GLOBAL LEGAL REVIEW
E-ISSN 2776-1347 P-ISSN 2776-0308

Fatihah, Citra Yuda Nur. 2022. "Indonesia's Approach on Cyberattack Attribution through its Foreign Policy" *Global Legal Review* vol. 2, no. 2: page 121-42. https://doi.org/10.19166/glr.v2i2.5140.

INDONESIA'S APPROACH ON CYBERATTACK ATTRIBUTION THROUGH ITS FOREIGN POLICY

Citra Yuda Nur Fatihah
University of California, Berkeley
citra.jatmiko@berkeley.edu

Abstract

It is clear that cybersecurity has now become a matter of increasing concern for Indonesian citizens, the private sector and the Indonesian government. Indonesia is ranked among the top countries from which cyberattacks are launched, while at the same time is itself very vulnerable to cyberattack. Indeed, Indonesia is currently in the early stages of developing a national cybersecurity strategy. The legal framework for cybersecurity in Indonesia is still weak that there is no clear classified security law or policy, and security practices are spread across different legislation while there are no specific cybersecurity provisions in place. Indonesia also lacks of national policy and strategy when it seeks to defend itself against cyberattack, particularly those hacking activities from foreign actors or state-sponsored groups. While majority of states in the world have two different approaches on cyberattack attribution from the context of sovereignty in international law, those applied sovereignty as a rule and as a principle, Indonesia has never stated clearly its position. Therefore, based on the analysis on how Indonesia's approach on sovereignty through its foreign policy, from the perspectives of diplomacy practices and national policies, relevant sovereignty-violation cases, and its international framework and cooperation on cybersecurity, we may conclusively view that Indonesia appears to endorse the sovereignty-as-a-rule position, where it upholds the principle of respect for state sovereignty on cyberspace.

Keywords: *Cyberattack, Cybersecurity, Cyber-attribution, Cyberspace, Sovereignty, Foreign Policy*

1. INTRODUCTION

As the world's fourth most populous nation in the world, Indonesia has experienced significant growth in the number of people connected to the internet. At the same time, this increasing base of consumers of internet and internet-enabled services surely has made Indonesia the largest and the fastest-growing digital economy in South East Asia.[1]

[1] The World Bank, "Ensuring a More Inclusive Future for Indonesia through Digital Technologies." Accessed October 5, 2021. https://www.worldbank.org/en/news/press-release/2021/07/28/ensuring-a-more-inclusive-future-for-indonesia-through-digital-technologies.lusive Future."

Consequently, Indonesia is currently home to many of the sub-region's most prominent digital platforms that are not only attracting a large volume of investments into the country but are also providing new and innovative solutions that are increasingly transforming the economic and social lives of Indonesians.[2] However, all those startups, digital economy platforms, and other related online activities with their customers and the whole citizen, on the other hand, definitely establish and develop their own cyber risks.

Meanwhile, Indonesia is currently in the early stages of developing a national cybersecurity strategy. The legal framework for cybersecurity in Indonesia is still very weak. Furthermore, there is no clear classified security law or policy, and security practices are spread across different legislation while there are no specific cybersecurity provisions in place. This all situation and condition make cybersecurity in Indonesia truly at risk. The Indonesian National Cyber and Crypto Agency (Badan Siber dan Sandi Negara or BSSN), for example, reported 290.3 million cases of cyberattacks in 2019.[3] Likewise, the Criminal Investigation Agency of the Indonesian National Police (Bareskrim) saw an increase in police reports of cybercrimes, as 4,586 police reports were filed on "Patrolisiber," a Bareskim website for reporting cybercrime, in 2019. [4]

While lacking data protection regulation and any related cybersecurity provisions, Indonesia also lack of national policy and strategy when it seeks to defend itself against cyberattack, particularly those hacking activities from foreign actors or state-sponsored groups. Kristen Eichensehr in one of her papers said that "When a state seeks to defend itself against a cyberattack, must it first identify the perpetrator responsible."[5] It is because, basically, the international law on state responsibility permits a state that has suffered an internationally wrongful act, in this case a severe cyberattack, to take countermeasure, but only against the state responsible. Therefore, this restriction implies that attribution is a compulsory prerequisite to countermeasures.

In the article, it is briefly explained that majority of countries have two different approaches on cyberattack attribution from the context of sovereignty in international law, those applied sovereignty as a rule and as a principle, to the extent whether international law prohibits violations of sovereignty that do not amount to a prohibited intervention or use of force.[6] Countries that have definitively taken the position that sovereignty is a principle view sort of small-scale cyberattacks those would not constitute use of force as actions that do not violate international law and therefore no need to invoke countermeasures or engage in attribution.[7] While countries those endorse sovereignty as a rule position, tend to have a rigid

[2] *Id.*

[3] "Cyberattack Data (January – April 2020)," The Indonesian National Cyber and Crypto Agency, accessed October 1, 2021, https://bssn.go.id/rekap- serangan-siber-januari-april-2020.

[4] *Id.*

[5] Kristen E. Eichensehr, "Cyberattack Attribution as Empowerment and Constraint," Hoover Working Group on National Security, Technology, and Law, *Aegis Series Paper*, No. 2101 (January 15, 2021): 1-2, https://www.lawfareblog.com/cyberattack-attribution-empowerment-and-constraint.

[6] *Id.*

[7] *Id.*

foreign policy that no matter how small the cyberattack is, it still constitutes a breach of sovereignty in international law.[8]

In fact, there are only a few states have declared their position on this sovereignty question, while the rest of the states remain silent about their position, including Indonesia. Indonesia has never stated clearly its position on this sovereignty approach whether it endorses sovereignty-as-a-rule view or sovereignty-as-a-principle view. Therefore, this paper will examine and demonstrate Indonesia's approach on cyberattack attribution from the context of sovereignty in international law through its foreign policies, from the perspectives of diplomacy practices and national policies, relevant previous related cases, and international framework and cooperation, whether it is positioning sovereignty as a rule or as a principle, and how it will be implemented through its foreign policy.

2. RESEARCH METHODS

The fact that the Indonesia is still left behind in this cyberattack attribution practices from the context of sovereignty in international law, raises the question of the condition of the implementation of whether it endorses sovereignty-as-a-rule view or sovereignty-as-a-principle view. Therefore, this research seeks to discuss this problem. The object of this research is to study Indonesia's approach on cyberattack attribution from the context of sovereignty in international law through its foreign policy. The aspects of this discussion include international law, cybersecurity law, national policies, and international relations perspectives.

This research belongs to an analytical legal research where it examines and demonstrates the use of existing available data, facts, and information to critically study the present situation. This research also analyzes the whole range of facts and information critically where it relies upon the existing concepts and theories to either re-interpret it into a new concept or formulate from it.

3. ANALYSIS AND DISCUSSION

This part is intended to examine Indonesia's approach on cyberattack attribution from the context of sovereignty through its current foreign policy priorities, based on its diplomacy practices and national policies, several related sovereignty-violation cases, and its international framework and cooperation on cybersecurity to finally view its approach on cyberattack attribution from the perspective of sovereignty.

