https://doi.org/10.18196/hi.v9i21.10522

JURNAL HUBUNGAN INTERNASIONAL
VOL. 9, NO. 2 (2020): October 2020-March 2021

Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post-Indonesia-Australia Cyberwar in 2013

Elva Azzahra Puji Lestari
Department of International Relations, Faculty of Social and Political Sciences, Universitas Indonesia, Indonesia
elva.azzahra97@gmail.com
Submitted: 3 December 2020; Revised: 19 February 2021; Accepted: 23 February 2021

Abstrak

Kedekatan geografis antara Indonesia dan Australia menciptakan hubungan yang harmonis antara kedua negara terutama dalam bidang keamanan. Perkembangan teknologi informasi menjadi salah satu bidang yang menjadi fokus Indonesia dan Australia dalam menjaga keamanan kawasan. Kerjasama keamanan telah terjalin antara Indonesia dengan Australia. Dampak perkembangan tersebut dapat menjadi perselisihan antara Indonesia dengan Australia terutama pada konflik cyberwar tahun 2013. Peristiwa cyberwar diakibatkan oleh cyber attack Australia terhadap Indonesia melalui penyadapan jaringan komunikasi Presiden Yudhoyono. Namun, pasca cyberwar antara Indonesia dan Australia tidak memberikan ketegangan dalam hubungan kedua negara. Indonesia menandatangani MOU dalam Cyber Security Cooperation dengan Australia tahun 2018. Penelitian ini bertujuan untuk menganalisis penyebab Indonesia dan Australia memilih untuk tetap melanjutkan kerjasama keamanan melalui cyber security cooperation pasca cyberwar Indonesia-Australia tahun 2013. Penelitian ini menggunakan teori complex interdependence dan politik domestik yang kemudian dianalis menggunakan metode analisis kualitatif. Hasil penelitian menunjukkan bahwa sumberdaya soft power Australia, kredibilitas politik Australia, keuntungan Indonesia dan Australia sebagai negara demokratis, dan keberlangsungan politik pemimpin menyebabkan Indonesia dan Australia memilih untuk tetap melanjutkan kerjasama keamanan pasca cyberwar Indonesia-Australia tahun 2013.
Kata kunci: Indonesia, Australia, Cyber Security Cooperation, complex interdependence, politik domestik.

Abstract

The geographical proximity between Indonesia and Australia leads to harmonious relations between these two countries, especially in security. The development of information technology is one of the areas becoming the focus of Indonesia and Australia in maintaining regional security. Security cooperation has been established between Indonesia and Australia. This development can have an impact on a dispute between Indonesia and Australia, particularly in the 2013 cyberwar conflict. An Australian cyber-attack on Indonesia by tapping President Yudhoyono's communication network caused the cyberwar incident. However, the post-cyberwar between Indonesia and Australia did not cause tension in the relations between the two countries. Indonesia approved the MOU of Cybersecurity Cooperation with Australia in 2018. This study aims to analyze the causes of Indonesia and Australia's choice to continue their cybersecurity cooperation after the Indonesia-Australia cyberwar in 2013. This research utilized the theory of complex interdependence and domestic politics and qualitative analysis methods. The results revealed that Australia's soft power resources, Australia's political credibility, the advantages of Indonesia and Australia as democratic countries, and the political survival of individual leaders caused both countries to continue their cybersecurity cooperation after the Indonesia-Australia cyberwar in 2013.
Keywords: Indonesia, Australia, Cybersecurity Cooperation, complex interdependence, domestic politics.

INTRODUCTION

Indonesia and Australia are two countries with geographical proximity. The adjacent geographical location between Indonesia and Australia brings an impact on their relationships. Although the geographic conditions are contiguous, these two countries have different government and political systems, economic

impact on their relationships. Although the geographic conditions are contiguous, these two countries have different government and political systems, economic conditions, historical backgrounds, religions, cultures, and perspectives. These conditions cause the dynamics of their bilateral cooperation to experience ebb and flow.

Bilateral relations between Indonesia and Australia have intertwined in various fields. The relatively close geographical position between these two countries underlies the creation of security stability through security cooperation. At the 5th of KTT ASEAN in 1995, Indonesia and Australia agreed on a security agreement named Agreement on Maintaining Security (AMS). It was Indonesia's first security agreement with other countries. Meanwhile, Australia assumed that the agreement was a part of Prime Minister Paul Keating's plan to strengthen the relationship of Australia with its neighbor countries in the Asia Pacific region, either economically or strategically (Firth, 1999; Firth, 2018).

Since the post-fall of Soeharto in 1998, the problem of Timor-Timur has been a talk complicating diplomatic relations between Indonesia and Australia. After the referendum results by the Timor-Timur people were announced, the Indonesian people carried out various anti-Australian demonstrations. However, the tension could be solved after doing mutual visits and dialogue development between the two countries. On November 13th, 2006, Indonesia and Australia signed a security cooperation framework agreement called Traktat Lombok (Lombok Treaty). Even though it has been signed since 2006 and in effect since 2008, the security disputes between Indonesia and Australia persist. One of the security disputes between these two countries occurred in the scope of cyberspace.

