International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 2, Number 4, February 2023, *Page. 1326 - 1333*
Email : editorijhess@gmail.com

Cyber Diplomacy
(A Perspective From Indonesia - Australia Cyber Cooperation)

Ujang Priyono[1], Yoedhi Swastanto[2], Budi Pramono[3]
[1]Study Program of Defense Diplomacy, Faculty of Defense Strategy,
[2,3]Post-Graduated Program of the Republic of Indonesia Defense University, Jakarta, DKI Jakarta, Indonesia

*Corresponding Autor
E-mail: masterjaunk@gmail.com, yoedhiswastanto83@gmail.com, budi.pram@idu.ac.id

Abstract

To address the increasing cyber threats, Indonesia is attempting to develop its cyber capabilities, one of which is collaboration with Australia. In practicing cyber diplomacy, the two countries employ different diplomatic models. Indonesia conducts cyber diplomacy through the Ministry of Foreign Affairs and the National Cyber and Crypto Agency (BSSN), whereas Australia conducts it through its cyber ambassador. This research will investigate how the Indonesian and Australian cyber diplomacy models work in cyber diplomacy using a descriptive-analytic approach. Based on the research results, even though Indonesia already has BSSN as the leading cybersecurity sector, Indonesia's foreign policy continues to emphasize the role of the Ministry of Foreign Affairs as the leading sector of foreign policy diplomacy. including dialogue or bilateral collaboration with other countries in the sphere of cybersecurity. This, of course, extends the coordinating framework for carrying out cyber cooperation. As a result, efforts by the Indonesian government are required to develop more effective cyber diplomacy policies in order to enhance Indonesia's cyber capabilities.

Keywords: **Cyber Security, Cyber Cooperation, Cyber Diplomacy, Indonesia - Australia**

INTRODUCTION

According to data from Pusat Operasi Keamanan Siber Nasional (National Cyber Security Operations Center) BSSN, there has been a two-fold rise in cyber attacks against Indonesia from 2020 to 2021. There have been roughly 490 million cyberattacks during the first year of the Covid-19 pandemic, with a huge spike of nearly one billion cyberattacks in 2021. This record indicates that the trend of cyber-attacks will continue to rise as people shift from physical to online activities. Malware infection is the most frequent attack, accounting for 62% of all attacks, followed by trojan activity (10%) and target information collection effort (9%). Attacks reached a record high of 1.652.521.839 by end of 2021, and it is expected that number will continue to grow in 2022. According to research by Frost and Sullivan that was started for Microsoft in 2018, cyber security has cost Indonesia a deficit of up to 478.8 trillion IDR, or 34.2 billion USD, and it continues to grow on occasion.

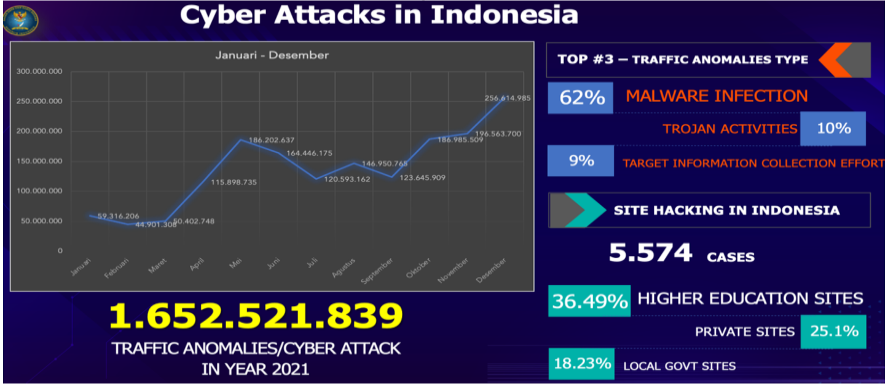

Figure 1 Indonesia`s Cyber Attack 2021
Source : www.bssn.go.id

Based on these conditions, one of the foundations for growing cyber security is Indonesia's attempts to build cyber security capacities through cooperation with other parties/countries. As a result, on August 31, 2018, a Memorandum of Understanding (MoU) was signed between BSSN (as the representative of Indonesia) and the Department of Foreign Affairs and Trade or DFAT (as the representative of Australia) to improve cyber security, which has become one of the Indonesian nation's international strategies to prevent cyber threats. The re-signing of the MoU between Indonesia and Australia in 2021, as one of the outcomes of the 2+2 dialogue summit between Indonesia and Australia, continues to strengthen this partnership.