3.1. Approach on Sovereignty based on Diplomacy Practices and National Policies

Diplomacy is understood as "the attempt to adjust conflicting interests by negotiation and compromise."[9] Another scholar, Hedley Bull, stated that diplomacy is "a custodian of the idea of international society, with a stake in preserving and strengthening

[8] *Id.*
[9] Wight M., *System of States* (Leicester: Leicester University Press, 1979), 176.

it."[10] According to him, there are five main functions to the diplomatic practice: to facilitate communication in world politics, to negotiate agreements, together intelligence and information from other countries, to avoid or minimize "friction in an international relations" and, finally, to symbolize the existence of a society of states.[11] It is not even just about relations between states. It now has to take into account "wider relationships and dialogues, involving such entities as regional and international organizations–be they intergovernmental (IGOs) or non-governmental (NGOs)–multinational firms, sub-national actors, advocacy networks, and influential individuals."[12]

Now, diplomacy has also progressively extended to new policy areas over the years, entering uncharted political territories such as climate negotiations or, lately, cyber issues. Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace.[13] Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda.[14] Predominant issues on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance.[15] Cyber-diplomacy is therefore conducted in all or in part by diplomats, meeting in bilateral formats (such as the US-China dialogue) or in multilateral fora (such as in the UN).[16] Beyond the traditional remit of diplomacy, diplomats also interact with various non-state actors, such as leaders of internet companies (such as Facebook or Google), technology entrepreneurs or civil society organizations.[17] In other simple words, cyber-diplomacy is the use of diplomatic tools and diplomatic mindset to resolve issues arising in cyberspace.

Cyber-diplomacy, indeed, as defined in this paper, is relatively a new concept, especially for Indonesia. As mentioned earlier, Indonesia is currently in the initial stages of developing a national cybersecurity strategy, including those cyber-diplomacy related policies. There is not yet any printed document or official white paper on Indonesia's cyber-diplomacy, those like the US DoD "defend forward" cyber strategy policy or a US CYBERCOM "Command Vision" document. Therefore, when considering the emergence of Indonesia's cyber-diplomacy, it is important to first understand the priority of Indonesia's foreign policy for the next 5 years (2019-2024) as the continuity of the

[10] *Id.*

[11] Bull H., *The Anarchical Society: A Study of Order In World Politics* (3rd ed) (Basingstoke: Palgrave, 1977/2002), 171.

[12] Bull, *The Anarchical Societ*, 165.

[13] Jönsson C. and Langhorne R., *Diplomacy: Volume III. Problems And Issues In Contemporary Diplomacy* (London: Sage Publications, 2004), 7-8.

[14] *Id.*

[15] *Id.*

[16] Barrinha A. and Renard T., *Cyber-Diplomacy: The Making of An International Society In The Digital Age Global Affairs*, 2017.

[17] *Id.*

implementation of foreign policy for the past 5 years (2014-2019). It is a certain that Indonesia's foreign policy is a derivative of the 4th paragraph of Preamble to the 1945 Constitution, and the Presidential/Vice President's Vision and Mission for 2019-2024.

Indonesia's foreign policy priorities will rest on *4+1 Formula*; improving the economic diplomacy, protection diplomacy, sovereignty and nationality diplomacy, as well as Indonesia's role in the region and globally.[18] The 'plus' is the improvement of diplomacy infrastructure. In relation with the cyber-diplomacy and security issues, it's important to highlight the current Indonesian Foreign Minister statement that "In order to strengthen the diplomacy of sovereignty and nationality, the integrity of the Republic of Indonesia is non-negotiable."[19] Therefore, from this clear statement, it's obvious that Indonesia has never been compromised with its sovereignty.

Furthermore, in several occasions, Indonesia's current Foreign Minister, Retno Marsudi, has repeatedly reiterated that Indonesian diplomacy will be done to protect the sovereignty of the Republic of Indonesia.[20] She emphasized that international relations should be based on the principle of respect for territorial integrity of each country and "Indonesia will not allow these principles are violated by anyone else."[21]

In addition, even though Indonesia has not yet issued any official national cybersecurity strategy, the 2020 BSSN's NCSS draft has stated explicitly the Indonesian government main responsibility to protect its sovereignty and all Indonesian nationals as stipulated under the 4th paragraph of Preamble to the 1945 Constitution. As explained previously in the second part, this draft also further enlightens one of the main purposes of the NCSS is to establish Indonesia a state which shall be independent, united, sovereign, just, and prosperous.[22] Thus, from the Indonesia current foreign policy priorities and the NCSS draft we may recognize how the Indonesian government seems to lean in the direction that sovereignty as a rule, not a principle.

Besides putting sovereignty as one of Indonesia's main foreign policy priorities and stated in the national cybersecurity strategy draft, we can also analyze how the country place the concept of sovereignty in the realm of cybersecurity from the one and only legal basis for regulating cybersecurity, privacy, and security, the EIT Law. Article 2 of the EIT Law states that "This Law shall apply to any person to take legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia,

[18] "Indonesian FM Presents the Diplomacy Priorities 2019-2024 to the House of Representatives," Ministry of Foreign Affairs of The Republic of Indonesia, accessed November 14, 2021, https://kemlu.go.id/portal/en/read/786/berita/indonesian-fm-presents-the-diplomacy-priorities-2019-2024-to-the-house-of-representatives

[19] *Id.*

[20] "Indonesia's Foreign Policy Priorities in 5 Years Ahead," Cabinet Secretariat of The Republic of Indonesia, accessed November 9, 2021, https://setkab.go.id/en/indonesias-foreign-policy-priorities-in-5-years-ahead/

[21] *Id.*

[22] The Indonesian National Cyber and Crypto Agency, *Indonesia National Cyber Security Strategy* (Jakarta: BSSN, 2020), 5.

which has legal effect within jurisdiction of Indonesia and/or outside jurisdiction of Indonesia and detrimental to the interest of Indonesia."[23]

In the Part of Explanation of this law, the explanation of Article 2 further describes that this law has a range of jurisdiction for all legal acts those not only apply in Indonesia and/or carried out by Indonesian nationals, but also apply to all legal acts committed outside the jurisdiction of Indonesia, both by Indonesian nationals or Indonesian legal entities and by foreign nationals or foreign legal entities, that have legal consequences in Indonesia.[24] It further explains that what is meant by "detrimental to the interest of Indonesia" includes but not limited to harming the interests of the national economy, protection of strategic data, national dignity, defense and security of the state, *state sovereignty*, citizens, and Indonesian legal entities.[25]

A more or less similar sound is also stipulated in Article 37 which states that " Any Person who knowingly commits prohibited acts as intended by Article 27 through Article 36 outside the territory of Indonesia towards Electronic Systems residing within jurisdiction of Indonesia."[26] By reading the two articles, it can be concluded that the scope of jurisdiction of the EIT Law does not only apply to Indonesia's sovereign territory, but also outside Indonesia. In other words, Article 2 and Article 37 of the EIT Law have exceeded the (extra) principle of territorial jurisdiction.

