Global-Local Interactions: Journal of International Relations
http://ejournal.umm.ac.id/index.php/GLI/index
ISSN: 2657-0009
Vol. 3, No. 2, December 2023, Pp. 93-102

Efforts to Enhance Australia's Cyber Security by Developing of a Partnership with Indonesia in the Field of Cyber Diplomacy

M. Aditya Gerald
UPN Veteran Jawa Timur

Article Info
Article history:
Received July 20, 2023
Revised December 22, 2023
Accepted December 22, 2023
Available online December 22, 2023

Cite:
Gerald, M, Aditya (2023). Efforts to Enhance Australia's Cyber Security by Deveoping of a Partnership with Indonesia in the Field of Cyber Diplomacy. Global-Local Interactions: Journal of International Relations, 3(2).

E-mail address:
adityagerald077@gmail.com

Abstract

This article examines the Australian government's endeavors to enhance cybersecurity by means of cyber diplomacy with Indonesia. This article utilizes qualitative descriptive methodologies. The data sources utilized encompass scholarly publications, books, research reports, and electronic media pertaining to the research topic. This article will examine the use of Australia's cyber diplomacy with Indonesia by utilizing the principles of cybersecurity and cyber diplomacy to enhance the robustness of cybersecurity. Australia engages in cyber diplomacy with Indonesia to enhance cybersecurity, based on the principle of international cooperation in this field. Australia implements a capacity building strategy, aligned with its 2017 International Cyber Engagement Strategy policy, to fortify Indonesia's cybersecurity. This endeavor will also contribute to the enhancement of Australia's own cybersecurity, given the interconnected nature of cyber threats. Australia's efforts to enhance Indonesia's capabilities are implemented through various collaborative initiatives, specifically the Cyber Policy Dialogue and Cyber Bootcamp programs. Examining this research is intriguing because to the involvement of Australia and Indonesia in cyber warfare, as well as their recent efforts to re-establish cyber-related diplomacy.

***Keywords**: Capacity Building, Cyber Diplomacy, Cybersecurity*

Introduction

Technological advancement is an inevitable aspect of every era. It has significantly influenced humanity, encompassing many sectors and diverse varieties of technology. Each of these sectors has a distinct impact on technology based on its utilization and the individuals who utilize it. Nevertheless, it is important to acknowledge that not all technology has beneficial consequences; in fact, technology can often exert adverse effects on humanity. Similar to computer and internet technologies, computers and the internet contribute to the formation of cyberspace. The word "cyberspace" was initially introduced in 1984 by William Gibson in his novel Neuromancer (Murray, 2007). Within the realm of cyberspace, individuals can engage in communication while maintaining anonymity and transcending geographical boundaries, enabling global interactions (Nugraha, 2013). The recent development of cyberspace has spawned a new category of criminal activities known as cyber threats. Cyber dangers encompass a range of manifestations, including cybercrime, cyber assault, cyber espionage, and cyberterrorism.

The rise in internet users correlates with an increase in the misuse of cyberspace. Presently, cybercrime possesses the capacity to inflict harm upon national defense. Worldwide, the number of internet users has experienced a significant surge, as indicated by the data from the World Bank's International Telecommunication Union (ITU). For instance, in 2017, over 49% of the global population were online users. This segment has had a significant surge in comparison to the year 2000, where it was just approximately 6.7%. This is attributed to the rapid growth of internet technologies. Nations worldwide presently see cybercrimes as a significant domestic and global peril due to the escalating risk of cyber attacks in tandem with the advancement of information technology. Nations worldwide have recognized the potential risks emanating from the digital realm and are actively endeavoring to mitigate them. Enhancing cybersecurity is now of utmost significance for nations to bolster national defense and safeguard other national interests.

