cybersecurity collaboration between countries (United Nations, 2020). However, while this approach is considered effective, its implementation still faces major challenges, including differences in political interests, technological gaps and lack of trust between countries.

Indonesia's efforts to improve cybersecurity have begun, such as the establishment of the National Cyber and Crypto Agency (BSSN), which is tasked with overseeing and securing the national digital system (Presidential Regulation No. 133 of 2017). However, challenges still arise, especially in the face of large-scale attacks involving international actors. Indonesia's cybersecurity is also affected by the level of technological readiness, suboptimal regulations, and coordination between the government and the private sector that still needs to be improved. This situation shows that Indonesia needs a more mature strategy and international support to effectively counter cyber threats. A multilateral approach is considered to be one potential solution. With international cooperation, countries can share information, technology and resources to tackle cyberattacks more efficiently. In the Southeast Asian region, for example, ASEAN has initiated various frameworks for regional cybersecurity (ASEAN Cybersecurity Cooperation Strategy, 2022). However, the level of implementation and commitment among member states still varies, so the effectiveness of this cooperation needs to be improved.

This research aims to explore national security strategies in the face of global cyber threats using a multilateral approach. The main focus is to identify how international cooperation can improve the effectiveness of a country's cybersecurity, as well as analyze the obstacles that arise in implementing this approach. The results of this research are expected to provide relevant recommendations for policymakers in formulating national security strategies that are resilient and responsive to global cyber threats.

METHODOLOGY

This research uses a qualitative approach with a descriptive-analytical design to explore national security strategies in dealing with global cyber threats through a multilateral approach. According to Creswell (2014), a qualitative approach is suitable for research that aims to understand phenomena in depth through descriptive data analysis. The descriptive-analytical design allows researchers to map the phenomenon, identify challenges and provide strategic recommendations based on the available data. The data sources in this research are entirely derived from secondary data, as suggested by Yin (2018) in case study-based studies, which include official government documents, such as the annual reports of the National Cyber and Crypto Agency (BSSN) as well as national cybersecurity regulations; reports of international organizations, such as cybersecurity reports from ASEAN, the United Nations (UN), and NATO; scientific journal articles and books related to cybersecurity; as well as news from trusted mass media that report global and national cyberattack incidents. This secondary data is able to provide rich and relevant information to support analysis and interpretation.

Data collection techniques were conducted through literature studies, document analysis, and news searches. As explained by Bowen (2009), document analysis is an effective method for reviewing data available in the form of written text to understand the context of the research. The literature study was conducted by browsing scientific articles, reports, and books from academic databases, such as Google Scholar, Springer, or ScienceDirect. Yin (2018) mentions that desk research is an efficient method in research that utilizes secondary data without requiring direct primary data collection. Document analysis includes policy reviews, annual reports, and official data published by government agencies and international organizations. News searches were conducted to gather the latest information on global cyberattack incidents and multilateral cooperation efforts, focusing on credible news sources. The collected data was analyzed using the content analysis method. Elo and Kyngäs (2008) explain that content analysis is effective for systematically categorizing unstructured data and helping to identify key patterns. The analysis steps included data reduction, which selected information relevant to the research focus; categorization of data into key themes, such as cyber threats, national responses, and multilateral initiatives; and interpretation to understand the relationships between concepts and draw in-depth conclusions.

The unit of analysis in this study is national cybersecurity policy and practice, focusing on Indonesia's efforts as well as multilateral initiatives involving ASEAN, the UN or NATO. As stated by Miles and Huberman (1994), the unit of analysis is necessary to define the boundaries of the research focus and assist the researcher in interpreting the data in a targeted manner. This study also includes case analysis of data leaks in Indonesia and international cybersecurity cooperation to provide a more specific context to the research objectives. In ensuring the validity of the data, this study applied source triangulation, as proposed by Patton (1999), by comparing information from different types of documents, journal articles, and trusted media reports. In addition, data consistency was also tested by comparing findings from different sources to ensure that the data used was valid and reliable