Therefore, Article 2 of the EIT Law even visibly encompasses the principle of extraterritorial jurisdiction. It is plainly written that the legal construction of the EIT Law does not only apply to Indonesian citizens, but also foreign nationals, both within and outside the territory of Indonesia. The juridical argument that underlies the application of this article is only if the legal action taken "has legal consequences within the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and is detrimental to the interests of Indonesia". Thus, it is clear that legal consequences within and/or outside the territory of Indonesia are not sufficient, but these legal actions must also harm Indonesia's interests. From all the articles and explanations, we can see how Indonesia positions significantly the concept of sovereignty in cyberspace. Even for the EIT Law, for instance, it can extend its jurisdiction outside the territory of Indonesia for any legal actions raising any consequences which detriment to the sovereignty of Indonesia.

3.2. Approach on Sovereignty based on Related Legal Cases

We can further observe Indonesia's approach on cyberattack attribution from the context of sovereignty through several related sovereignty-violation cases as an integral part of its foreign policy. Most of these cases were related to Indonesia's responses to foreign vessels conducting illegal fishing over the country's Exclusive Economic Zone (EEZ) around the Indonesia's Natuna Islands and the famous South China Sea issues, and

[23] Indonesia Electronic Information and Transactions Law No. 11/2008, Art. 2.
[24] *Id.*
[25] *Id.*
[26] *Id.,* Art. 37.

also a few cases over Indonesia's air-sovereignty violation. Meanwhile, other major cases related to Indonesia's cyberspace when dealing with foreign cyberattacks will be examined in the next part.

For the EEZ regime, we may realize that under the international law of the sea, particularly as regulated in the United National Convention on the Law of the Sea (UNCLOS), the territorial sea extends 12 nautical miles from the coastline, while the additional (contiguous) zone extends a further 12 nautical miles. The EEZ, meanwhile, extends a further 176 nautical miles from the edge of the contiguous zone – or 200 nautical miles from the coastline. In this case, around the Natuna Islands, Indonesia has a territorial sea, a contiguous zone, and an EEZ in accordance with the UNCLOS. According to the convention, Indonesia only has sovereignty over the waters of the territorial sea and the inland sea that exists between the islands.

These three sea regimes, furthermore, grant Indonesia different rights. In the territorial sea, Indonesia enjoys the same sovereignty as it does on the islands, with a few exceptions. In the EEZ, meanwhile, Indonesia enjoys so-called "sovereign rights," which grant it the exclusive right to utilize the natural resources that lie within it. No other countries have this right, but foreign ships are free to sail through EEZs without utilizing natural resources. If foreign ships want to take advantage of natural resources and carry out survey activities, they must get permission from Indonesia.

In relation with these three sea regimes concept, Indonesian patrol ships have also repeatedly attempted to detain Chinese fishing boats those were fishing illegally in the Natuna Sea or at least drove away those vessels from North Natuna waters, which is part of the Indonesia's EEZ. When the Natuna incident escalated in 2019, for instance, the Indonesian Coast Guard approached the Chinese Coast Guard and requested the vessels to order the Chinese fishing vessels to cease the illegal fishing activities and promptly leave the Indonesia's EEZ. This major incident has also led the Indonesian Government through its Foreign Ministry to summon the Chinese ambassador in Jakarta, and to issue a protest through a diplomatic note ad-dressed to the Chinese government via its embassy in Jakarta. The diplomatic note dated 30 December 2019, for example, utilized the "hardest" diplomatic terminologies those may be used in diplomatic correspondence to show the Indonesian Government's utmost displeasure.[27] Indonesia would also never recognize the Nine-Dash Line claimed by China since it does not have a legal basis recognized by international law, including the UNCLOS.[28]

From this case, we can learn how Indonesia has responded to Chinese vessel's illegal activities firmly, consistently, and persistently, even over such a "sovereign rights" regime. We may view how the country keeps showing its current position to remain firm on the matter of sovereignty as a rule, that is Indonesia's sovereign rights guaranteed by

[27] Damos Dumoli Agusman and Citra Yuda Nur Fatihah, "Celebrating The 25th Anniversary of Unclos Legal Perspective: The Natuna Case," *Indonesian Journal of International Law* (2020), Vol. 17 No. 4: 558-559, https://doi.org/10.17304/ijil.vol17.4.799

[28] *Id.,* 560-561.

the UNCLOS, as the Indonesia's EEZ had been acknowledged as Indonesia's territorial waters through the UNCLOS, and therefore there is no room for any negotiation. Even the Indonesian President Joko Widodo declared that "there is no bargaining when it comes to our sovereignty, our country's territorial," following the incident.[29] Therefore, the government of Indonesia has shown its standpoint to never negotiate for any questions on sovereignty.

Furthermore, in several other illegal fishing cases over Indonesia's EEZ conducted by other states, the Indonesian coast guard authorities have also continually blown up those foreign vessels after charging them with fishing illegally in the country's waters, bringing the number of vessels destroyed by the Government under the policy to more than hundreds up to now.[30] Even though this ship-sinking-policy is still debatable under the international law, here, the government of Indonesia tries to figure out that the idea of the ship-sinking policy against violators is legitimate because Indonesia has full authority as a sovereign country. Furthermore, all illegal activities done within the jurisdiction of Indonesia have been regulated in a certain way because Indonesia is a sovereign country and obliged to protect all territories judicially.[31]

Moreover, in several occasions, the related authorities have also clearly stated that the Indonesian government must protect all its citizens and territories as mandated under the Constitution. This responsibility, particularly, includes a commitment to maintain its sovereignty, where these authorities enlightened that sovereignty is not just covering territories but also on how people can be sovereign and standing for themselves.[32] In this case, the economic sovereignty as a maritime country is essential because many people depend on the fisheries and maritime sectors.[33] Therefore. presence of a constitutional platform as the supreme law confirms that Indonesia has everything needed to handle and maintain its sovereignty.

In the air-sovereignty regime, meanwhile, Indonesia has also shown its intention in endorsing sovereignty-as-a-rule. In a most recent case, in January 2019, two Indonesian F-16 fighter jets forced an Ethiopian Airlines cargo plane to land at an airport on Batam island, Indonesia, after it had flown into Indonesian airspace without permission.[34] The

[29] M Risyal Hidayat, "Indonesia Adds Patrols after Detecting Ships in South China Sea," *Al Jazeera*, September 17, 2021, https://www.aljazeera.com/news/2021/9/17/indonesia-increases-sea-patrols#:~:text=%E2%80%9CThere%20is%20no%20bargaining%20when,Widodo%20declared%20following%20the%20incident.&text=Maritime%20and%20Fisheries%20Minister%20Susi,fishing%20illegally%20in%20Indonesian%20waters.

[30] "Indonesian Government Destroys over 20 Foreign Vessels Due to Illegal Fishing," Stop Illegal Fishing, accessed November 1, 2021, https://stopillegalfishing.com/press-links/indonesian-government-destroys-20-foreign-vessels-due-illegal-fishing/

[31] Joko Setiyono, Muhamad Azhar, Solechan, Nanik Trihastuti, and Arief R. Hakim, "Justification of the Ship-Sinking Policy in the Territorial Jurisdiction of Indonesia," *AACL Bioflux* Volume 13, Issue 5 (2020): 2611.