Australia is highly committed to addressing both the risks and advantages presented in the realm of cyberspace. Australia has been subjected to a range of cyber attacks. Since 2011, the frequency of cyber attacks in Australia has consistently risen. The Australian government responds to a range of cyber attacks, including cyber espionage, cyber crime, cyber terrorism, and other forms of attacks. Australia is taking measures to enhance its cybersecurity in response to the rising number of cyber attacks and the growing significance of national cybersecurity. Australia has implemented a strategy in the field of cyber activities, specifically known as Australia's International Cyber Engagement Strategy 2017. This policy aims to position Australia favorably to take advantage of opportunities while effectively managing associated risks. Australia's participation in global cyber affairs aims to safeguard its citizens and advance its national interests, consequently enhancing Australia's ability to withstand cyber threats and capitalize on existing opportunities in the cyber industry.

Australia has also created a governmental organization dedicated to protecting against cyber threats, known as the Australian Cyber Security Center (ACSC). In addition to that, the Australian Department of Foreign Affairs and Trade (DFAT) is also enhancing its involvement in the field of cybersecurity. DFAT currently perceives cyberspace as a domain capable of exerting influence on all facets of international affairs. The Department of Foreign Affairs and Trade (DFAT) acknowledges that cyberspace has the potential to impact various aspects of national security, economic security, the safeguarding of human rights, and the promotion of sustainable development goals (SDGs) (DFAT, 2017). Australia recognizes that fostering strong cybersecurity necessitates international collaboration to cultivate prospects in the cyber realm. Australia recognizes that the cyber domain has the potential to either benefit or hurt a nation's national interests. Consequently, Australia is of the opinion that participating in global cyber affairs will help accomplish its cybersecurity goals (Government, 2020).

Global Cyber Security identifies five fundamental pillars for establishing a comprehensive global security index in the field of cybersecurity. These pillars encompass legislative, technical, organizational, capacity development, and cooperation measures. This ranking is designed to align with the specific cyber security principles and objectives of each individual country (ITU, 2023). The significance lies in the realm of international collaboration, particularly in the context of reciprocal efforts to combat cyber threats. Australia engages in cyber diplomacy as a means to enhance cybersecurity. Australia's cyber diplomacy is executed through the Cyber Cooperation Program. This program facilitates international partnerships to further Australia's strategic objectives in the field of cybersecurity.

Australia engages in cyber diplomacy with Indonesia through the implementation of the Cyber Cooperation Program. Both countries are dedicated to collaborating in addressing the challenges and possibilities that emerge from the digital realm. This strategy is intriguing because to Australia's cyber dispute with Indonesia in 2013. Australia will engage in cooperative efforts with global allies and provide assistance to nations in the vicinity to enhance their capabilities in addressing cybercriminal activities, with the ultimate goal of enhancing global cybercrime prevention and prosecution (Government, 2017). Australia's cyber diplomacy with Indonesia through the Cyber Cooperation Program is Australia's strategic step in improving cybersecurity. Australia's cyber diplomacy with Indonesia is the right thing because apart from the fact of Indonesia's geographical location, Indonesia is also considered capable of creating regional cyber stability. Through the Cyber Cooperation Program, Australia will increase Indonesia's cyber capacity to support increasing Indonesian cybersecurity and regional cyber stability. This will also have an impact on improving Australia's cybersecurity because based on the 2020 Global Cyber Security Index, to respond effectively to cyber-related digital security issues, the government must develop collective capacity while facilitating international collaboration and partnerships (ITU I. T., 2020). This paper examines Australia's diplomatic endeavors to enhance cyber security cooperation with Indonesia.

