Technology Disruptions in International Relations:

The Needs for Cyber Diplomacy by Indonesia

Arindha Nityasari
Universitas Gadjah Mada, Indonesia
arindha.nityasari@ugm.ac.id

10.22146/globalsouth.50432

The research will discuss about the impacts of technology disruption in international relations. This study aims to increase awareness about several disrupted areas in international politics, particularly in security niche. It will also examine technology disruptions in Indonesia as one of the Global South countries and see the gaps between South and North relations in the field of cyber security. This article also argues that multidiscipline and multi-stakeholder approach through cyber diplomacy is the most feasible solution to tackle the issues arising from technology disruption.

Keywords: *cyber security; cyber diplomacy; technology disruption*

Introduction

The advancement of technology has emerged and been amplified through many campaigns such as the known Industrial Revolution 4.0. It said that we are now entering an era where technology transforms in an unprecedented way that it will affect society and industry with the supports of digital, physical, and biological technologies being developed. It is associated with development of internet, the use of cloud for storage, artificial intelligence, robots, and other technologies to assist humans in conducting their activities. Nevertheless, this phenomenon also affects political scope in national and international level. Some changes have taken place ever since this technology advancement (Schwab, 2016).

In national level, technology advancement particularly impacts the bureaucracy, for instance, technology enables wider public engagement, thus it changes the policy and decision-making process of the government in either positive or negative ways (Schwab, 2016). In international level, technology advancement brings about new form of conflict. In the past, conflict involved traditional weaponry such as guns, bombs, tanks, and such kinds. Meanwhile nowadays, modern conflict happens through digital media, for instance is the information stealing by other countries (Schwab, 2016).

In terms of international relations, in his book, Barston (2014, 112-123) argues that technology revolution has brought about four fundamental changes in the nature of diplomacy. First is technology has modified the relations of distance and time. This refers to the fact that technology enables previously domestic issues to be brought to global attention through fast-paced media channels such as television or mobile phones. Secondly, traditional diplomacy way of conflict or issue assessment becomes

difficult to implement because of information abundance circulated in the media. Third is technology has blurred the line between private and public sphere. The personal communication system is functionally widened to the extent that it is used for a diplomatic tool. Lastly, technology revolution brings along new potential threats to the existing diplomatic system. In this sense, he concludes that there will be wider array of issues that needs to be tackled by cyber diplomatic means (Barston, 2014).

With the issues on cyber-related problems have been going around in the global level, Indonesia is deemed as lacking of persistence in the attempt to engage in the field of cyberspace. As of this paper is being written, Indonesia has zero arrangement with other countries in cyberspace regulations and cooperation, but Indonesia has had to deal with cyber threats. In 2018, data showed that Indonesia has been hit by more than 200 million cyber-attacks (Natalia, 2019). Moreover, Kaspersky predicted Indonesia to be facing cyber threats during 2019 presidential process, especially on tampered data of casted votes (Nugraha, 2019).

With the issues on cyber-related problems have been going around in the global level, Indonesia is deemed as being late to catch up with the issues. Tracing back to its historical context, Indonesia has started to pay attention on cybersecurity since 2007 when the first Indonesian law addressing internet protocol to ensure telecommunication safety was released (Peraturan Menteri Komunikasi dan Informatika Nomor 27/PER/M.KOMINFO/9/2006 tanggal 20 September 2006).

In fact, Indonesia has dealt with cyber threats such as what happened in 2018 when data showed that Indonesia has been hit by more than 200 million cyber-attacks (Natalia, 2019). Moreover, Kaspersky predicted Indonesia to be facing cyber threats during 2019 presidential process, especially on tampered data of casted votes. This prediction was made out of the past experience when data collection for quick count was impeded (Nugraha, 2019). The prediction came into realisation in which General Election Commission of Indonesia received thousands of cyber-attacks nearing the election process back in April 2019. Such attacks used Internet Protocol (IP) address from Russia and China (Situs KPU Kerap Diretas Lewat 'IP Address' Rusia dan China, 2019). However, that does not necessarily mean that the perpetrators were Russian and Chinese. Indonesian who resided domestically might also be able to be the doers of the operations. With the technology advancement, a sophisticated user can disguise their IP address by pointing at another connection node as if the activity was conducted through that particular node. Besides, IP address is not enough to provide the individual information because tracking a perpetrator by the IP address is like trying to identify a driver only with the license plate (Singer & Friedman, 2014).