[32] *Id.,* 2612.

[33] *Id.*

[34] Agustinus Beo Da Costa and Aaron Maasho, "Indonesian Jets Force Ethiopian Cargo Plane to Land over Airspace Breach," *Reuters*, January 14, 2019, https://www.reuters.com/article/us-indonesia-airlines-ethiopia/indonesian-jets-force-ethiopian-cargo-plane-to-land-over-airspace-breach-idUSKCN1P815S

cargo flight ETH 3728 had been flying from the Ethiopian capital Addis Ababa to Hong Kong in which the plane had made an urgent unscheduled flight to drop an aircraft engine in Singapore for maintenance.[35] In responding to this incident, Indonesian Air Force First Marshal Novyan Samyoga said in a statement that "the plane was crossing the Indonesian airspace in accordance with the ICAO Chicago Convention Article 5, by which a non-scheduled flight can overfly the airspace of a friendly country without prior permission."[36]

Even though again that policy was still debatable at that time and the political row between Indonesia and Singapore might have complicated the matter, we can conclude from the Indonesian Air Force claim that the Ethiopian Cargo was overflying Indonesia's sovereign skies without a permit. Here, the Indonesian authorities just want to show that the rules they enforce were clear: if anyone is overflying any Indonesian sovereign-territory, they must get an overflight permit, regardless of the flight level.[37] In this case, once more, the government of Indonesia seems appear to support the sovereignty-as-a-rule position.

3.3. Approach on Sovereignty based on Framework and Cooperation on Cybersecurity

Another important aspect of Indonesia's foreign policy is the international framework and cooperation among states, and therefore it is important to first understand the underlying logic of international cooperation in this policy domain. Indeed, cyberspace cumulates a number of characteristics that frame diplomatic engagement among stakeholders.[38] To begin with, it is a global domain connecting nations and citizens worldwide in a variety of manners, generating interactions and frictions between them. Furthermore, cyberspace is usually considered as a "global commons", defined as a "resource domain to which all nations have legal access."[39] In other words, various actors, both state and non-state, have the potential threat to disrupt the network because of the difficulty of identifying actors in cyberspace for certain actions and actions in a place that has an effect or impact in all parts of the world.[40] At the same time, both state and non-state actors, as well, have the main responsibility to secure and protect the cyberspace.

In relation to this international framework and cooperation on cybersecurity, we may also further analyze the Indonesia's approach on sovereignty. We can further develop those analysists based on Indonesia's cyber-diplomacy strategy and policy from the level of bilateral, regional, and multilateral. On international cyberspace policy, it participates actively in the Internet Governance Forum, the UN Group of Governmental Expert (UN

[35] *Id.*

[36] David Mumford, "Indonesia is Intercepting Aircraft – Outside Their Airspace," *OPS Group*, January 15, 2019, https://ops.group/blog/indonesia-is-intercepting-aircraft-outside-their-airspace/

[37] *Id.*

[38] A. Fathan Taufik, "Indonesia's Cyber Diplomacy Strategy as A Deterrence Means yo Face the Threat in the Indo-Pacific Region," *Journal of Physics: Conference Series*, The International Conference on Defence Technology (Autumn Edition, 2020): 5, https://doi:10.1088/1742-6596/1721/1/012048

[39] Buck S., *The Global Commons: An Introduction* (Washington, DC: Island Press, 1998), 8.

[40] A. Fathan Taufik, "Indonesia's Cyber Diplomacy Strategy," 6.

GGE), World Summit on the Information Society (WSIS), G20, the Asia-Pacific Economic Cooperation, the Association of Southeast Asian Nations (ASEAN), and the Organization of Islamic Cooperation.

In fact, Indonesia has some cyber-surveillance and cyber-espionage capabilities, but there is little evidence of it planning for, or having conducted, offensive cyber operations. Overall, Indonesia is a third-tier cyber power. Given that it is expected to become the fourth-largest economy in the world by around 2030, it could be well placed to rise to the second tier if the government decides that strategic circumstances demand greater investment in the cyber domain.

3.3.1. Bilateral Framework and Cooperation

At the bilateral level, Indonesia currently has Memorandum of Understanding (MoU) or Letter of Intent (LoI) on the cybersecurity or cyberspace cooperation with 10 countries: The United States, United Kingdom, Russia, China, Australia, Saudi Arabia, Poland, Turkey, Qatar, and the Czech Republic. The LoI between Indonesia and the United States, for example, has the purpose to provide a framework to promote cooperation and capacity building in cyber space between the two countries.[41] It has the scope of cooperation in some areas, including discussion on national cyber strategy development, national incident management capabilities, cybercrime capacity and cooperation, multi-stakeholder partnership, promotion of cyber security awareness, and cooperation in other relevant regional venues as appropriate.[42]

Furthermore, besides the LoI between Indonesia and the U.S. on cyber-cooperation, there is also one MoU between Indonesia and the United Kingdom on cybersecurity cooperation which also has the similar purpose to provide a framework for cooperation between the two states on cybersecurity.[43] Here, the two states will undertake to cooperate in the following areas of cybersecurity: National Cybersecurity Strategy Development and Implementation, Incident Management; Cybercrime; Promote Cybersecurity Awareness and Training; and Capacity Building.[44]

Meanwhile, the MoU between the Indonesia's BSSN and the China's Cyberspace Administration will provide a framework for cooperation in developing cyber security capacity and technology between the participants. In this Indonesia-

[41] "Letter of Intent Between the Government of the Republic of Indonesia and the Government of the United States of America on Promoting Strong Cyber Space Cooperation," Indonesia's Foreign Ministry, accessed November 3, 2021, https://treaty.kemlu.go.id/apisearch/pdf?filename=USA-2018-0367.pdf

[42] *Id.*

[43] "Memorandum of Understanding Between the Government of The Republic of Indonesia And the Government of the United Kingdom of Great Britain and Northern Ireland on Cyber Security Cooperation," Indonesia's Foreign Ministry, accessed November 3, 2021, https://treaty.kemlu.go.id/apisearch/pdf?filename=GBR-2018-0068.pdf

[44] *Id.*

China MoU, most importantly, the two states agreed to uphold *the principle of respect for state sovereignty on cyberspace* and work together to promote the establishment of a multilateral, democratic and transparent international internet governance system, data security, and the building of a peaceful, secure, open, cooperative, responsible, and orderly cyberspace as well as information and communication technology development.[45] The MoU also highlighted that the participants should respect each other's jurisdiction and governance of data and shall not obtain data located in the other participant through companies or individuals without the other participant's permission. Moreover, the participants should require domestic information and communication technology products and services providers not to install backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices.[46]

We can obviously see from these three MoUs and LoI the significant differences on the sovereignty approach endorsed by those states. In the MoU between Indonesia and the U.S., and between Indonesia and the U.K., for example, the two states did not specifically mention about sovereignty and even any other issues related to sovereignty. Here, we may conclude explicitly that both the U.S. and the U.K. endorse sovereignty-as-a-principle. In contrast, the LoI between Indonesia and China clearly highlighted the importance for the two countries to respect each other's sovereignty on cyberspace and jurisdiction. From this LoI we may view China's approach on sovereignty that appear to endorse the sovereignty-as-a-rule position. Indonesia, similarly, tends to endorse the sovereignty-as-a-rule position where it upholds the principle of respect for state sovereignty on cyberspace, as stipulated in the MoU or LoI on cybersecurity cooperation between Indonesia and other states outside the U.S. and the U.K.