Method

This article employs the notions of cybersecurity and cyber diplomacy as a foundation for subsequent discourse. The idea of cybersecurity aligns with the principles outlined in Australia's International Cyber Engagement Strategy 2017. According to Global Cyber Security (2007), international collaboration is conducted in five specific areas of endeavor to facilitate conversation and coordination in addressing cyberthreats and enhancing cybersecurity. In order to enhance or establish robust cybersecurity, it is imperative to foster international collaboration. This is because the realm of cyber threats is not limited to a single nation, but affects all countries, necessitating the need for global cyber stability. This article also employs the notion of cyber diplomacy, which, as defined by Hamonangan & Assegaf (2020), encompasses three distinct aspects: communication, negotiation, and information gathering with other nations. As a means to protect national interests in the digital realm, cyber diplomacy serves as a strategy to safeguard defense in cyberspace through diplomatic efforts. Given the global nature of cyber crime, multiple countries engage in cyber diplomacy with one another to collectively enhance state security in the online domain. Moreover, as stated by Pawlak (2022), capacity building serves as the fundamental foundation in cyber diplomacy, with distinct goals including fortifying the domestic legal structure, establishing and reinforcing responsive measures, and enhancing training and awareness. Australia is enhancing Indonesia's cyber diplomacy by implementing various cooperation projects to develop Indonesia's capabilities. Australia's efforts to enhance Indonesia's capabilities involved raising awareness and providing training through the Cyber Policy Dialogue and Cyber Bootcamp partnership initiatives.

Finding and Discussion

Australia's International Cyber Engagement Strategy 2017 sebagai Strategi Peningkatan *Cybersecurity* Australia

Australia perceives cyberspace as both a potential advantage and a potential danger. Australia intends to actively participate in global cyber activities in order to capitalize on the benefits and mitigate the risks that arise in the digital realm. In addition to that, Australia has a specific objective, which is to enhance the cybersecurity of its nation. Australia will endeavor to enhance international and regional cyber stability with the objective of bolstering Australia's cybersecurity. Australia devised a policy approach, known as Australia's International Cyber Engagement approach 2017, in order to accomplish this objective. The International Cyber Engagement Strategy 2017 of Australia outlines a framework centered around seven key themes: Digital Trade, Cyber Security, Cybercrime, International Security, Internet Governance & Cooperation, Human Rights & Democracy Online, and Technology for Development. Each subject is accompanied by a specific and realistic action plan. Australia's foreign policy white paper will serve as the basis for reaffirming the crucial and growing significance of cyber concerns in Australia's foreign policy. Australia's adoption of this strategy will strategically position the country to capitalize on favorable circumstances while effectively mitigating potential risks. By actively engaging in international cyber affairs, Australia aims to safeguard its citizens and advance its national objectives. Consequently, this approach will enhance Australia's ability to withstand cyber threats and enable the country to exploit the various prospects available in the cyber domain (Government, 2017).

Australia will engage in cyber diplomacy and collaborate with global partners to combat and mitigate hostile cyber operations conducted by criminals, state actors, or their proxies. This includes addressing interference in a nation's internal democratic processes. Australia's approach to enhancing cybersecurity and exploring cyber prospects is guided by a distinct goal and a well-defined work program. Australia's cyber affairs agenda has a worldwide outlook and a specific emphasis on the area. Australia should strategically utilize its cyber capacity development resources in the Indo-Pacific area to promote the free and secure use of the internet, thereby enhancing Australian cybersecurity. Australia's efforts to enhance the capabilities of its international partners in the Indo-Pacific region will play a crucial role in promoting global cyber stability. This is particularly important because certain countries in the Indo-Pacific region lack sufficient cyber capabilities, and some countries have yet to fully grasp the significance of cybersecurity in the realm of international affairs. Australia aims to enhance prosperity and security for itself, the area, and the global community in the cyber domain through the implementation of the cyber diplomacy scheme.