According to DAKA Advisory Research on cyber security in Indonesia (2013; 17), most of the politically-motivated cyberattack in Indonesia is hacktivism and government website defacing. In addition, as the report said, Indonesia is prone to other non-political cyberattack particularly cybercrime on financial fraud, malware attack on personal computers, social engineering through emails, as well as identity-theft on social media. In which, most of those cyberattacks are due to the people's lack of

awareness (DAKA Advisory, 2013, 18-19).

The mentioned notions prove how weak Indonesia's cyber security still is. To add, these significant examples also give an illustration that as technology becomes more advanced, dealing with cyber-attacks becomes transnational. Hence, cyber diplomacy becomes an essential solution for the said problems. Cyber diplomacy, to put it simply, is known as the government's attempt to conduct diplomacy in order to maintain and secure their interest in the niche of cyberspace (Riordan, 2016).

To elaborate the arguments, the paper will be divided into three parts. The first part will give understanding about technology disruption in the context of international relations. In this part, several cases of cyber-attacks or cyber war in the global level will be provided to better grasp the idea of technology disruption. The second part will discuss about the needs for cyber diplomacy for Indonesia to anticipate the future problems. This part will include how cyber diplomacy is ideally conducted according to the scholar, as well as practically conducted by practitioners. The last part will be conclusion.

Methodology

This paper focuses on how technology has disrupted international relations and to what extent is the impact on Indonesia's cyber diplomacy. In the end, this paper will be equipped with some recommendations on how Indonesia should direct its cyber diplomacy is based upon 1) the concept from books or articles and 2) empirical cases from news and articles. Thus, this research will be conducted by qualitative assessment where data being used are secondary ones. The data collected include previous publication such as from news, articles, and books that have relevancies with cyber issues (i.e. cyber-attack, cyber warfare, cybersecurity, and cyber diplomacy) from international and domestic contexts.

Technological Disruptions in International Relations

Theories of International Relations in the Context of Technological Disruption

Apart from the phenomena happen during the era of technological disruption in the international arena, as a discipline, International Relations have been equipped with several basic theories to see and explain international relations occurrences. The most used, classic theories in International Relations include realism, liberalism, and Marxism. In his book, Deibert (2002) elaborated that new technologies that penetrate our lives today have affected many layers of society including the world politics. As a prominent discipline discussing about world politics, International Relations is deemed lacking of theories to describe the disrupted area of world politics due to new technologies.

Realism is slow in grasping the idea that new technologies are coming. It is in the sense that realists deem new technologies as tools to facilitate the existing power play. Realists argue that new technologies do not change power or social relations structurally, but only transform the way the existing structure works. Realists believe in the notions of power competition among states. Thus, realism sees new technologies as mere tools to achieve and lubricate power competition to balance world politics. As realists often assert military power

and warfare as the main elements for states to compete with each other, new technologies are viewed altering the techniques of warfare and the military affairs. However, the downsides of realism in explaining new technologies in International Relations lays upon the absence of recognition for non-state actors that are, in fact, emerging fast with a help from new technologies. (Deibert, 2002, pp. 30-31).

On the other hand, liberalism perceives new technologies as a tool that enables an increase in the flow of information. Consequently, this situation will reduce the possibility of misunderstanding among actors regarding identities or other matters that are sensitive trigger for conflicts. Moreover, increased flow of information across borders will generate greater interdependence which is the disincentive for states to go to war. States will more likely to settle their conflicts or solve their common problems through the international cooperation or institutions. Therefore, international peace will be eventually established. Liberalism simplifies the global communication structure by putting an ideal structure in which the actors are interacting positively between each other without really paying attention to the power and social relations among the actors. This also becomes the critics for liberalists (Deibert, 2002, pp. 31-33).