RESULTS AND DISCUSSION

Cybersecurity is currently a very relevant and urgent issue in many countries, including Indonesia. Countries are increasingly recognizing that cyber threats, which transcend geographical boundaries, require close international collaboration. Efthymiopoulos' report (2019) highlights that NATO, through innovative strategies such as the establishment of Cyber Operations Centers, has improved its cyber resilience. ASEAN, through its cybersecurity strategy 2023, has also focused on information sharing and joint training. Increasing cyber threats, whether from individuals, organized groups or states, have had a profound impact on vital sectors such as banking, energy, health and government. As a country that increasingly relies on digital technology, Indonesia is not exempt from this threat. The annual report of Indonesia's National Cyber and Crypto Agency (BSSN) in 2023 shows that Indonesia has faced more than 3,000 cyberattacks targeting various sectors, with most attacks focusing on the government and critical sectors. According to BSSN (2023), ransomware, phishing, and malware-based attacks are the most common threats. This rise in attacks shows that Indonesia's digital infrastructure is vulnerable to evolving cyber threats from both domestic and international actors.

Global and National Cyber Threats

The cyber threats facing Indonesia reflect broader global trends. The annual report from ASEAN (2023) states that ransomware attacks are one of the biggest threats facing ASEAN member countries, including Indonesia. In the report, ASEAN highlighted the importance of strengthening joint cybersecurity policies to respond to threats involving transnational actors. Attacks on the world's largest energy companies, such as Colonial Pipeline in the United States, involving ransomware, show how this threat knows no borders and has a global impact (UN, 2022). According to BSSN (2023), Indonesia has also been the target of cyberattacks with significant impact on national critical infrastructure, such as attacks on tax information systems and personal data.

Ransomware and data leaks are increasingly becoming serious threats to cybersecurity in the ASEAN region. According to IBM Security's 2023 report, the average cost of data leakage in Southeast Asia reached a record USD 3.05 million. The financial services and energy sectors face even greater losses, largely due to breaches involving mixed data environments, such as public and private clouds, which complicate detection and mitigation. The use of automation and artificial intelligence (AI) technologies is proven to reduce the duration of breach handling by 99 days, saving USD 1.25 million per incident (Tech Wire Asia, 2023). In Indonesia, the rapid adoption of digital technologies increases the risk of cyberattacks, especially ransomware targeting critical infrastructure such as the energy and financial sectors. However, challenges such as gaps in the adoption of cybersecurity technologies and weak regional regulations are significant barriers. While reporting to authorities can speed up resolution and reduce financial losses, many organizations in the ASEAN region are reluctant to do so for fear of complicating the situation (FutureCIO, 2023; Tech Wire Asia, 2023).

Threats to personal data are also a major concern in Indonesia. Based on data from BSSN, throughout 2022 there were more than 1,000 data leakage incidents involving millions of Indonesians. At the global level, the UN in its cybersecurity report (2023) revealed that personal data protection is becoming an increasingly important issue, with

many countries facing difficulties in effectively tackling data leaks. The increase in cyber-attacks, both individual and more organized, requires countries to continue developing policies and infrastructure that can protect sensitive data from cyber threats.

The threat to personal data in Indonesia is increasingly alarming. According to data from the National Cyber and Crypto Agency (BSSN), more than 1,000 data leak incidents were recorded in 2022, involving millions of citizens. One significant incident was the leak of Indonesian passport data involving more than 34 million individuals, increasing the risk of identity theft and fraud (Hope, 2023). Additionally, a ransomware attack targeting Bank Syariah Indonesia in 2023 led to the theft of up to 1.5 terabytes of data (CNN Indonesia, 2024). At the global level, the United Nations (2023) highlighted that many countries face major challenges in protecting their personal data from leaks, which demands policy updates as well as closer international collaboration to effectively improve cybersecurity.