Given this context, cyberspace requires adequate protection in order to avoid the potential for harm to individuals, companies, and even the state. To boost cyber security, Indonesia must undoubtedly collaborate with other countries that have superior cyber security capacities. The presence of cyber cooperation between Indonesia and Australia demonstrates this. This study will examine the model of cyber diplomacy employed by Indonesia in the development of cyber cooperation with Australia. The model here is related to the states' cyber cooperation methods and approaches. The opportunity is the Indonesian government's policy of cooperating in the cyber field in order to enhance national cyber capacity.

RESEARCH METHODS

To assess the problem, this paper employs a literature review. This article will use the descriptive-analytic method to investigate how the cyber diplomacy models of Indonesia and Australia perform in cyber diplomacy. To strengthen analysis and reasoning, data and information were gathered from relevant journals, books, and websites. This analysis will attempt to compare the Indonesian and Australian cyber diplomacy models derived from the data and material examined above in order to make recommendations to the Republic of Indonesia's government on how to construct effective cyber diplomacy

RESULT AND DISCUSSION

Definition of Cyber Diplomacy

According André Barrinha and Thomas Renard (2017) Cyber diplomacy is described as the utilization of diplomatic measures to secure a state's interests and goals in cyberspace. [1] All diplomatic methods are used in cyber diplomacy (both online and offline means of communication and information exchange). According to this definition, cyber diplomacy must be capable of performing at least four diplomatic functions: 1) information collection and reporting on the subject and/or the interests and activities of other governments and stakeholders; 2) Communications and public outreach about a state's foreign policy interests in relation to a cyber issue; 3) Negotiations about a state's foreign policy interests in relation to a cyber issue; 4) Diplomatic reactions to undesirable cyber activity, whether attributing the sources of an unwelcome cyber operation or imposing consequences on those that engage in it.[3] Diplomatic procedures and foreign policy or interests of a state should not be confused. Diplomacy is the means of communication, not the message itself. To be effective in cyber diplomacy, a state must first address its cyber foreign policy objectives. The scope and depth of the challenges addressed by cyber diplomacy are broad, and their importance to states is expanding.

The State's Role in Cyberspace

There are at least three reasons why states should learn about and undertake cyber diplomacy. First, cyberspace issues are becoming relevant and concerning not just a few select states, but all nations, including cybersecurity.[4] Threats in the digital domain have the ability to affect any country in a connected world, and they are increasingly doing so.

Second, diplomacy has a long history of addressing international issues and resolving crises before they develop or grow. Although cyberspace presents unique and dynamic difficulties, it is no more immune to diplomatic scrutiny than other complex global issues such as terrorism or climate change. Indeed, cyber diplomacy provides governments with a ready-made and reasonably efficient means of acquiring information about the challenges at hand as well as the perspectives and interests of other states and stakeholders. Aside from providing vital feedback, cyber diplomacy can assist states in advancing their ideas and foreign policy interests.

Third, cyber diplomacy talks are common and ongoing. States with cyber diplomacy capabilities can take part in these discussions and negotiate the terms and contents of any agreements that result. States lacking such power, on the other hand, will either be excluded from any agreements or accept them as a political decision.

States can thus engage in a myriad of readymade forums to address these concerns, such as:

- Bilateral dialogue: Through closed-door discussions and the identification of similar values and interests, states with a cyber diplomacy capacity can establish coalitions of like-minded states. They may also generate chances for cooperation and capacity building between two or more governments, as well as improve trust and confidence in a sphere where understanding other states' interests and capacities can be challenging.
- Regional forums: It allow governments to gather collective resources, establish political will, and reduce capacity gaps. The EU Diplomatic Toolbox, for example, offers a regional framework for preparing diplomatic measures to cyber operations.[5] Some regional organizations, such as the OAS, have internal cybersecurity capacities that may aid states who are new to these challenges.[11] Regional dialogues, such as the ASEAN-hosted "Asian Regional Forum" (ARF), provide a platform for states to express shared interests, facilitating communication, reducing tensions, and increasing prospects for agreement.
- Multilateral forums: Efforts at the United Nations have already resulted in agreement on numerous crucial cyber rules. 11 These discussions have usually occurred in the Group of Governmental Experts (GGE) on Information Security, which for the first time started in 2004.[8] [9] The sixth GGE, and also the Open-Ended Working Group on advancements in the field of ICTs in the Context of International Security (OEWG), a parallel forum open to all member states to study cyberspace peace and security, adopted consensus reports in 2021.