Cybersecurity in Indonesia has not been a priority and still under development. Indonesia's cybersecurity and defense system are still weak if compared to other countries. It was evidenced in the tapping incident of President Yudhoyono's communication network by Australia in 2013. The tapping incident by Australia against Indonesia was named a cyber-attack. This incident was caused by the emergence of new security threats, not only a military dimension (Tobing, 2002). This cyber-attack has a negative impact on the cyberspace between Indonesia and Australia, affecting the cyberwar between the Anonymous Community of both countries, resulting in a tense relationship between them. Several government and commercial sites from both countries have become victims (Ningrat, 2015), thereby showing their cyber development differences. Australia has paid attention to cybersecurity systems as a primary priority in international security. However, its actions can be a threat to cybersecurity conditions in Indonesia.

In 2018, Indonesia decided to sign the MOU of Cybersecurity Cooperation with Australia in responding to cybercrime. It reflects that Indonesia needs Australia to develop a cybersecurity system and continue the security cooperation with Australia. Therefore, it is interesting to investigate further why Indonesia and Australia chose to continue their cybersecurity cooperation after the Indonesia-Australia cyberwar in 2013. Accordingly, this research aims to analyze the causes of Indonesia and Australia's choice to continue their security cooperation through cybersecurity cooperation after the Indonesia-Australia cyberwar in 2013.

Several previous studies have many classifications in viewing bilateral security cooperation relationships. The dynamics of bilateral relations between Indonesia and Australia have a variety of issues related to international security. The academic study of Indonesia-Australia bilateral relations in cybersecurity established in 1995 was divided into three major classifications: (1) bilateral relations, (2) multilateralism, and (3) national security.

The first classification discusses bilateral relations between Indonesia and Australia in viewing cyber problems, including international stability security efforts and the enhancement of bilateral relations in cybersecurity. International security studies in bilateral relations between Indonesia and Australia used the concept of security cooperation (Phillips, A. & Hiariej, E., 2016; Singh, S. & Krupakar, J., 2014), national interest (DuPont, A., 1996; Gounder, R. & D. P. Doessel., 1997), security dilemma (Day, R., 2015), securitization (McKenzie, M., 2019), domestic politics (Sulistiyanto, P., 2010), foreign policy (Nabbs-Keller, G.,

2020; Sukma, R., 1997), security agreement (Kaye, S., 1997), threat (Philpott, S., 2001), bonded and embedded trust (Throat, S., 2019), and policy transfer (Nethery, A. & Carly, G., 2014). Bilateral relations in security cooperation between Indonesia and Australia have a very high institutional that increases the expansion of security cooperation, impacting Asia-Pacific region stabilities in more complex challenges. Therefore, bilateral relations in security cooperation between these two countries require high institutional, mutual trust, information exchange, policy transfer and capacity building.

The second classification deals with the multilateralism of Indonesia and Australia in security cooperation using the concept of trilateral cooperation (Kelton, M. & David W., 2019), security regionalism (Mcdougall, 2001), security cooperation (Zimmerman, E., 2014), and cyber cooperation (Gultom, Supriyadi, & Kustana, 2018). Several concepts explain each country's self-interest, encouraging foreign policy to increase regional cooperation relationships. Therefore, multilateralism connects each country's importance by attempting efficient and effective actions to lead to the successful operation of non-traditional security issues.

The third classification discusses national security in viewing cyber problems, including implementing the right security strategy for Indonesia. National security strategy can be implemented using cybersecurity policy concepts (Rizal & Yanyan, 2016), cyber development (Paterson, T., 2019), and International Humanitarian Law and National Cyber Defense Policy (Setiyawan, et al., 2018). Several concepts mention the strategy of more serious cybersecurity policy implementation. Therefore, in overcoming cyber problems, Indonesia's security strategies implement cybersecurity, build the capacity of cybersecurity and national defense policies to maintain the stability of national security, and establish policies to prevent and anticipate cyber-threats and cyber-attacks.

Previous studies have described various perspectives in viewing cybersecurity issues from various analysis levels. However, those studies have limitations that must be reviewed further. The limitations on the classifications to view cybersecurity resulted in some general analyses. Moreover, they have not discussed in detail the cooperation condition that has been quite long and has experienced several conflicts but still has close cooperation, either bilateral or multilateral. Therefore, the perspective of cooperative security in overcoming cybersecurity problems must be studied further.

THEORETICAL FRAMEWORK

COMPLEX INTERDEPENDENCE AND DOMESTIC POLITICS

Transnational political issues, such as trade, monetary relations, and maritime policy, show that modernists point appropriately to the fundamental changes. Nevertheless, they often assume that without adequate analysis, technology advances and the enhancement of social and economic transactions will lead to a new world when the state's power is no longer critical. The revolution has dramatically changed one feature, "Power and Interdependence" as "complex interdependence". The friction of these feature meanings is due to the multiplication of security objects (Ramadhanie, 2017).

Robert O. Keohane and Joseph S. Nye (1977) introduced complex interdependence as a world where security and power are less critical and various social and political relationships connect the states. The information revolution has increased the number of contact channels between societies, one of three complex interdependence dimensions. However, the information revolution has not made dramatic changes in two conditions of complex interdependence. Military power still plays an essential role in intercountry relations. Moreover, in a critical condition, security still surpasses other issues in foreign policy. Interdependence can be seen in the formation of friendship patterns with cooperation and hostility patterns with fears (Putri, 2013). The information revolution does not change world politics into new interdependent politics because it does not flow in a vacuum but the political space. Therefore, Keohane and Nye divided three variables from complex interdependence: (1) soft power resource of large state; (2) politics of credibility; and (3) the democratic advantage (Figure 1.).