3.3.2. Regional Framework and Cooperation

The ASEAN region indeed presents an excellent strategic and commercial opportunity which is already a core part of the world's economy. ASEAN economies are fast growing and the region's population is growing rapidly as well: the region is set to become the equivalent of the world's fourth-largest economy by 2030, with a current population of around 637 million people.[47] Digital disruption across the region has been rapid, and the demand for digital goods and services is accelerating.

[45] "Memorandum of Understanding Between the National Cyber And Crypto Agency of The Republic of Indonesia And the Cyberspace Administration of The People's Republic of China On Cooperation In Developing Cyber Security Capacity And Technology," Indonesia's Foreign Ministry, accessed November 3, 2021, https://treaty.kemlu.go.id/apisearch/pdf?filename=CHN-2021-0228.pdf

[46] *Id.*

[47] "ASEAN Remains Prime Target for Cyberattacs," *Nikkei Asian Review*, 8 February, 2018, asia.nikkei.com/Business/Business-trends/ASEAN-remains-prime-target-for-cyberattacks

As ASEAN economies thrive, their digital threat landscape has expanded. This has triggered demand for all types of cyber security and across all types of organisations – from government agencies to app developers. According to A.T. Kearney, countries within ASEAN are being used as a launch pad for malicious cyber activities. Vietnam, Indonesia and Malaysia are global hotspots for malware attacks.[48] Therefore, the need to protect fast-evolving digital economies creates a vast, addressable market for cyber specialists. The US-based Asia Pacific Risk Centre projects that the global cost of data breaches to businesses in the region will be approximately $2.8 trillion by 2020.[49]

As a consequence, particularly within the ASEAN framework, the cybersecurity issues have been one of the most priorities issues in three main ASEAN mechanisms. They are the *ASEAN Defence Ministers' Meeting Plus (*ADMM-Plus**)** where the cybersecurity issues are discussed through the *ADMM-Plus Experts' Working Group on Cyber Security* (EWG on CT), the *ASEAN Ministerial Meeting on Transnational Crime* (AMMTC) where the cybercrime issues are examined through the ASEAN Senior Officials' Meeting on Transnational Crime Working Group on Cybercrime (ASEAN SOMTC), and the *ASEAN Regional Forum* (ARF), where the cybersecurity cooperation are arranged under the framework of *Security of and in the Use of Information and Communication Technologies* (ICTs).

Indeed, one of the Indonesia's strategic alliances in cybersecurity policy is by cooperating with the ASEAN as it is also one of the Indonesia's commitments to realize ASEAN's three pillars, the ASEAN Economic Community, the ASEAN Socio-Cultural Community, and the ASEAN Political-Security Community. Another commitment is to have a stronger cooperation with ARF to support the three pillars. Indonesia was also one of the countries that initiated the Treaty of Amity and Cooperation (TAC). Substantially, the fellow member states do not attack each other and resolve conflicts in a peaceful manner[50]

Indonesia has also been consistently partnering with ASEAN in cyber security sector, because of the prominence of Malaysia's and Singapore's cybersecurity development.[51] Malaysia, for example, has prepared cyber security supporting policies, institutions, infrastructures, and programs and the effort has been discussed in international cooperation forums. The institution in-charge that runs cyber security functions in Malaysia is called "Siberoc," which coordinates with Malaysia's information security institutions such as Malaysian Computer

[48] Cyber Security in ASEAN: An Urgent Call to Action (2017), A.T. Kearney, 10.

[49]"Southeast Asia Cybersecurity Emerging Concern," *The ASEAN Post*, 20 May, 2018, theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern

[50] Muhamad Rizal and Yanyan M. Yani, "Cybersecurity Policy and Its Implementation in Indonesia," *Journal of ASEAN Studies* 4, No. 1 (2016): 73.

[51] *Id.*

Emergency Response Team (MyCERT).[52] Meanwhile, Singapore excels in its human resources, having the highest number of information security experts in ASEAN.[53]

Indonesia and ASEAN have been consistently partnering in security sector because ASEAN has given some contribution to Indonesia to deal with cyber threats. In ASEAN Regional Forum (ARF), Indonesia and ASEAN work together in tackling cybercrime by improving the security level in states' cyber-sector. Consequently, along with other ASEAN countries, Indonesia was committed to develop its cyber security and would consistently do so until the beginning of ASEAN Community in 2015.

One of the most recent and relevant documents related to cybersecurity cooperation among ASEAN member states would be the ASEAN Leader's Statement on Cybersecurity Cooperation that was established by all 10 member's heads of state/government during the 32nd ASEAN Summit in 2018. In the document, all member states clearly state that they acknowledge the *state sovereignty* and international norms and principles that flow from sovereignty apply to the conduct by states of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory. Here, we can obviously observe how all the member states highlighted the significance of the concept of the state sovereignty, as well as the international norms and principle derived from that concept to be applied by the member states in any ICT-related activities. Therefore, ASEAN as a regional organization with 10-member states, including Indonesia with its similar position as well, appear to endorse the sovereignty-as-a-rule position.

In other words, South East Asia remains a region where strong nationalism prevails and ASEAN has always favored a strong commitment to preserving and respecting national sovereignty. In this context, the elaboration of cyber norms, which would define proper state behavior in cyberspace in conformity with a set of collective expectations, will obviously depend on the member states' true political will to engage in this work.

3.3.3. Multilateral Framework and Cooperation

At the multilateral level, Indonesia participates actively in the UNGGE and so far has become a member in 2012, 2014, and 2019-2021. In any multilateral forums and meetings, particularly during the Indonesia's presidency of the United Nations Security Council (UNSC) for the period 2019-2020, Indonesia has been consistently emphasizing the need for all states to adhere to the principles of the

[52] The Ministry of Defense of the Republic of Indonesia, *A Road Map to Cyber Defense National Strategy*, (Jakarta: The Ministry of Defense of the Republic of Indonesia, 2013), 42.

[53] *Id*, 58.

UN Charter and international law in maintaining peace and stability in cyberspace. Furthermore, the country also underlined that all states and entities share common responsibilities to ensure the use of ICTs for peaceful purposes. Indeed, controlling the behavior of malicious non-state actors in the ICTs environment, in this regard, poses special difficulties. This makes international cooperation and collaboration all the more critical.