The main focus of cyber diplomacy

A number of countries have recognized the necessity for a cybersecurity main focus inside their government, as well as a similar function when it comes to dealing with foreign policy and cyberspace in general. There are numerous approaches to this:

- The Cyber Ambassador Model: A foreign ministry office, coordinator, or "cyber ambassador" is assigned to organize the promotion and pursuit of the state's interests, values, and strategies externally, while the performance of those functions is distributed internally among various government agencies or even non-state actors. This job is often high-level, with extensive coordinating power over a wide range of cyber-related concerns, rather than being compartmentalized within a single functional bureau.

- The Cyber Agency Model: A new government agency is established, similar to previous themed departments, to centralize all cyber-related activity (e.g., Ministries of Finance or the Environment).
- Disaggregated Diplomacy: For various cyber concerns, distinct diplomatic capacities are built. For example, a state may have a various cyber lead for data protection than it does for negotiating principles for responsible state behavior. States may structure each lead differently under this paradigm; for example, Germany has designated a coordinator for all cyber issues (including internet freedom and internet governance), as well as a distinct department for only some of them (e.g., cybersecurity and cyber capacity building).[1] Alternatively, under this paradigm, a state may appoint cyber ambassadors to all of its institutions who will play a role in cyber entities (e.g., ministries of defense, law enforcement, finance, communications)

Discussion

According to the 2020 Global Cyber Security Index, in order to effectively respond to cyber-related digital security concerns, governments must develop collective capacities while facilitating international collaboration and partnerships. Cybersecurity threats are becoming increasingly global, and collaboration remains a vital tool for dealing with cybersecurity difficulties. Because of the corresponding expansion in connections and infrastructure, cyber security remains an international challenge. The security of the global cyber ecosystem cannot be guaranteed or maintained by a single stakeholder, and its reach and influence needs national, regional, and international coordination. As a result, a country should work together to improve its cyber capacity by:

- Bilateral agreements on cybersecurity cooperation with other countries
- Government participation in international mechanisms related to cyber security activities
- Cyber security multilateral agreements
- Partnerships with the private sector (PPPs)
- Inter-agency partnerships

Cyber cooperation between Indonesia and Australia is one of Indonesia's collaborative initiatives to strengthen its cyber competence. Cyber cooperation between Indonesia and Australia is tied to the two nations' cyber policy dialogue agenda. Canberra hosted the first Australia-Indonesia Cyber Policy Dialogue on Thursday, May 4, 2017.[6] The Dialogue was held in a spirit of collaboration and openness, with the purpose of developing cyber cooperation as a common goal. The gathering remembered Prime Minister Turnbull and President Widodo's February 26, 2017 Joint Statement, in which they appreciated Foreign Ministers Bishop and Marsudi's agreement to create the Dialogue.

Australia and Indonesia have reiterated their approach to an open, free, and safe cyberspace for economic growth and creativity, and they have committed to strengthen their partnership to battle cyber threats. They committed to work closely with other regional partners to reduce cyber risk. The two countries also concurred that the Cyber Policy Dialogue established a strong platform for future partnership. The two sides discussed a wide range of cyber topics, including their various visions of the internet and cyberspace, cyber threat perceptions, policies and strategies, as well as regional and international trends. The discussion also included the possibility of bilateral cooperation to foster a safe, open, and secure internet for economic and social development.

The Dialogue was conducted by Dr. Tobias Feakin, Australia's Ambassador for Cyber Affairs, and Ambassador Desra Percaya, Indonesia's Director General for Asia Pacific and Africa Affairs, Ministry of Foreign Affairs. On the Australian side, representatives from the Department of Foreign Affairs and Trade, the Prime Minister's Department, the Department of Communications and the Arts, and the Australian Cyber Security Centre participated in the Dialogue, as did representatives from the Attorney-Department, General's the Department of Defence, the Australian Federal Police, and the Australian Criminal Intelligence Commission. The Dialogue was attended by representatives from the Indonesian Ministry of Foreign Affairs, the Ministry of Communications and Information Technology, the Coordinating Ministry for Political, Legal, and Security Affairs, the BSSN, and the Indonesian National Police.

The second Australia-Indonesia Cyber Policy Dialogue was conducted in Jakarta on August 3, 2018.[7] The Conversation proved the value of open dialogue, cooperation, and collaboration on cyber concerns once again. By signing a Memorandum of Understanding on Cyber Cooperation, Australia and Indonesia pledged to expand their relationship in cyber affairs, security, and digital economic growth.