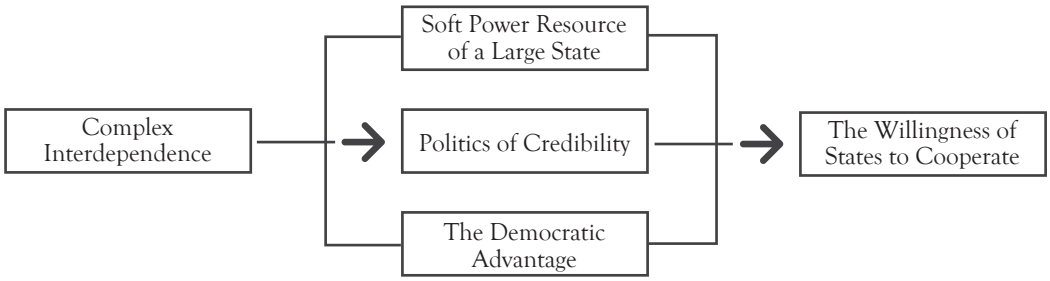

Figure 1. Operational Model Theory of Complex Interdependence (Keohane & Nye, 1977)

The soft power resource of a large state is the ability to get desirable results because both parties have the same desire. It works by convincing others to agree on the norms and institutions that produce desirable behavior. In the next century, information technology is broadly defined and might be the most essential resource.

Through politics of credibility, the governments can convince potential partners that they will not act opportunistically and that everyone will have an advantage over competitors who have less credibility of promises. Credibility is the reputation development for providing correct information; even simultaneously, it will negatively impact the country as an information provider. Credibility can be trusted if the information is generated through an appropriate process with professional norms and is marked with transparency and procedural fairness.

The democratic advantage explains that transparency is a primary asset for countries seeking investment. The ability to stockpile information that once seemed valuable to authoritarian states ruins the credibility and transparency needed to attract investment with global competitive requirements. Furthermore, the ability to disseminate free information increases persuasion potential in world politics.

The continuity of individual leaders' politics in international negotiations is often discussed by bachelors of International Relations who focus on the interaction between domestic politics and foreign policy. Peter Gourevitch (1977) proposed that individual leaders tend to mobilize national resources to strengthen politics in the legitimacy of domestic power competition. Individual leaders will find diplomatic success, which will empower domestic authorities (Figure 2.).

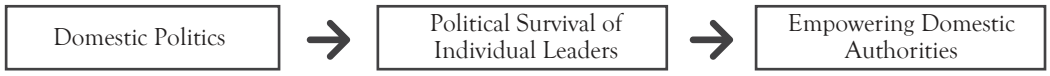

Figure 2. Operational Model Theory of Domestic Politics (Gourevitch, 1977)

Based on the two theoretical operational models above, this study analyzed the reasons why Indonesia and Australia chose to continue their security cooperation after the 2013 cyberwar using four variables: (1) soft power resource of a large state; (2) politics of credibility; (3) the democratic advantage; and (4) political survival of individual leaders (Figure 3.). The four variables were the causes covered in this research's objective. Therefore, the two operational models of the theory could achieve the aim of the research.

RESEARCH METHOD

This research used a qualitative method to view the process to the causal mechanism. The data used to view the cause and effect were sourced from secondary data, such as journals, books, related documents, and online media from 2013 to 2019. The time taken from this research was based on the bilateral relations between Indonesia and Australia after the cyberwar in 2013. The secondary data were collected from online media and

documents related to the bilateral relations of the two countries. Furthermore, the data were processed using the Microsoft office and Arc-GIS software. The triangulation process was performed by finding the validity and reliability of data collection. The triangulation results were analyzed using descriptive qualitative analysis to study why Indonesia and Australia continue their security cooperation through cybersecurity cooperation after the Indonesia-Australia cyberwar based on space and time.

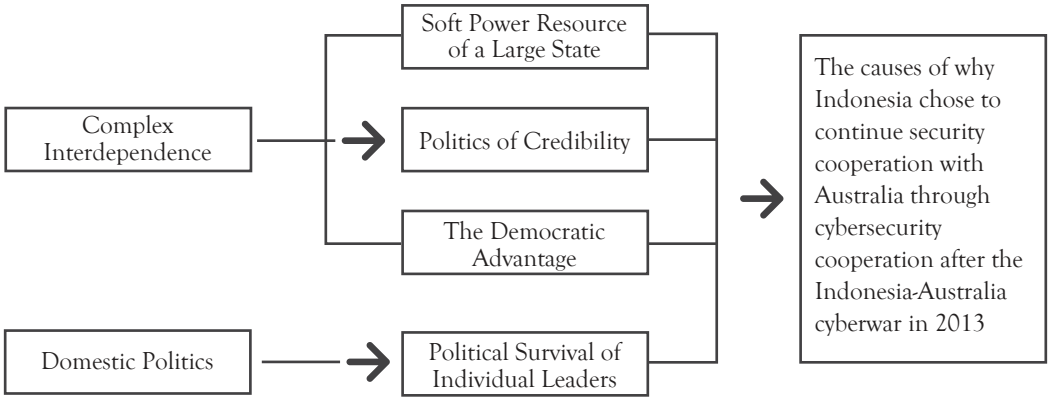

Figure 3. Analytical Framework (Keohane & Nye, 1977; Gourevitch, 1977)

RESULT AND ANALYSIS

This research used variables of complex interdependence by Robert O. Keohane and Joseph S. Nye to operationalize the analytical framework. Complex interdependence provides three variables: soft power resources in a large country, political credibility, and the advantages of a democratic country. Besides, domestic politics provides a variable called the political survival of individual leaders. The theory of complex interdependence by Robert O. Keohane and Joseph S. Nye, as well as domestic politics by Peter Gourevitch, are relevant for this research.