The primary goal of Australia's International Cyber Engagement Strategy is to enhance the country's cybersecurity by establishing a robust and resilient cyber security framework for Australia, the Indo-Pacific region, and the global community. Australia has identified four key areas of focus to effectively pursue its aim. These focus points will play a crucial role in Australia's strategic endeavors to accomplish the desired outcome. Australia will preserve robust cyber security alliances with global partners through cyber diplomacy and other avenues at both regional and global levels. Australia recognizes that the internet's global reach exposes it to cyber threats originating from any location. To enhance its cyber security, Australia actively engages in international cyber initiatives, fostering strong relationships with partner nations. This collaboration aims to bolster Australia's knowledge and capabilities in cyber defense, ultimately strengthening its national security posture. Australia prioritizes partnerships with countries that share economic, diplomatic, social, and geopolitical ties with Australia. Enhancing the cybersecurity of our international allies will bolster Australia's national defense. Furthermore, Australia will actively promote inventive cybersecurity solutions and offer top-notch cybersecurity guidance to its overseas counterparts. Currently, Australia will share cyber security technical advice generated by the ACSC (Australian Cyber Security Centre) with foreign partners. Additionally, Australia aims to enhance the cyber security capabilities of new goods, systems, and services. Australia will enhance its regional cyber security capabilities as its third objective. Australia will actively support its regional partners by enhancing their ability to address cyber threats, bolstering cybersecurity measures, and combating cyber crime through the Cyber Cooperation Program. Furthermore, Australia aims to bolster the Australian cyber security industry by actively supporting the growth and presence of Australian cyber security enterprises in the worldwide market.

Achieving enhanced cybersecurity through the implementation of Australia-Indonesia Cyber Diplomacy

Geographically, Indonesia is the nearest country to Australia. Given Indonesia's substantial population and number of internet users, it serves as a valuable ally in Australia's efforts to enhance its cybersecurity. Indonesia's cybersecurity is considered to be lacking, which can indirectly impact Australia's cybersecurity. Therefore, Australia should engage in cyber diplomacy with Indonesia to enhance its cyber capabilities, ultimately improving Australia's cybersecurity as well. Australia's cyber diplomacy with Indonesia is executed via the Cyber Cooperation Program, which involves two collaborative initiatives: the Cyber Policy Dialogue and the Cyber Bootcamp.

Cyber Policy Dialogue

Australia conducted this program three times as part of its cyber diplomacy with Indonesia. The objective of this program was to enhance Indonesia's cyber capacity and raise awareness in the cyber domain. It aimed to strengthen cybersecurity relations between the two countries, ultimately serving as Australia's strategy to enhance cybersecurity. The Cyber Policy Dialogue is an Australian initiative aimed at engaging other nations in raising awareness about cybersecurity. Through this program, two or more countries engage in dialogue to establish a foundation for practical cooperation. The objective is to enhance Australia's existing bilateral relationships, facilitate the sharing of information on cyber threats, exchange perspectives, and advocate for Australia's interests. (Government, 2016). The program will engage in discussions and collaborations with international partners to accomplish key objectives regarding international cyber matters, such as international law, responsible state conduct norms, and confidence-building measures. This program serves as a venue to promote the significance of enhancing a nation's cybersecurity and to advocate for a secure and open internet that fosters economic and social progress. Its goal is to raise international partners' understanding about the cyber domain.

The inaugural Cyber Policy Dialogue between Australia and Indonesia took place in Canberra on 4 May 2017 (DFAT, 2017). Dr. Tobias Feakin, Australia's ambassador for cyber matters, led the debate, while Ambassador Desra Believe represented Indonesia. The Cyber Policy Dialogue I was conducted with a focus on fostering collaboration, transparency, and a shared objective of enhancing cooperation on cyber-related matters. This program underscores Australia's dedication to fostering an open, unrestricted, and secure internet to drive economic advancement, encourage innovation, and safeguard national defense against cyber threats (DFAT, 2017). Australia engaged in discussions regarding diverse cyber risks, encompassing the conceptualization of the internet and cyberspace. They exchanged perspectives on cyber threats with Indonesia, as well as deliberated on national policies and strategies pertaining to the cyber realm. Australia also emphasized the significance of regional and worldwide advancements in the field of cybersecurity. The Cyber Policy Dialogue I marked the initiation of cyber diplomacy between Australia and Indonesia. This dialogue served as Australia's initial endeavor to enhance Indonesia's understanding and capability in achieving regional cyber stability, while also bolstering Australia's cybersecurity measures.