On September 2, 2020, the third Indonesia-Australia Cyber Policy Dialogue was performed online from their respective representative offices.[2] The discussion reiterated the two countries' continued commitment to enhance bilateral relations and common understanding on cyber issues in compliance with the Indonesia-Australia Comprehensive Strategic Partnership Action Plan (2020-2024), which was signed in Canberra on February 10, 2020 by the two countries' Foreign Ministers. On this occasion, it was also agreed that, given the successful execution of the MoU and the advantages for both countries, Indonesia welcomes the extension of the MoU on Cyber Cooperation for the next two years while respecting and protecting the sovereignty of partner countries.

As a result of these forums, Indonesia and Australia signed a Memorandum of Understanding on Cyber Cooperation and Emerging Cyber Technology on September 9, 2021, which was signed by Indonesia's Head of BSSN and Australia's Ambassador for Cyber Affairs. This agreement is an extension of the previous agreement, which was signed in 2018. The purpose of this MoU is to promote partnerships and provide a framework of cooperation on cyber and emerging cyber technology issues between two countries. The scope of cooperation is:

1. Sharing of Information and Best Practice
2. Capacity Building and Strengthening Connection
3. Participants will work together to deepen understanding of the application of international law and norms in cyberspace, as well as supporting the development and operationalization of practical confidence building measures in the region to promote the development of open, secure, stable, accessible and peaceful cyberspace.
4. Digital Economy
5. Cybercrime.

We can see from the cyber cooperation that exists between Indonesia and Australia that each government has chosen the main objective of its cyber diplomacy in a different way. This is likely influenced by the emphasis on foreign affairs considerations, such as the establishment of norms for responsible online behavior and internet governance, or by greater and broader powers embracing economic issues such as digital commerce or technology regulation. Cyber ambassadors provide a single point of contact for external engagement, with the promise of faster or more flexible placement. However, cyber ambassadors, like other foreign ministry officials, might be segregated from other domestic agencies in charge of certain cyber-related issues, limiting the ambassador's powers. Such issues are less likely to arise if a single entity handles both internal and external participation in cyber concerns. Disaggregated diplomacy tactics attempt to circumvent this difficulty, but do so at a far higher cost in terms of resources, not to mention the possibility of discordant messaging given the number of individuals/offices involved.

Defining the main focus of cyber diplomacy is merely the start of cyber diplomacy capability. Cyber diplomacy necessitates the participation of several parties both within and outside of governments. All parties involved must be aware of and support the policies and norms aimed at by diplomatic efforts. Building that support necessitates the incorporation of cyber diplomacy focal points within overall governance procedures. Some governments complete the process simply by adding cyber themes to existing national or domestic security council agendas.

Alternatively, a determined cyber main focus might lead in person, giving the foreign ministry the authority to undertake cyber diplomacy on behalf of all relevant government parties. All departments and ministries involved in cyber policy, including defense, law, human rights, the economy, and other ministries entrusted with constructing information technology infrastructure, might take part in the process. The Australian Ambassador to Cyber Affairs, for example, leads a quarterly government-wide International Cyber and Critical Technology Engagement Group. These sessions contribute to the effectiveness of cyber ambassadors' work by improving communication and collaboration across departments and ensuring optimal coordination and prioritizing.

Strong cyber diplomacy must begin with increasing government knowledge of the issue. This has the potential to have a significant influence not just on worldwide cyber stability, but also on the home economy, trade talks, and other foreign activities. Cyber concerns are an important part of a country's foreign policy agenda, and they should clearly explain areas of government concentration while emphasizing long-term goals for international collaboration, including which players (e.g., public, commercial, regional, global) would be involved.

Cyber diplomacy is complex. This necessitates the capacity to engage in international and domestic legislation while also comprehending various government department judgments pertaining to local industry and technology use. As a result, governments must select and establish critical priorities for their cyber diplomacy activities, even if they have a variety of models to pick from. This may necessitate close collaboration across several government institutions to ensure that stated policy stances in the international arena are coordinated and aligned with other government authorities.

Countries find it challenging to prioritize cyber diplomacy among so many other open diplomatic contacts. Initially, governments may want to concentrate their cyber diplomacy efforts on influencing regional bodies or emphasizing certain programs rather than participating in all relevant venues.