This research discovered why Indonesia and Australia chose to continue their security cooperation through cybersecurity cooperation after the Indonesia-Australia cyberwar in 2013. It was due to four factors: (1) the resources of Australia's soft power; (2) Australia's political credibility; (3) the advantages of Indonesia and Australia as democratic countries; and (4) political survival of individual leaders (Figure 4.). The discussion of the four factors was supported by secondary data related to operations that Indonesia and Australia have done in interlacing cybersecurity cooperation relationships from 2013 to 2019.

THE RESOURCES OF AUSTRALIA'S SOFT POWER

Australia has resources of appreciable soft power. Australia has created various policy strategies related to cybersecurity that aim to increase resources in the national to the international scope. Its strategies are the responses to current developments and partly due to persistent geo-strategic realities. Moreover, the enhancement of the population in Australia is needed to strengthen national security and economic development (Aziz, 2004). Strong cybersecurity is a fundamental element of Australia's growth and prosperity in the global economy, requiring partnerships that involve government, private sector, and society.

In 2016, the Australian Government issued a Cybersecurity Strategy that reflects the development role of digital networks in international relations, trade and investment, and strategic security problems. The strategy includes an investment of more than $ 230 million in five programs to the 2020 period, including national cyber partnerships, cyber stinger defenses, global responsibility and influence, growth and innovation, and a cybernation (Australian Government, 2020).

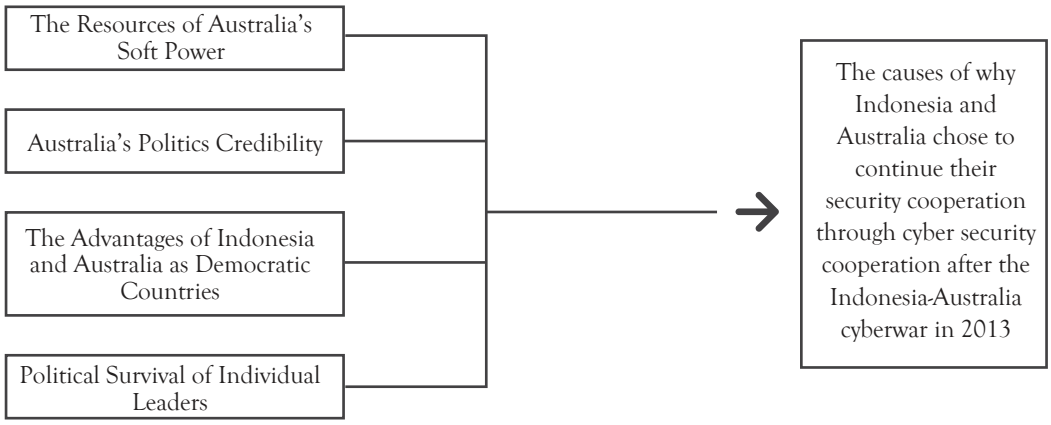

Figure 4. Visualization of the Analysis Flow (Author's work, 2020)

The Australian Government is committed to increase innovation, growth and prosperity for all Australians through strong cybersecurity. It is in line with the Innovation Agenda and National Science of the Australian Government vaster to create a modern and dynamic economy of the 21st century for Australia. The strategy attempts to chart a new way for Australia's cyber future that is creative, collaborative and adaptable.

On October 4th, 2017, Australia created a strategy policy of International Cyber Engagement. The strategy is organized into eight themes: (1) digital trade; (2) cybersecurity; (3) cybercrime; (4) security and international cyberspace; (5) internet management system and cooperation; (6) human rights and online democracy; (7) technology development; and (8) comprehensive and coordinated cyber affairs. These eight realms are partly the importance of Australian traditional that has been changed by the inevitable rise of digital communication technology.

Australia has built domestic capability through the eSmart library program of more than 75 percent of its 1,500 libraries. The concept of online security for thousands of Australians of all ages each year gives the skills required to safely and responsibly use digital technology. Moreover, Australia has released the 2017 Cyber Security Sector Competitiveness Plan: Establishing Cyber Security Innovation Nodes across Australia, working with stakeholders to develop Australia's cybersecurity qualification and cyber level certificate based on first national skills.

Australia launched an agenda named Australia's Tech Future, developed with the help of society, a business, industry group, state and territory, and the research sector. The Australian government will build momentum created by the agenda launch to push meaningful complicity. Several agenda launched by the Australian government include (1) maintaining collaboration with industry, community groups and academia; (2) working closely with the governments of states and territories; and (3) tracking Australia's performance (Australian Government, 2018). Outlinely, the agenda carries out discussion, coordination, and collaboration in activities to strengthen Australia's future tech. Moreover, the agenda implicates the Commonwealth Government with states and territories either bilaterally or through the skills council and COAG industry to advance Australia's future tech. The government will track Australia's performance relative to other countries in the global metric.