In addition, Australia's cyber diplomacy with Indonesia persisted through the Cyber Policy Dialogue II, which took place in Jakarta on 3 August 2018. This program once again showed the significance of intimate deliberation, cooperation, and collaboration on matters related to cybersecurity (Goverment, 2018). The Cyber Policy Dialogue II was attended by both parties with the same composition. The Australian delegation was headed by Tobias Feakin, the ambassador for cyber affairs, while the Indonesian delegation was led by Desra Believe, the Director General for Asia Pacific and African Affairs. During the Cyber Policy Dialogue II, Australia is actively advocating for donations to enhance Indonesia's awareness and capacity in the field of cybersecurity. Additionally, Australia is promoting a vision and mission of fostering international cyber stability, which is based on established international law, voluntary and non-binding norms of behavior, responsibility, practical confidence-building measures, and cooperative capacity development. The conversation proceeded by examining the reports from 2013 and 2015 by the UN Government Expert Group on advancements in the realm of informatics and telecommunications within the framework of global security (UNGGE). Australia and Indonesia have reaffirmed their commitment to advancing a collection of voluntary and non-binding universal principles of responsible conduct by states, as outlined in the 2015 UNGGE report. During the Cyber Policy Dialogue II, Australia and Indonesia established a comprehensive cooperation agreement in the areas of cyber affairs, security, and digital economic growth. This agreement was formalized by a memorandum of understanding (MoU) on cyber cooperation. The Memorandum of Understanding (MoU) was executed on August 31, 2018, in Bogor, Indonesia.

In addition, Australia and Indonesia maintained their cyber diplomacy efforts with the virtual Cyber Policy Dialogue III, conducted on 2 September 2020 as a result of the Covid-19 epidemic (Goverment, 2020). During this talk, Australia and Indonesia enhanced their collaboration and alliances in the areas of information exchange, cyber security protocols, skill development, and the advancement of the digital economy, while also addressing cyber crime. During the Cyber Policy Dialogue III, both countries reaffirmed their dedication to enhancing bilateral involvement in the cyber realm. Subsequently, Australia and Indonesia expressed profound apprehension regarding the escalating occurrence and severity of cybersecurity incidents, which encompass perilous cyber operations conducted by entities aiming to exploit the Covid-19 pandemic. Australia acknowledges the necessity of global cooperation in order to avoid and address cyber threats that have the potential to harm international peace and security. Additionally, Australia emphasizes the significance of international and regional cyber frameworks in establishing cyber stability. During the Cyber Policy Dialogue III, Australia and Indonesia reaffirmed their dedication to working together in the field of cybersecurity. They emphasized their commitment to collaborating with many parties to build trust, raise awareness, and enhance capabilities. This includes their involvement in the ASEAN regional cyber security workstream. Subsequently, the conversation proceeded with an examination of the 2018 Australia-Indonesia Cooperation MoU, encompassing the favorable outcomes achieved by both entities. The conversation concluded with a consensus to prolong the Memorandum of Understanding (MoU) for an additional duration of 2 years.

The cyber Policy Dialogue is a component of cyber diplomacy that occurs throughout the communication and negotiation phase. Australia is currently pursuing a negotiation forum with Indonesia to enhance collaborations in the realm of cyber security. Australia's proactive measures to mitigate cyber dangers are seen through the consistent implementation of communication initiatives and the attainment of bilateral agreements.