National Response to Cyber Threats

Indonesia has taken various steps to respond to cyber threats, which are reflected in existing policies and regulations. One important step was the establishment of BSSN in 2017, which has the mandate to coordinate and implement national cybersecurity policies. Based on BSSN's annual report (2023), some of the policies that have been implemented include the development of cybersecurity standards, the strengthening of cyber protection infrastructure in the public and private sectors, and increasing public awareness regarding the importance of personal data security. In addition, stricter regulations related to personal data protection were also implemented through the Personal Data Protection Law (PDP Law), which came into effect in 2024. Nonetheless, major challenges remain, including the lack of human resources trained in cybersecurity and reliance on foreign technologies that are vulnerable to cyber threats.

In the BSSN annual report (2023), it is mentioned that Indonesia has also started efforts to strengthen cooperation between the public and private sectors in dealing with cyberattacks. One of them is a cybersecurity training and certification program for the workforce that aims to strengthen capabilities and knowledge in the face of increasingly complex cyberattacks. However, the biggest challenge facing Indonesia is the shortage of human resources trained in cybersecurity. BSSN (2023) notes that Indonesia still lacks experts who can handle increasingly sophisticated cyber threats. In a study published by Mardiasmo et al. (2020), it was found that the lack of effective training in cybersecurity is one of the biggest obstacles in creating adequate cyber defenses in Indonesia. In addition, efforts to raise awareness of the importance of cybersecurity among the public are also still limited, despite BSSN's efforts to increase public understanding through various campaigns.

Multilateral Cooperation in Cyber Security

Increasingly global cyber threats encourage the importance of multilateral cooperation in building better cyber resilience. Countries around the world are increasingly recognizing that cyber threats know no borders and require closer collaboration at the international level. A UN report (2022) shows that member states have begun to introduce more cooperative international policies, such as agreements on personal data protection and regulations on cyberattacks that lead to critical infrastructure damage. One notable example is the UN's Group of Governmental Experts (GGE), which encourages the establishment of international norms in dealing with cyber threats. The

UN also encourages countries to work together to build national capacity and share information about threats that could affect other countries.

In the Southeast Asian region, ASEAN has committed to strengthening cooperation in cybersecurity through the ASEAN Cybersecurity Cooperation Strategy published in 2023. The ASEAN Report (2023) highlights the importance of establishing information exchange centers and joint training to improve the capacity of member states to deal with cyber threats. Indonesia, as a member of ASEAN, has actively participated in various such initiatives, including joint exercise programs and information sharing on cyber attack trends. In this context, this multilateral cooperation is crucial to strengthen Indonesia's ability to detect and respond to increasingly complex cyber threats.

At the global level, NATO also plays an important role in strengthening its members' cyber defenses. NATO in its cyber security report (2022) revealed that cyber attacks have become one of the main threats to the collective security and stability of the alliance. NATO has developed policies that enable its member states to assist each other in addressing cyberattacks, including sharing information and technology to strengthen cyber defenses. NATO also conducts joint exercises to improve the readiness of its member states to respond to increasingly dynamic cyber threats. This shows the importance of multilateral cooperation in dealing with transnational threats.

Although multilateral cooperation in cybersecurity has been strengthened, major challenges remain in its implementation. Differences in the level of technological and policy readiness between countries are the main obstacles in strengthening global cyber resilience. Developed countries such as the United States, the United Kingdom and European Union member states have more mature cybersecurity infrastructure and policies, while developing countries, including Indonesia, still face limitations in terms of resources and technology. According to research by Li et al. (2021), these differences in technological capacity and policy readiness can affect the effectiveness of multilateral cooperation in addressing cyber threats. He emphasized the importance of addressing the technology gap between countries to make multilateral cooperation more effective in dealing with dynamic cyber threats

CONCLUSION

Increasingly complex cyber threats that transcend national borders demand more adaptive and coordinated national security strategies. A multilateral approach has proven to be an important solution to address global cyber threats by sharing information, technology and resources. While Indonesia has initiated strategic measures to strengthen its cybersecurity, such as the establishment of the National Cyber and Crypto Agency (BSSN), major challenges remain in addressing large-scale attacks and international actors. The success of this strategy relies heavily on international cooperation, which must be strengthened through improved infrastructure, collective awareness and technological capacity building across countries. Through joint efforts, countries can enhance global cyber resilience that is more effective and responsive to increasingly sophisticated threats.