The critics would be answered by Marxism nonetheless. Marxism's fundamental tenet is about economic class and its relations with modes of production that will determine social and political class. Hence, in viewing new technologies, Marxism has a reductionist tendency of discerning economic control for the new technologies (i.e. telephone, Internet, radio, television). The given illustration by Deibert (2002; 35-37) states that who owns the technologies matter as they will utilize the technologies for their own benefits accordingly to the social class that have been determined by the mode of production they own.

Apart from what is being illustrated by Deibert, Daniel R. McCarthy also agreed on the fact that International Relations, as a discipline, has been absent in the technological advancement discourses despite the existing interrelationship between those two variables. He pointed out that many International Relations scholars tried to develop the holistic approach of International Relations in the era of technological development by taking on Science and Technology Studies (STS) (McCarthy, 2018, 1-2). McCarthy's argument on the combination of both STS and International Relations (STS-IR) has resulted in the understanding that all global politics is socio-technical that has dealt with empirical issues such as Internet governance, nuclear weapons, even mapping technologies (McCarthy, 2018, 13-14).

Moreover, one of the tenets in STS is significantly relevant to International Relations such what Bueger and Stockbruegger viewed about Actor-Network Theory (ANT). ANT positions technology as an equal object to human (Bueger and Stockbruegger, 2018, 42-43). It also invites non-diplomat and non-government actors—specifically addressing scientists, to take role on the deals about international relations such as the issues on environment and critical security (Bueger, Stockbruegger, 53-55). Hence, with technology, International Relations has evolved into a broader arena with

high complexity of actor-networks.

International Relations theories and their relevance with technological disruption era are still emerging and need for more exploration. In fact, the study of technology in IR has not been particularly addressed but being embedded to other study—STS. However, the world gradually becomes a place for technologies that are getting more developed as the time passes. As of today, Internet and cyberspace have been the predominant technologies which disrupts the conduct of traditional international relations. While the illustration of the disruptions will be given in the next sub-section, it is great to note that the theoretical explanation will always be following and not predicting due to the rapid advancement of technologies.

The Disrupted International Affairs: the Concept of Cyberspace and Its Implications

National government has utilized technologies in doing their jobs. For example, technologies to increase public services such as found in Indonesian Ministry of Foreign Affairs which has utilized digital command centre to increase its efficiency in boosting up digital diplomacy (Pernyataan Pers Tahunan Menteri Luar Negeri RI Tahun 2017, 2017). They also start building up command centre that connects them with public to expedite the efforts of digital diplomacies (Kemlu_RI, 2017). Additionally, the local government of Seoul, South Korea, is having big screen showing real-time situation across Seoul City put on the mayor's office. This enables the mayor to view statistical data on fires, emergencies, even complaints from the citizens (Government, 2017). The incorporation of technology within the scope of government and politics are commonly found in other pledged world's top e-governances such as New Zealand, Japan, UK, Australia, Canada, USA, and Netherlands (Dunleavy, Margetts, Bastow, & Tinkler, 2007).

Looking at the rapid growth of technological usage within government and politics, this led to information of citizens, relevant data, and the national's secret documents being integrated and stored to an online cloud in which the information being kept within such technology becomes the jurisdiction of a national government or typically referred as cyberspace (Winterfeld & Andress, 2013). Thus, there should be high protection over this data especially by taking note on the fact that the compromised data due to the technology misplacement are relevant to the national security and sovereignty. The loss of the data to other country may cause future disruptions in international relations (e.g. cyber warfare). In the context of international relations and global security, such technological disruptions have emerged during these past years.

Technically speaking, cyber-attack is known as a harmful endeavour made by an individual or an organization to hack the information system of other individual or organization for their own benefits (Cisco, n.d.). This form of attack apparently makes use of cyber weapon such as malware, viruses, spam, worms, etc. With those means, the attacker intends to exploit the confidentiality, integrity, and availability of the host by cracking passwords, compromising applications, or exploiting vulnerabilities that the host possesses. For the government's position, the attacker targets their military, commerce, laws,

critical infrastructures, and emergency services. Although the attackers are mostly individuals or from small organizations, when it comes to attack governments, there are several cases where those attackers were indicated to be endorsed by the government of other countries. This situation is usually described with the term 'Advanced Persistent Threat' (APT) (Winterfeld & Andress, 2013).