Cyber Bootcamp

Australia is developing a training program for Indonesia in the field of cybersecurity to enhance Indonesia's competence and establish robust cybersecurity measures. This initiative will also have a positive influence on Australia's own cybersecurity. The Cyber Bootcamp work program is a component of the Cyber Cooperation Program. It aims to offer practical professional guidance and skills training to foreign partners (Governement, 2020). This program involves a partnership between the Australian government and academic institutions, specifically the National Security College University and the Australian National University. The primary purpose of Cyber Bootcamp is to enhance comprehension of national cyber policy coordinating initiatives. Gaining a comprehension of this coordination method is valuable for devising policy strategies for international collaborators in the cyber realm. The second objective is to enhance comprehension of cyber vocabulary, internet architecture, and security rules. Thirdly, this involves raising knowledge about cyber dangers and issues, both within Australia and among international partner regions. Fourthly, this involves specifically advocating for the implementation of the international stability framework for cybersecurity. This approach aims to foster global stability in the cyber domain, hence enhancing cybersecurity. The fifth objective is to foster cooperative partnerships among government, academia, civic society, and the commercial sector in order to collectively address cyber issues. Effective collaboration is important in order to combat cyber risks. Therefore, it is crucial to establish strong links among government entities, academic institutions, civil society organizations, and the commercial sector in this context. The final task is identifying the specific roles and duties associated with incident response. The Cyber Bootcamp program is a two-week rigorous program in Australia that includes interactive seminars, training scenarios, visits to industrial sites, and discussions with Australian government agencies. International partners will actively participate in these activities. This program aims to execute initiatives that address cyber challenges or opportunities that are pertinent to the domestic responsibilities of foreign partners, who will subsequently contribute to the establishment of a robust regional cyber space.

Indonesian delegates participated in a program that encompassed training sessions, workshops, visits to industrial sites, and dialogues with Australian government agencies.

Australia anticipates that this initiative will enable Indonesia to effectively execute training and educational programs focused on addressing domestic cyber concerns, hence enhancing cybersecurity within the regional area (Magrisa, 2020). During the initial week of this program, Indonesian delegates examined a range of topics and difficulties in the realm of cyber, including international legislation and standards, identification and prevention, safeguarding vital infrastructure, fostering an environment of ingenuity, and combating cyber criminality(ANU, 2019). Following that, the program proceeded with a specialized course led by Dr. Lesley Seebeck, the CEO of ANU Cyber Institute. Dr. Seebeck emphasized that the objective of this activity was to enhance the capabilities of Indonesian delegates in comprehending, constructing, and upholding cybersecurity systems in order to mitigate cyber threats (Magrisa, 2020). The Cyber Bootcamp program is a direct implementation of Australia's policy to enhance Indonesia's cyber security capabilities, which in turn has implications for Australia's own cybersecurity.

According to the aforementioned idea of cyber diplomacy, which encompasses communication, negotiation, and data collecting, it is evident that Australia is striving to surpass these benchmarks. The collaboration between Australia and Indonesia extends beyond mere communication and information exchange, encompassing the establishment of cooperative initiatives aimed at enhancing cyber technology.

The Sustainability of Indonesia's Cyber Diplomacy with Australia

The Cyber Cooperation Program between Australia and Indonesia undoubtedly yields benefits and advantages for both nations in the realm of cyber diplomacy. Australia and Indonesia possess distinct objectives and concerns that predate the commencement of diplomatic relations. Australia derives advantages and benefits from engaging in cyber diplomacy with Indonesia, primarily through the acquisition of information and the exchange of best practices within the context of cooperation. The material is presented in the form of legislation, a national cyber strategy and policy, discussions on cyber dangers, and expert opinions on best practices in cyber concerns. This information is highly valuable for Australia since it will enhance the understanding of Australian cybersecurity, hence contributing to the overall effectiveness of Australian cybersecurity measures. The second objective is to enhance capacity and foster stronger links. Australia aims to bolster Indonesia's cybersecurity capabilities, which in turn will provide valuable insights to Australia for boosting its own cybersecurity measures. Australia will get Indonesia's support in digital economic links, in addition to enhancing cybersecurity, as the third area of focus is the digital economy. This information holds significant importance as per Australia's 2017 white paper, Australia anticipates Indonesia's ascension to the position of the fifth largest economy by 2030. This long-term advantage in economic terms presents Australia with an opportunity. However, it is crucial to acknowledge that Indonesia's potential as the largest economy also brings forth the likelihood of heightened cyber threats. Given the nature of cyber warfare, Australia pledges to assist Indonesia in enhancing its cybersecurity measures, which will consequently impact Australia's own cybersecurity. Lastly, Australia will be granted enhanced intelligence on cyber crime. The primary advantages that Australia can gain from engaging in cyber diplomacy with Indonesia include the establishment of robust cybersecurity measures for both nations, fostering bilateral trust with Indonesia, and contributing to international and regional cyber stability to ensure a secure cyberspace.