Furthermore, on May 22, 2020, Estonia, supported by other co-sponsors including Belgium, Indonesia, Kenya, and the Dominican Republic, held a virtual *Arria Formula* entitled "Cyber Stability, Conflict Prevention, and Capacity Building". The meeting discussed the global efforts in strengthening the stability and preventing the conflicts related to various threats in the cyber realm, as well as the global, regional, and national norms and mechanisms in overcoming those cyber threats as efforts to promote international cooperation and collaboration. Moreover, on August 26, 2020, Indonesia initiated another virtual *Arria Formula* entitled "Cyber Attacks Against Critical Infrastructure" which was attended by 40 speakers with three briefers (ICRC President, UNOCHA Deputy, and UNIDIR Director), 14 UNSC member countries and 23 non-UNSC member countries, with the participation from 20 delegates at the Ambassadorial level. The meeting discussed the issue of critical infrastructure vulnerabilities and the humanitarian consequences of cyberattacks, as well as the global efforts in protecting that critical infrastructure from cyberattacks and the aspects of international legal protection and norms related to state behavior in cyberspace to protect such a critical infrastructure from the context of maintaining international peace and security.[54]

In this regard, with the ever-increasing cyber connectivity, critical infrastructure is exposed to an array of threats and vulnerabilities, which raise new security concerns, where Such challenges are faced by an ever-growing number of countries, Indonesia is therefore of the view that protection of critical infrastructure against cyberattacks will become even more important in the future. Indonesia then underlined three points.[55] First, Indonesia encourages all states to acknowledge that cyber-attacks on critical infrastructure can have widespread consequences, including humanitarian and therefore more attention needs to be paid on cyberattacks against critical infrastructure by both state and non-state actors, including proxies. Cyberattacks also pose risks towards instability in international peace and security with consequences becoming uncontrollable, even potentially claim human lives. Second, the protection of critical infrastructures requires strengthening of norms, international law as well as national legislation and therefore the principles of international law and the UN Charter provide the

[54] Perutusan Tetap Republik Indonesia untuk PBB di New York, Kompilasi Statement Indonesia di Dewan Keamanan PBB 2019-2020 (Kementerian Luar Negeri Republik Indonesia: Jakarta, 2001), 877-879.

[55] *Id.*

fundamental framework in guiding states on their use of ICT. Consequently, Indonesia supports the norms of responsible state behavior outlined in the UNGA Resolution 70/237, as there must not be any intentional damage or impairment in the use and operation of critical infrastructure. The norms also underline the importance of appropriate measures by states to protect their critical infrastructure from the ICT threats with due regard to their applicable national laws. To that end, Indonesia supports the ongoing processes in the General Assembly, particularly through the current meaningful works of the GGE and the OEWG.

There is also a need to widen understanding and deepen engagement among countries and regions, including to address divergent views on some of the major concepts in international law that apply in cyberspace since there is no universal concept of critical infrastructure, the determination of critical infrastructure lies in domestic domain. Therefore, it is necessary to address gaps in cyber resilience among countries in not only ICT infrastructure, and to build capacity for the implementation of international law and cyberspace norms, within the national policy frameworks.

And third, the country again highlighted that bilateral, regional and global efforts are necessary and mutually reinforcing in the advancement of common understanding on cyber security issues, where more capacity and confidence building measures (CBMs) are required to bolster stability of cyberspace. This process should involve private sector, technical community and civil society. In this regard, Indonesia restated that regional organizations play an indispensable role in peacemaking on the ground. There is considerable potential yet in stepping up their presence in cyberspace, both regionally and globally, to innovatively advance the sustaining peace agenda.

As mentioned earlier in previous part, Indonesia has emphasized that regional organizations play an indispensable role in peacemaking on the ground. There is considerable potential yet in stepping up their presence in cyberspace, both regionally and globally, to innovatively advance the sustaining peace agenda. For instance, Indonesia, bilaterally, and through various ASEAN mechanisms is working actively to bolster ASEAN peacemaking initiatives via the cyber front. In that context, ASEAN CBMs through the establishment of Points of Contact, regular information exchanges, dialogues and sharing of best practices are already resulting in more meaningful collaboration with important benefits for Southeast Asia and beyond. In this regard, Indonesia also sees the potential ways forward in linking CBMs across the region with a view to promote exchanges of regional best practices to be taken into the global scale.

It is indeed necessary to address gaps in cyber resilience among countries and regions in not only ICT infrastructure, but also in the implementation of international law and cyberspace norms. Some of the challenges are the lack of

awareness, varying understanding and interpretation, as well as technical capacity and financial constraints for the implementation of existing voluntary and non-binding norms. Overall, Indonesia underlines a holistic approach for capacity building, which covers technical, policy, and legal aspects along with adequate interaction and support from multi-stakeholder entities.

Finally, we may imply that on various multilateral forums and meetings, Indonesia always underscore all the states to respect the principles of the UN Charter and international law is essential in maintaining peace and stability in cyberspace, including the principle to respect the state sovereignty. Meanwhile, during its UNSC chairmanship, it stressed the importance of responsible behavior in cyberspace, the role of regional organizations in conflict prevention, and the essentials of capacity building for cyber resilience.

4. CONCLUSION

From the analysis through all parts of this paper we may conclude that Indonesia is currently in the early stages of developing a national cybersecurity strategy where the legal framework for cybersecurity in is still weak. At the same time, Indonesia has been recently become one of the most cyber-attack targeted country in the world due to this lack of cyber capacities and capabilities. While lacking data protection regulation and any related cybersecurity provisions, Indonesia also lack of national policy and strategy when it seeks to defend itself against cyberattack, particularly those hacking activities from foreign actors or state-sponsored groups. In this regard, majority of states in the world have two different approaches on cyberattack attribution from the context of sovereignty, those applied sovereignty as a rule and as a principle. Meanwhile, Indonesia has never stated clearly its position Indonesia belongs to those countries that has never stated clearly its position whether it endorses sovereignty-as-a-rule view or sovereignty-as-a-principle view. However, based on the analysis on the previous part, we may conclude that Indonesia appears to endorse the sovereignty-as-a-rule position, where it upholds the principle of respect for state sovereignty on cyberspace.

REFERENCES

Agusman, Damos Dumoli and Citra Yuda Nur Fatihah. "Celebrating The 25th Anniversary of UNCLOS Legal Perspective: The Natuna Case." *Indonesian Journal of International Law* (2020), Vol. 17 No. 4: 558-559. https://doi.org/10.17304/ijil.vol17.4.799.

Anjani, Noor Halimah. "Policy Brief No. 9: Cybersecurity Protection in Indonesia." *Center for Indonesian Policy Studies*, March, 2021.

The ASEAN Post. "Southeast Asia Cybersecurity Emerging Concern." Accessed 20 May, 2018. https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern.

Barnsby, Robert E. and Shane R. Reeves. "Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Chapter." 95 *Texas Legal Review* (2017): 1529.

Barrinha A. and Renard T. *Cyber-Diplomacy: The Making of An International Society in The Digital Age Global Affairs.* 2017. https://doi.org/10.1080/23340460.2017.1414924.

C., Jönsson and Langhorne R. *Diplomacy: Volume III. Problems and Issues in Contemporary Diplomacy.* London: Sage Publications, 2004. https://doi.org/10.4135/9781446261392.