Due to adequate information technology resources and defense, Australia has provided assistance to Indonesia regarding soft power resources. In 2011, the AFP and the police inaugurated Cyber Crime Investigation Center (CCIC). The construction of the CCIC was Australia's effort to help Indonesia, aiming to increase police's cyber forensic abilities (Connery, Sambhi & McKencie, 2014: 9-10). The CCIC is located at the Area Headquarters of Indonesia National Police (Mabes Polri), North Jakarta. The cyber-crime investigation office was built around the Regional Police

(Polda) located at four locations, from now on named the Cyber Crime Investigation Satellite Office (CCISO).

Australia has provided fund assistance of ten million dollars to Indonesia for the construction of CCIC and CCISO. The Australian Government has provided fund and equipment grants for cyber investigation, reaching 20 million Australian dollars, particularly for the construction of the cybercrime investigation office (Sondakh, 2015: 188). The assistance included funds and sophisticated investigative equipment, such as technology and computers, to carry out cyber-crime investigations. After completing the construction of the CCIC and CCISO, Australia has contributed to surveillance efforts and computer equipment maintenance at the CCIC and CCISO. Australia formally funded the assistance to maintain both countries' operations against transnational crime (Connery et al., 2014: 5-9). Australia's desire to increase the number of cyber skill analysts in Indonesia becomes important that impacts both parties.

Jusuf Kalla (Vice President of the Republic of Indonesia) received Paul Grigson (Australian Ambassador to Indonesia) to discuss cybersecurity cooperation. Grigson said that cybersecurity was a crucial issue for both countries. Indonesia and Australia faced similar challenges in cybersecurity (Jaramaya, 2017). Therefore, both agreed to increase cybersecurity cooperation. The Australian Minister of Cybersecurity met with the Coordinating Minister for Political, Legal, and Security Affairs of the Republic of Indonesia at the Singapore Cyber Week a short time ago. Several Australian cyber experts would come to Indonesia to exchange cybersecurity experiences from the meeting.

The development of an effective cybersecurity strategy in Indonesia is highly needed. According to Wiranto (Coordinating Minister for Political, Legal and Security Affairs of the Republic of Indonesia), Indonesia, with a very open national cyber position, must develop an effective cybersecurity strategy that has deterrence (Jaramaya, 2017). As the country with the second-largest internet user globally, Indonesia has an essential role in forming the endurance of a multicultural Indonesian society and respecting democracy and pluralism. Therefore, Indonesia's commitment is reaffirmed in doing cooperation with Australia. It aims to strengthen cybersecurity cooperation, such as agreed in the 2 + 2 Dialogue and Ministerial Council on Law and Security meeting, and build a strong e-commerce sector.

AUSTRALIA'S POLITICS CREDIBILITY

Indonesia's geographical facts become the importance of strategy to Australia. Proximity to Indonesia, as well as ethnic and religious differences, become Australia's permanent interest in its friendship and stability with Indonesia. However, Indonesia can be a serious threat to Australia's security. Therefore, gradually Australia attracts Indonesia's attention by interacting and contacting routinely between government officials and society.

Australia is also involved with Indo-Pacific partners to harmonize the efforts and share the best practice to ensure it stays on the front line of technology innovation and cybersecurity. It has trust in the ability of digital infrastructure to face cybersecurity threats. It has a desire to build good relations and cooperation in the security and defense field with Indonesia. Julia Gillard, the 27th former Prime Minister of Australia, said Indonesia was considered as a "close friend" and colleague that could advance conciliation and security in the region. Besides, she emphasized that Indonesia and Australia had transparency toward the importance of facing security and defense so that the two countries would continue to cooperate appropriately in facing the threats.

The collaboration between Indonesia and Australia in the digital sector allows the two countries to increase mutual trust. The digital forum between the two countries aims to deepen and expand cooperation between the leaders, practitioners, the private and academics from each country. Forum participants will discuss the possibilities and challenges of the digital era and consider the opportunity for developing new partnerships.

The collaboration forum between Indonesia and Australia in the digital sector focuses on five programs: the creative industry, cybersecurity, digital health, financial technology (fintech) and start-up, and smart government. The creative industry is a program that

provides a platform for sharing perspectives and develop concepts for greater cooperation between Indonesia and Australia in the creative industry (Australian Embassy in Indonesia, 2018). Moreover, the program will allow the creative sector ability of the two countries to represent government, institutions, arts and culture, creative industry agency, a game application, and industry application. In addition, Indonesia and Australia have a strong common interest in cybersecurity as welfare. The cybersecurity program focuses on building connections between the industry and the Indonesian-Australian governments, mapping a new cooperation field (Australian Embassy in Indonesia, 2018). The digital health program discusses its role in the future of health service distribution in Indonesia and potential fields from bilateral cooperation (Australian Embassy in Indonesia, 2018). Additionally, FinTech and Start-up programs introduce the ecosystem in Indonesia and check the opportunities and challenges for digital innovation, fintech and start-up (Australian Embassy in Indonesia, 2018). The Smart Government program unites Indonesian participation from government, entrepreneurs, and researchers who will focus on the government's readiness for the alteration and the opportunity to utilize the technology for smart and responsive government to address gaps and promote inclusion (Australian Embassy in Indonesia, 2018). The collaboration is designed to push the Indonesian and Australian approach, which is practical in giving solutions together.