Conclusion

Cyberspace demands careful consideration in the global arena due to its role in giving rise to new transnational offenses, including cybercrime, cyber attacks, cyber espionage, and cyberterrorism. Australia's cyber diplomacy with Indonesia aims to address cyber dangers and opportunities. This is being done through the implementation of Australia's International Cyber Engagement Strategy 2017, which focuses on creating capacity to enhance cybersecurity for both countries. Australia can enhance its cybersecurity by increasing its capacity. This is important because cyber threats in any country can have an impact on Australia, and vice versa. Strengthening cybersecurity globally will also strengthen Australia's cybersecurity. It may be inferred that Australia's endeavors to enhance cybersecurity through cyber diplomacy with Indonesia, by implementing various work programs, are a successful endeavor to enhance Australia's cybersecurity.

References

ANU, A. N. (2019, November 20). *Cyber Bootcamp Project kicks-off with Indonesian partners*. Dipetik July 10, 2023, dari https://nsc.crawford.anu.edu.au/: https://nsc.crawford.anu.edu.au/news-events/news?combine=boot+camp

DFAT. (2017). *Cyber affairs and critical technology*. Diambil kembali dari https://www.dfat.gov.au/: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/default

DFAT. (2017, May 4). *First Australia-Indonesia Cyber Policy Dialogue*. Dipetik July 10, 2023, dari https://www.dfat.gov.au/: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australia-indonesia-cyber-policy-dialogue

Goverment, A. (2018, August 3). *Second Australia-Indonesia Cyber Policy Dialogue: Joint Statement*. Dipetik July 10, 2023, dari https://www.internationalcybertech.gov.au/: https://www.internationalcybertech.gov.au/node/91

Goverment, A. (2020, November 4). *Third Australia-Indonesia Cyber Policy Dialogue*. Dipetik july 10, 2023, dari https://www.internationalcybertech.gov.au/: https://www.internationalcybertech.gov.au/node/1

Governement, A. (2020, November 5). *Cyber Bootcamp Project*. Dipetik July 6, 2023, dari https://www.internationalcybertech.gov.au/: https://www.internationalcybertech.gov.au/Cyber-Bootcamp-Project

Government, A. (2016). *AUSTRALIA'S CYBER SECURITY STRATEGY 2016.*

Government, A. (2017). *AUSTRALIA'S INTERNATIONAL CYBER AND CRITICAL TECH ENGAGEMENT STRATEGY.* Canberra: internationalcybertech.gov.au.

Government, A. (2017). *AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY.*

Government, A. (2020). *AUSTRALIA'S CYBER SECURITY STRATEGY 2020.*

ITU. (2023). *Global Cybersecurity Index*. Diambil kembali dari ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU, I. T. (2020). *Global Cybersecurity Index 2020.* Development Sector.

Magrisa, D. (2020). KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) INDONESIA DENGAN DEPARTMENT OF FOREIGN AFFAIRS AND TRADE (DFAT) AUSTRALIA DALAM PENGEMBANGAN CYBER SECURITY. *JOM FISIP Vol. 7: Edisi II*, 1-11.

Murray, A. (2007). *The Regulation of Cyberspace: Control in the Online Environment.* Routledge-Cavendish.

Nugraha, P. C. (2013). Konsepsi Kedaulatan Negara Dalam Borderless Space. *Opini Juris Volume 13 Mei-Agustus Tahun 2013*, 22 - 46.