Cabinet Secretariat of The Republic of Indonesia. "Indonesia's Foreign Policy Priorities in 5 Years Ahead," Accessed November 9, 2021. https://setkab.go.id/en/indonesias-foreign-policy-priorities-in-5-years-ahead/ .

Center for Indonesian Policy Studies. "Protecting People: Promoting Digital Consumer Rights." Accessed September 27, 2021. https://www.cips-indonesia.org/digital-consumer-rights-pp27 .

Chatham House Royal Institute for International Affairs. Cyber and International Law in the 21st Century, May 23, 2018. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century .

Cimpanu, Catalin. "Indonesian Intelligence Agency Compromised in Suspected Chinese Hack." The Record by Recorded Future, September 10, 2021. https://therecord.media/indonesian-intelligence-agency-compromised-in-suspected-chinese-hack/.

Corn, Gary P. & Robert Taylor. *Sovereignty in the Age of Cyber*. 111 Am. J. Int'l L. Unbound 208 (2017). https://doi.org/10.1017/aju.2017.57.

Corn, Gary P.. *Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention* 6–14 (Hoover Inst. Working Group on Nat'l Sec., Tech., and L., Aegis Series Paper No. 2005, 2020). https://www.hoover.org/sites/ default/files/research/docs/corn_webready.pdf

Corn, Gary P.. Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses, Just Sec. (Feb. 11, 2020). https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/

Czech Republic. Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace, Director of Cybersecurity Department, 2nd Substantive Session of the Open-Ended Working Group on Developments in the Field of Info. & Telecomm. in the Context of Int'l Sec. of the First Comm. of the General Assembly of the United Nations Feb. 11, 2020. https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20%20 International %20Law%2011.02.2020.pdf.

Da Costa, Agustinus Beo and Aaron Maasho. "Indonesian Jets Force Ethiopian Cargo Plane to Land over Airspace Breach." *Reuters*, January 14, 2019. https://www.reuters.com/article/us-

indonesia-airlines-ethiopia/indonesian-jets-force-ethiopian-cargo-plane-to-land-over-airspace-breach-idUSKCN1P815S.

Deeks, Ashley. *Defend Forward and Cyber Countermeasures 2,* Hoover Inst. Working Group on Nat'l Sec., Tech., and L., *Aegis Series Paper* No. 2004, 2020. https://www.hoover.org/research/defend-forward-and -cyber-countermeasures.

Djafar, W., Sumigar, F., & all. *Perlindungan Data Pribadi di Indonesia: Ulasan Pelembagaan Dari Perspektif Hak Asasi Manusia*. Jakarta: ELSAM Press, 2016.

Eichensehr, Kristen E.. "Cyberattack Attribution as Empowerment and Constraint." Hoover Working Group on National Security, Technology, and Law, *Aegis Series Paper,* No. 2101 (January 15, 2021). https://www.lawfareblog.com/cyberattack-attribution-empowerment-and-constraint.

Eichensehr, Kristen E. "The Law and Politics of Cyberattack Attribution." 67 *UCLA Law Review* (2020): 522.

Finnemore, Martha & Duncan B. Hollis. "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity," *European Journal of International Law*, (forthcoming 2020) (manuscript at 12). https://doi.org/10.1093/ejil/chaa056.

Finnish Ministry of Foreign Affaris, Press Release. Finland Published Its Positions on Public International Law in Cyberspace (Oct. 15, 2020). https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace.

French Ministry of the Armies. International Law Applied to Operations in Cyberspace (2019). https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+oper ations+in+cyberspace.pdf.

Greenberg, Andy. *A Brief History of Russian Hackers' Evolving False Flags, Wired*, October 21, 2019. https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/.

H., Bull. *The Anarchical Society: A Study of Order in World Politics* (3rd ed). Basingstoke: Palgrave, 1977/2002. https://doi.org/10.1007/978-1-349-24028-9.

Hidayat, M. Risyal. "Indonesia Adds Patrols after Detecting Ships in South China Sea." *Al Jazeera*, September 17, 2021. https://www.aljazeera.com/news/2021/9/17/indonesia-increases-sea-patrols - :~:text="There is no bargaining when,Widodo declared following the incident.&text=Maritime and Fisheries Minister Susi,fishing illegally in Indonesian waters.

The Indonesian National Cyber and Crypto Agency. "Cyberattack Data (January – April 2020)." Accessed October 1, 2021. https://bssn.go.id/rekap- serangan-siber-januari-april-2020.

The Indonesian National Cyber and Crypto Agency. *Annual Report 2020: Cybersecurity Monitoring*. Jakarta: BSSN, 2020.

The Indonesian National Cyber and Crypto Agency. *Indonesia National Cyber Security Strategy*. Jakarta: BSSN, 2020.

The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, UN Doc. A/56/10 (2001).

The International Telecommunication Union. *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity*. Geneva: ITU Publications, 2021.

Jeff, Kosseff. *Cybersecurity Law*. United States: Wiley, 2019. https://platform.virdocs.com/r/s/0/doc/1488325/sp/156513543/mi/507507143?cfi=%2F4%2F2%2F6%2F4%5Bhead-2-98%5D%2C%2F1%3A0%2C%2F1%3A0.

Jurriëns, Edwin and Ross Tapsell. "Challenges and Opportunities of the Digital 'Revolution' in Indonesia." In *Digital Indonesia.* Singapore: ISEAS Publishing, 2017. https://doi.org/10.1355/9789814786003-007.

Kearney, A.T.. Cyber Security in ASEAN: An Urgent Call to Action (2017).

Kementerian Komunikasi dan Informasi Republik Indonesia. "DPR telah Adakan Rapat Dengar Pendapat Umum terkait RUU PDP." Accessed September 27, 2021. https://aptika.kominfo.go.id/2020/07/dpr-telah-adakan-rapat-denger-pendapat-umum-terkait-ruu-pdp/.

Kilovaty, Ido. *Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare, Cyber Warfare and The Jus Ad Bellum Challenges* (2014).

Lin, Herbert. "Attribution of Malicious Cyber Incidents 5." Hoover Inst. Working Group on Nat'l Sec., Tech., and L., *Aegis Series Paper* No. 1607, 2016. https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

M, Wight. *System of States*. Leicester: Leicester University Press, 1979.

Miller, Greg et al. "Obama's Secret Struggle to Punish Russia for Putin's Election Assault." *Washimgton Post,* June 23, 2017. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/.

The Ministry of Defense of the Republic of Indonesia. *A Road Map to Cyber Defense National Strategy*. Jakarta: The Ministry of Defense of the Republic of Indonesia, 2013.

The Ministry of Foreign Affairs of the Republic of Indonesia. "Indonesian FM Presents the Diplomacy Priorities 2019-2024 to the House of Representatives." Accessed November 14, 2021. https://kemlu.go.id/portal/en/read/786/berita/indonesian-fm-presents-the-diplomacy-priorities-2019-2024-to-the-house-of-representatives.

The Ministry of Foreign Affairs of the Republic of Indonesia. "Letter of Intent Between the Government of the Republic of Indonesia and the Government of the United States of America on Promoting Strong Cyber Space Cooperation." Accessed November 3, 2021. https://treaty.kemlu.go.id/apisearch/pdf?filename=USA-2018-0367.pdf.