THE ADVANTAGES OF INDONESIA AND AUSTRALIA AS DEMOCRATIC COUNTRIES

Indonesia and Australia are democratic countries. They have the potential for democratic partnerships that can develop and deepen the relationships to handle the differences and the disunities with a sense of huge maturity and responsibility. Cooperation between Indonesia and Australia is essential for strengthening relations between governments. Moreover, the leaders from government institutions have regularly met and got to know each other better. Indonesia's strategic relationship with Australia is built based on a common interest that refers to two things: security cooperation viewed in Australia's overall bilateral relations with Indonesia and the enhancement of cooperation between the two countries toward the development of new security architecture for the Asia Pacific region.

Indonesia's foreign policy is currently essential to look at Indonesia as a democratic strength. Cyber cooperation offers Indonesia an opportunity to expand security cooperation in the future with Australia in entering several non-military problems that can potentially impact the national security of the two countries but cannot be solved unilaterally due to transnational causes and effects. Indonesia's hope related to cyber cooperation is to become the largest country for the digital economy in Southeast Asia by 2030, according to Standard Chartered Bank report (Ariesta, 2019). Cyber cooperation for Indonesia can be seen as a multiplier of significant political and military power for Indonesia's importance. It is due to Australia's strong regional military abilities, adequate technology accessibility, training and sophisticated Western intelligence, and Australia's close relations with the United States as a superpower country in the world.

Australia's strategy in the container of human rights and democracy refers to the international human rights standard. It aims to reunite human rights commitment and promote human rights internationally through advocacy and capacity building. Australia's national importance has several purposes vital to Indonesia, consisting of (1) to avoid entering into a military conflict or serious conflict to Indonesia; (2) to help Indonesia become a country that is stable, prosperous and continues to evolve; (3) to uphold the maintenance of a united Indonesia; (4) to help Indonesian society maintain a unique version of tolerant, moderate, and eclectic Islam; and (5) to achieve the closest level of involvement with Indonesia at the society level through bridge construction (Pearson, 2018). This cooperation promotes the strategic importance of a wider Canberra because it connects Australia as a regional country with a relatively low population, but its technology and economic advancement become one of the rising middle power in the East Asia region.

On May 4th, 2017, Indonesia and Australia held a Cyber Policy Dialogue meeting in the spirit of collaboration and openness to strengthen the cooperation on cyber issues. The meeting remembered the Joint Statement on February 26th, 2017, by Prime Minister Turnbull and President Widodo in welcoming the approval between Bishop Foreign Minister and Marsudi to form a dialogue (DFAT, 2017). Australia and Indonesia affirmed their commitment to an open, free and safe internet for economic growth and innovation and decided to deepen the cooperation to deal with cyber threats. The two countries also agreed that the dialogue would give a strong foundation for future cooperation. Both parties discussed various cyber problems, including their vision from the internet and cyberspace, exchange cyber threat perception, policy and strategy, and regional and international developments. It also discussed the potential of bilateral cooperation to promote a safe, open and secure internet for economic and social construction. The two countries decided to hold the next round of dialogue in Indonesia in 2018 (DFAT, 2017). Indonesia appreciated the holding of a Cyber Policy Dialogue by Australia. Consultation of the two countries was very intensive in building communication and defense through dialogue forums, including The Indonesia-Australia Defence Strategic Dialogue (IADSD), Australia-Indonesia High-Level Committee (HLC Ausindo), and The Two Plus Two between the Ministry of Foreign Affairs and Ministry of Defense of the two countries.

The third Australia-Indonesia Cyber Policy Dialogue was held virtually on September 2nd, 2020. The multi-agency dialogue reinforced the close cyber cooperation and partnerships between the two countries in information sharing, cybersecurity best practices, capacity building and enhancing the digital economy and addressing cybercrime. The dialogue affirmed the two countries' ongoing commitment to enhance bilateral engagement on, and mutual understanding of, cyber issues consistent with the Plan of Action for the Indonesia-Australia Comprehensive Strategic Partnership (2020-2024), signed by the Foreign Ministers in Canberra on February 10th, 2020 (DFAT, 2020). Participants discussed the evolving situation in cyberspace, including main challenges and best practice approaches to manage strategic threats, national cybersecurity strategies and relevant legislation.

POLITICAL SURVIVAL OF INDIVIDUAL LEADERS

President Joko Widodo embodies foreign politics, which is collaborative and gives concrete benefits for Indonesian society. The government has ensured the protection and secure sense, clean government, and the establishment of the legal system that has become a priority in developing the political field (Kantor Staff Presiden, 2019). Domestic political stability continues to be maintained by embodying a secure sense and ensuring a dialogue space to continuously increase the quality of democracy. Besides, in the framework of fulfillment of Minimum Essential Force II (MEF II), Indonesia's strength and weapon systems have increased, manifested either through the contribution of the national defense industry or the cooperation of foreign production.