LITERATURE

ASEAN. (2022). *ASEAN Cybersecurity Cooperation Strategy*. ASEAN Secretariat. https://asean.org

Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan Tahunan BSSN 2023*. Badan Siber dan Sandi Negara Republik Indonesia. https://www.bssn.go.id

Bowen, G. A. (2009). *Document analysis as a qualitative research method.* Qualitative Research Journal, 9(2), 27-40.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

Dunn Cavelty, M. (2018). *Cybersecurity and threat politics: US efforts to secure the information age.* Routledge.

Efthymiopoulos, M.P. A cyber-security framework for development, defense and innovation at NATO. *J Innov Entrep* 8, 12 (2019). https://doi.org/10.1186/s13731-019-0105-z

Elo, S., & Kyngäs, H. (2008). *The qualitative content analysis process.* Journal of Advanced Nursing, 62(1), 107-115.

Li, J., Wang, Y., & Zhang, H. (2021). *Cybersecurity Collaboration: Challenges and Opportunities in International Cooperation*. *Journal of Cybersecurity*, 16(1), 1-16. https://www.sciencedirect.com/science/article/pii/S2452074820300560

Mardiasmo, D., Santoso, D., & Pratama, R. (2020). *Human Resources Development for Cybersecurity in Indonesia: Issues and Challenges*. *Springer* https://link.springer.com/chapter/10.1007/978-3-030-36194-1_12

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Sage Publications.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44-71.

Organization of American States (OAS). (2018). *Latin American and Caribbean Cybersecurity Trends.* Washington, D.C.: OAS.

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Services Research, 34*(5), 1189-1208.

PBB (Perserikatan Bangsa-Bangsa). (2022). *Global Cybersecurity Threats and the Role of International Cooperation*. United Nations. Tautan: https://www.un.org/en/cybersecurity

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management.* CRC Press.

Peraturan Presiden Republik Indonesia Nomor 133 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN).

Perserikatan Bangsa-Bangsa (PBB). (2020). *Cybersecurity and International Peace and Security: Challenges and Developments.* United Nations Office for Disarmament Affairs.

Radoniewicz, F. (2022). International Regulations of Cybersecurity. In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) Cybersecurity in Poland. Springer, Cham. https://doi.org/10.1007/978-3-030-78551-2_5

Sari, D. K. (2022). Ancaman Kebocoran Data di Indonesia: Tantangan dan Solusi. *Jurnal Keamanan Siber*, 4(1), 23-35.

Tham, I. (20 July, 2018). "Singapore health data hack affects 1.5 million, including PM Lee." *The Straits Times*. Retrieved from https://www.straitstimes.com.

U.S. Department of Homeland Security. (2021). *Colonial Pipeline Ransomware Attack and Lessons for Critical Infrastructure.* Washington, D.C.: DHS.

Wardle, A. (2017). *WannaCry ransomware attack: A global perspective.* Cybersecurity Journal, 9(2), 15-30.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*. Sage Publications.

Tech Wire Asia. (2023). *The cost of a data breach in ASEAN: Record-high costs and increased complexity*. Tech Wire Asia. https://techwireasia.com

FutureCIO. (2023). *The growing role of AI in Southeast Asia cybersecurity*. FutureCIO. https://futurecio.tech

IBM Security. (2023). *Cost of a Data Breach Report*. IBM Security. https://www.ibm.com/security/data-breach

CNN Indonesia. (13 Mei, 2023). *Ransomware Lockbit 3.0 Klaim Lumpuhkan BSI dan Curi Data Pengguna.* https://www.cnnindonesia.com/teknologi/20230513093401-185-949046/ransomware-lockbit-30-klaim-lumpuhkan-bsi-dan-curi-data-pengguna

Hope, A. (13 July, 2023). *Data breach involving over 34 million Indonesian passports highlights security risks*. Retrieved from https://www.cpomagazine.com/cyber-security/