The Ministry of Foreign Affairs of the Republic of Indonesia. "Memorandum of Understanding Between the Government of The Republic of Indonesia And the Government of the United Kingdom of Great Britain and Northern Ireland on Cyber Security Cooperation." Accessed November 3, 2021. https://treaty.kemlu.go.id/apisearch/pdf?filename=GBR-2018-0068.pdf.

The Ministry of Foreign Affairs of the Republic of Indonesia. "Memorandum of Understanding Between the National Cyber and Crypto Agency of The Republic of Indonesia And the Cyberspace Administration of The People's Republic of China on Cooperation In Developing Cyber Security Capacity And Technology." Accessed November 3, 2021. https://treaty.kemlu.go.id/apisearch/pdf?filename=CHN-2021-0228.pdf.

Mumford, David. "Indonesia is Intercepting Aircraft – Outside Their Airspace." *OPS Group*, January 15, 2019. https://ops.group/blog/indonesia-is-intercepting-aircraft-outside-their-airspace/.

NCSI Project Team e-Governance Academy. "National Cyber Security Index 2020." Accessed October 1, 20201. https://ncsi.ega.ee/country/id/.

Netherlands Ministry of Foreign Affairs. Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the Int'l Legal Order in Cyberspace, Appendix at 8–9. July 5, 2019. https://www.government.nl/binaries/government/documents/parliamentary documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-orderincyberspace/ International+Law+in+ the+Cyberdomain+Netherlands.pdf.

New Zealand Foreign Affairs and Trade. The Application of International Law to State Activity in Cyberspace (Dec. 1, 2020). https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/.

Nikkei Asian Review. "ASEAN Remains Prime Target for Cyberattacks." Accessed 8 February, 2018. https://asia.nikkei.com/Business/Business-trends/ASEAN-remains-prime-target-for-cyberattacks.

Nugroho, A. "Personal Data Protection in Indonesia: Legal Perspective." *International Journal of Multicultural and Multireligious Understanding* 7, No. 7 (2020): 183-189. https://doi.org/10.18415/ijmmu.v7i7.1773.

Office of The Director of National Intelligence. A Guide to Cyber Attribution, September 14, 2018.

Owens, W. Et Al., Eds. *Technology, Policy, Law, And Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. National Research Council, 2009.

Paul C. Ney Jr. General Counsel, Dep't of Def. DOD General Counsel Remarks at U.S. Cybe Command Legal Conference (March 2, 2020). https://www.defense.gov/Newsroom/Speeches /Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

Perutusan Tetap Republik Indonesia untuk PBB di New York. Kompilasi Statement Indonesia di Dewan Keamanan PBB 2019-2020. Kementerian Luar Negeri Republik Indonesia: Jakarta, 2001.

Potkin, Fanny. "Indonesia's Tokopedia Probes Alleged Data Leak of 91 Million Users." *Reuters*, May 2, 2020. https://www.reuters.com/article/us-tokopedia-cyber/indonesias-tokopedia-probes-alleged-data-leak-of-91-million-users-idUSKBN22E0Q2.

Przemysław Roguski. *The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States* (May 11, 2020), https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-incyber space-by-austria-the-czech-republic-and-united-states/.

Rahardjo, Budi. "7 The State of Cybersecurity in Indonesia." In *Digital Indonesia.* Singapore: ISEAS Publishing, 2017. https://doi.org/10.1355/9789814786003-007.

Rid, Thomas & Ben Buchanan. *Attributing Cyber Attacks*. 38 J. Strat. Stud. 4, 14–23 (2015). https://doi.org/10.1080/01402390.2014.977382.

Riyadi, Gliddheo Algifariyano. "Policy Brief No. 7: Data Privacy in the Indonesian Personal Data Protection Legislation." *Center for Indonesian Policy Studies*, March, 2021.

Rizal, Muhamad and Yanyan M. Yani. "Cybersecurity Policy and Its Implementation in Indonesia." *Journal of ASEAN Studies* 4, No. 1 (2016). https://doi.org/10.21512/jas.v4i1.967.

S., Buck. *The Global Commons: An Introduction*. Washington, DC: Island Press, 1998.

Schmidt, Michael S. & Nicole Perlroth. U.S. Charges Russian Intelligence Officers in Major Cyberattacks, N.Y. Times, October 19, 2020. https://www.nytimes.com/2020/10/19/us/politics/russian-intelligence-cyberattacks.html.

Schmitt, Michael N. & Liis Vihul. *Sovereignty in Cyberspace: Lex Lata Vel Non?* 111 Am. J. Int'l L. Unbound 213 (2017). https://doi.org/10.1017/aju.2017.55.

Schmitt, Michael N., Ed. *Tallinn Manual 2.0 On the International Law Applicable To Cyber Operations* (2017). https://doi.org/10.1017/9781316822524.

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. "An Overview of the Development Indonesia National Cyber Security." *International Journal of Technology & Computer Science* (IJTCS) 6, (December 2012): 111.

Setiyono, Joko, Muhamad Azhar, Solechan, Nanik Trihastuti, and Arief R. Hakim. "Justification of the Ship-Sinking Policy in the Territorial Jurisdiction of Indonesia." *AACL Bioflux* Volume 13, Issue 5 (2020): 2611.

The Software Alliance. "Asia-Pacific Cybersecurity Dashboard." Accessed September 17, 2021, www.bsa.org/APACcybersecurity.

Stop Illegal Fishing. "Indonesian Government Destroys over 20 Foreign Vessels Due to Illegal Fishing." Accessed November 1, 2021. https://stopillegalfishing.com/press-links/indonesian-government-destroys-20-foreign-vessels-due-illegal-fishing/.

Taufik, A. Fathan. "Indonesia's Cyber Diplomacy Strategy as A Deterrence Means yo Face the Threat in the Indo-Pacific Region." *Journal of Physics: Conference Series*. The International Conference on Defence Technology (Autumn Edition, 2020): 5. https://doi:10.1088/1742-6596/1721/1/012048.

Tjan, Chandra. "The Land of Unicorns: The Rise of Start-Ups in Indonesia," *The Jakarta Post*, May 7, 2021. https://www.thejakartapost.com/paper/2021/05/06/the-land-of-unicorns-the-rise-of-start-ups-in-indonesia.html.

US Cyber Command. Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command (2018). https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=201806-14-152556-010.

US Cyber Command. The Fiscal Year 2021 Budget Request for U.S. Cyber Command and Operations in Cyberspace: Hearing Before the H. Comm. on Armed Servs., Subcomm. on Intelligence and Emerging Threats and Capabilities, 116th Cong. 44 (2020).

US Department of Defense. Summary: Department of Defense Cyber Strategy (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

The World Bank. "Ensuring a More Inclusive Future for Indonesia through Digital Technologies." Accessed October 5, 2021. https://www.worldbank.org/en/news/press-release/2021/07/28/ensuring-a-more-inclusive-future-for-indonesia-through-digital-technologies.