President Joko Widodo delivered a state speech in front of the annual session of the People's Consultative Assembly (MPR) of the Republic of Indonesia in 2019. In the speech in the 74th Independence Anniversary of the Republic of Indonesia in 2019, he expressed appreciation for the performance of MPR during this year (Badan Siber dan Sandi Negara, 2019). In one of his speeches, President Joko Widodo said that the government must be prepared to face the threat of cybercrimes, including data abuse. Because data is a new type of wealth of the nation, more valuable than oil. The utilization of technology can destroy politeness nation, endanger unity and entity, and endanger democracy, for that it must be regulated measuredly. Then regulation must give a secure sense and make it easy for everyone to do a good thing and push all parties to innovate toward an advanced Indonesia. Based on the monitoring of the BSSN Public Relation Team, the annual session was attended by several ministers in the working cabinet of President Jokowi and Vice President Jusuf Kalla, including Minister of Industry Airlangga Hartarto, Minister of Health Nila F Moeloek, Minister of Home Affairs Tjahjo Kumolo, Minister of Law and Human Rights Yasonna Laoly, Cabinet Secretary Pramono

Anung, and Minister of Foreign Affairs Retno Marsudi. Moreover, it was also attended by the Head of Cyber Agency and Country Code (BSSN) of the Republic of Indonesia, Hinsa Siburian (YH-RM).

The warm relationship between President Joko Widodo and Prime Minister Malcolm Turnbull has helped to reorganize the relation. Following an agitated period in a relationship marked by a series of political upheavals, the relationship has entered a stability period. The relationship between President Joko Widodo and Malcolm Turnbull has experienced positive development. The completion of this problem was also helped by the relationship between President Widodo and Prime Minister Turnbull, who agreed on a full recovery in defense cooperation and showed significant progress on various economic and security problems at their meeting in February 2017.

CONCLUSION

The dynamics of international politics have caused the tidal relation between Indonesia and Australia. The development of information technology has become one of the focuses of Indonesia and Australia in maintaining regional security. The development has affected the dispute between Indonesia and Australia, particularly in the cyberwar conflict in 2013. After the cyberwar incident, Indonesia decided to sign an MOU of Cyber Security Cooperation with Australia in responding to cyber-crime. The theories of complex interdependence by Robert O. Keohane and Joseph S. Nye and domestic politics by Peter Gourevitch are still relevant for this research. It reflects that Indonesia still needs Australia to develop a cybersecurity system and continue the security cooperation relationship with Australia. Therefore, the reasons why Indonesia and Australia chose to continue security cooperation through cybersecurity cooperation after the Indonesia-Australia cyberwar in 2013 were due to four factors: the resources of Australia's soft power, Australia's political credibility, the advantages of Indonesia and Australia as democratic countries, and political survival of individual leaders. Thus, these four factors caused both countries to maintain their good relations through cybersecurity cooperation.

REFERENCE

Ariesta, M. (2019). *Keamanan Siber Jadi Perhatian Khusus Indonesia dan Australia.* Retrieved July 10, 2020, from Medcom: https://www.medcom.id/internasional/asia/nN9wJq3k-keamanan-siber-jadi-perhatian-khusus-indonesia-dan-australia

Australian Embassy in Indonesia. (2018). *Indonesia Australia Digital Forum.* Retrieved July 7, 2020, from https://indonesia.embassy.gov.au/jakt/iadf2018.html

Australian Government. (2018). *Australia's Tech Future.* Retrieved from Australia's Tech Future: Department of Industry, Science, Energy and Resource: https://www.industry.gov.au/data-and-publications/australias-tech-future

Australian Government. (2020). *Cybersecurity.* Retrieved May 15, 2020, from Australian Government: Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

Aziz, A. (2004). Menelaah Konsep Human Securiy : Studi Kasus Penanganan Masalah Pengungsi Afganistan di Australia (1999 – 2000). *Global, 7*(1), 80–105.

Badan Siber dan Sandi Negara. (2019). *Sidang Tahunan MPR 2019, Jokowi: Pemerintah Harus Siaga Terhadap Kejahatan Siber.* Retrieved October 10, 2020, from Badan Siber dan Sandi Negara: https://bssn.go.id/sidang-tahunan-mpr-2019-jokowi-pemerintah-harus-siaga-terhadap-kejahatan-siber/

Connery, D., Sambhi, N., & McKenzie, M. (2014). A return on investment The future of police cooperation between Australia and Indonesia. *Australian Strategic Policy Institute.*

Day, R. (2015). West Papua and the Australia-Indonesia relationship: a case study in diplomatic difficulty, *Australian Journal of International Affairs, 69*(6), 670–691.

DFAT. (2017). *Australia's International Cyber Engagement Strategy.* Retrieved July 10, 2020, from https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/index.html

DFAT. (2017). *First Australia-Indonesia Cyber Policy Dialogue.* Retrieved May 15, 2020, from Australian Government: Department of Foreign Affairs and Trade: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australia-indonesia-cyber-policy-dialogue

DFAT. (2020). *Third Australia-Indonesia Cyber Policy Dialogue Joint Statement 2020.* Retrieved May 15, 2020, from Australian Government: Department of Foreign Affairs and Trade: https://www.dfat.gov.au/news/news/third-australia-indonesia-cyber-policy-dialogue

DuPont, A. (1996). The Australia-Indonesia Security Agreement. *The Australian Quarterly, 68*(2): 49-62.

Gounder, R. & D. P. Doessel. (1997). Motivation Models of Australia's Bilateral Aid Program: The Case of Indonesia. *Bulletin of Indonesian Economic Studies, 33*(3), 97– 110.

Gourevitch, P. (1977). International Trade, Domestic Coalitions and Liberty: Comparative Responses to the Crisis of 1873–1896. *Journal of Interdisciplinary History, 7*(2), 281–313.