To participate effectively in international debates, governments must develop extra cyber-related competences and abilities to supplement conventional diplomacy and trade techniques and processes. Even with limited resources, governments can undertake training for government personnel to increase their knowledge and awareness of cyber-related matters. Countries can employ a variety of official and non-governmental resources to create and strengthen their skills on a wide range of cyber-related topics, from internet governance to cybersecurity and, in some circumstances, cyber diplomacy itself.

Given the numerous bilateral, regional, multilateral, multistakeholder, and private networks in which cyber diplomacy may take place, governments must choose which fora, and how many, will help them achieve their foreign policy objectives. Countries can modify the depth and breadth of their cyber diplomacy capabilities based on this assessment.

Countries that develop cyber diplomacy must commit to upholding international law, especially international humanitarian law and human rights law. States must also show their commitment to following agreed voluntary state standards of cyberspace behaviour, as approved by the sixth UN GGE and the OEWG in 2021.

CONCLUSION

With the establishment of the National Cyber and Crypto Agency (BSSN) in 2017, Indonesia now has a government agency with a role in cyber security. This suggests that Indonesia employs the Cyber Agency model. In practice, however, Indonesia's foreign policy continues to stress the role of the Ministry of Foreign Affairs as the leading sector of foreign policy diplomacy, including dialogue or bilateral collaboration with other countries in the sphere of cyber security. In comparison to Indonesia, Australia followed the Cyber Ambassador model, appointing an ambassador under the Ministry of Foreign Affairs with the ability to conduct out cyber diplomacy with other countries and the function of distributing all forms of their work to other government departments involved in cyber security.

With the conditions indicated above, especially in relation to cyber security challenges in Indonesia, which are growing in all sectors, there is, of course, a need for better policies surrounding how Indonesia conducts its Cyber Diplomacy efforts. Other ways to cyber diplomacy must be considered (Disaggregated Diplomacy), in which specific sectors can be granted responsibility as coordinators for specific cyber security challenges, so that diplomatic activities in the field of cyber security can be carried out more extensively and effectively.
To strengthen its capability for cyber diplomacy, Indonesia must first establish a national cyber policy. These plans must not only focus on cyber security, but also outline the country's whole relationship with cyberspace. Furthermore, it is critical to raise awareness of cybersecurity problems throughout the country. Of course, this may be accomplished through collaboration and synergy between the government and all segments of society, including the telecommunications and information technology industries.

REFERENCES

André Barrinha and Thomas Renard, "Cyber Diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, nos. 4-5 (2017): 355. https://www.tandfonline.com/doi/pdf/10.1080/23340460.2017.1414924?needAccess=true

Bagian Komunikasi Publik, Biro Hukum dan Humas – BSSN. (2020, Sept 2). BSSN Inisiasi Lanjutan Kerja Sama Keamanan Siber Indonesia-Australia dalam 3rd Indonesia-Australia Cyber Policy Dialogue. Retrieved from bssn.go.id: https://bssn.go.id/bssn-inisiasi-lanjutan-kerjasama-keamanan-siber-indonesia-australia-dalam-3rd-indonesia-australia-cyber-policy-dialogue/

Barrinha and Renard, "Cyber Diplomacy: The Making of an International Society in the Digital Age," 355; "Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction," Shaun Riordan, *USC Center on Public Diplomacy*, May 12, 2016. https://www.uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

Carr, "Cyberspace and International Order," 178

Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 9916/17 (7 June 2017) http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf; Annegret Bendiek, "The EU as a Force for Peace in International Cyber Diplomacy," *SWP Comments*, no. 19 (2018): 3-5.

dfat. (2017, May 4). First Australia-Indonesia Cyber Policy Dialogue. Retrieved from dfat.gov.au: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/ Pages/australia-indonesia-cyber-policy-dialogue

dfat. (2018, August 3). Second Australia-Indonesia Cyber Policy Dialogue. Retrieved from dfat.gov.au: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/ Pages/second-australia-indonesia-cyber-policy-dialogue

Final Substantive Report: Open-ended working group on developments in the field of information and telecommunications in the context of international security. United Nations General Assembly. March 10, 2021 https://front.un-arm.org/wp-content/ uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. United Nations General Assembly. May 28, 2021. https://front.un-arm.org/wp-content/uploads/2021/ 08/A_76_135-2104030E-1.pdf

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. U.N. Doc. A/70/174, July 22, 2015, 26 ("2015 GGE Report").

OAS, "Cyber Security." https://www.sites.oas.org/cyber/en/pages/default.aspx.