Firth, S. (2018). *Instability in the Pacific Islands: A status report.* Lowy Institute.

Firth, S. (2020). *Australia in international politics: an introduction to Australian foreign policy.* Routledge.

Gultom, R. A., Supriyadi, A. A., & Kustana, T. (2018). A Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework. *International Journal of Management & Information Technology, 13,* 3288–3300.

Jaramaya, R. (2017). *Indonesia dan Australia Tingkatkan Kerja Sama Keamanan Siber.* Retrieved July 6, 2020, from Republika: https://www.republika.co.id/berita/trendtek/internet/17/10/02/ox6mq0-indonesia-dan-australia-tingkatkan-kerja-sama-keamanan-siber

Kantor Staff Presiden. (2019). *Lima Tahun Maju Bersama: Capaian Pemerintahan Joko Widodo - Jusuf Kalla.* Retrieved October 2020, 2020, from Kantor Staff Presiden: https://ksp.go.id/wp-content/uploads/2019/10/141019_Laporan-5-Tahun-Jokowi-JK_small-1.pdf

Kaye, S. (1997). The Australia-Indonesia Maritime Boundary Treaty: A Review. *Maritime Studies, 94*,28–32.

Kelton, M., David W. (2019). US-Australia-Indonesia Trilateral Security? Conditions for Cooperation. *Australian Journal of International Affairs, 73*(3), 289–311.

Keohane, R. & Joseph, S. (1977). Power and Interdependence in The Information Age. *Foreign Affairs, 77*(5), 81.

Mcdougall, D. (2001). Australia and Asia-Pacific Security Regionalism: From Hawke and Keating to Howard. *Contemporary Southeast Asia, 23*(1), 81–100.

McKenzie, M. (2019). Securitising transnational crime: the political drivers of police cooperation between Australia and Indonesia, *Policing and Society, 29*(3), 333–348.

Nabbs-Keller, G. (2020). Understanding Australia-Indonesia relations in the post-authoritarian era: resilience and respect, *Australian Journal of International Affairs*

Nethery, A. & Carly, G.(2014). Australia–Indonesia cooperation on asylum-seekers: a case of 'incentivised policy transfer', *Australian Journal of International Affairs, 68*(2), 177–193.

Ningrat, I. (2015). *Dampak skandal penyadapan Presiden RI oleh pemerintah Australia terhadap dunia maya (studi kasus cyber war Anonymous Indonesia-Australia).* (Diploma Thesis). Universitas Al Azhar Indonesia.

Paterson, T. (2019). Indonesian cyberspace expansion: a double-edged sword. *Journal of Cyber Policy, 4*(2), 216–234.

Pearson, E. (2018). *Hak Asasi Manusia Seharusnya Jadi Fokus KTT ASEAN-Australia.* Retrieved May 15, 2020, from Human Right Watch: https://www.hrw.org/id/news/2018/03/14/315706

Phillips, A & Eric, H. (2016). Beyond the 'Bandung divide'? Assessing the scope and limits of Australia–Indonesia security cooperation, *Australian Journal of International Affairs, 70*(4), 422–440

Philpott, S. (2001). Fear of the Dark: Indonesia and the Australian National Imagination, *Australian Journal of International Affairs, 55*(3), 371–388.

Putri, C. (2013). Central Asia as a Regional Security Complex from the Perspectives of Realism, Liberalism and Constructivism. *Global, 15*(1), 84–94.

Ramadhanie, A. (2017). Evolusi Konsep Keamanan Energi. Global: *Jurnal Politik Internasional, 19*(2), 98–120.

Rizal, M., Yanyan M. Yani. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies, 4*(1), 61–78.

Rogerson, K. (2000). INFORMATION INTERDEPENDENCE: Keohane and Nye's complex interdependence in the information age, *Information, Communication & Society, 3*(3), 415–436.

Setiyawan, A. dkk. (2018). Strengthening Indonesia's Policy on National Cyber Security to Deal with Cyberwarfare Threat. *South East Asia Journal of Contemporary Business, Economics and Law, 15*(5).

Sondakh, A. R. (2015). Kerjasama Polri dan AFP Dalam Menaggulangi Cyber Crime di Indonesia Tahun 20010-2012. *eJournal Ilmu Hubungan Internasional.*

Sukma, R. (1997). Indonesia's bebas-aktif foreign policy and the 'security agreement' with Australia, *Australian Journal of International Affairs, 51*(2), 231–241.

Sulistiyanto, P. (2010). Indonesia-Australia Relations in the Era of Democracy: The View from the Indonesian Side, *Australian Journal of Political Science, 45*(1), 117–132.

Singh, S. & Jayanna, K. (2014). Indo–US Cooperation in Countering Cyber Terrorism: Challenges and Limitations, *Strategic Analysis, 38*(5), 703–716.

Tobing, F. (2002). Aktivitas Drug Trafficking sebagai Isu Keamanan yang Mengancam Stabilitas Negara. *Global, 5*(1), 75–86.

Troath, S. (2019). Bonded but not embedded: trust in Australia-Indonesia relations, Keating & Suharto to Turnbull & Jokowi, *Australian Journal of International Affairs, 73*(2), 126–142.

Zimmerman, E. (2014). Security cooperation in the Indo-Pacific: nontraditional security as a catalyst, *Journal of the Indian Ocean Region, 10*(2), 150–165.