A cyber-attack has exacerbated the relationship between North Korea and US. It was in 2014 that a movie with fictional plot of plan to kill North Korean leader, Kim Jong-un, was set to release under Sony Pictures. The release was cancelled due to plot controversy. However, Sony had to eventually face the consequence, receiving cyber-attacks where hackers breached their system, causing the system to go down. This attack included threat to cancel the release of the movie and for some parts to be edited as accordingly to the message being left during the cyber-attack. Not only that, this incident has caused stealing of confidential information including e-mail passwords of the customers and employees. Later did they found that this cyber threat was signalled to be sponsored by the North Korean government (Feckler, Barnes, & Sanger, 2014). In another situation, recently, European Union found out that their diplomatic cable has been intercepted for three years. Diplomatic cable is a platform for diplomats to communicate, including exchange in confidential information. European Union is suspicious towards China behind this significant attack (European Union diplomatic communications 'targeted by hackers', 2018).

As the time passes, cases in relations to cyber-attacks have increased in numbers and frequencies. A report made by WEF on Global Risk showed that cyber-attack is the fifth most likely risk that will affect a country in 2019 (The Global Risks Report 2019, 2019, p. 5). In scoping cyber-attacks as a risk, the respondents of the report believed that cyber-attacks will lead to several problems such as: 1) data and money theft, 2) operational disruption, 3) fake news, and 4) loss of privacy (The Global Risks Report 2019, 2019, p. 16).

On another level, cyber warfare is also a form of technological disruption, but a more serious one. It is more serious because it is related to wars. What distinguishes cyber warfare from cyber-attacks is, according to Adam Segal, that cyber warfare cause death and infrastructure destruction and threatens national interest. If not, then it will be classified as mere cyber-attack (Beauchamp, 2014).

However, the definition of cyber warfare is still debatable due to the absence of authority addressing the issue of cyber security, cyber-attack, and cyber warfare. Hence there is no tangible definition yet or clear restriction on what can be classified as warfare or attack. Nevertheless, in the attempt to define cyber warfare, some scholars try to trace the definition of traditional war. For Winterfeld and Andress, they follow the definition compiled in 'On War,' documents on tactics being used in Napoleonic War in 1873, "…War is nothing but a duel on an extensive scale… Each strives by physical force to compel to the other to submit to his will… War therefore is an act of violence to compel our opponent to fulfil our will." (Winterfeld & Andress, 2013) From this definition, it can be interpreted that cyber warfare should be conducted massively. However, the On War's

definition is not relevant with cyber warfare because cyber warfare is perceived for having no physical force to involve with.

In addition, in his writing, Abebe tried to link cyber warfare with the definition of war provided in international law particularly UN Charter. In article 2(4) and 51, it said that war is force against another state and the self-defence as the retaliation. Abebe interpreted this definition as cyber war could be used as force measure to maintain international peace. Moreover, he also inclined to the US' position on cyber warfare as stated by Adam Segel previously (Abebe, 2016).

Nonetheless, Winterfeld, Andress, and Abebe in their respective studies recognized the absence of definition and regulations on cyber warfare. Associating cyber warfare and traditional warfare as stated in established laws are viewed incongruous because cyberspace is more complex. It cannot necessarily be justified, which one is the weapon or to some extent impact should be hazardous in order to be classified as physically, politically threatening the national security as traditional warfare is. Thus, up until now, there is no case of cyber-attacks that levelled up and pledged as cyber warfare, especially by looking at the cases being discussed above.

As opposed to the previous argument is the fact that cyber warfare could be translated to the usage of technologies to create physical damage indirectly. The attack might not necessarily cause casualties (Singer & Friedman, 2014). For example, how Stuxnet weakened security system of four Iranian nuclear facilities back in 2010 by attacking the centrifuges—a part of a machine that rotates constantly. Stuxnet is a malware that is specifically designed to weaken industrial machines. In Iranian context, centrifuges were controlled by a software named SCADA which is attached by Programmable Logic Controllers (PLC), a hardware that directly controls the centrifuges. Stuxnet attacked the centrifuges by intercepting the program commanded by SCADA to the PLC. Hence, it caused physical damage which was the die down of centrifuges. There was no further exposure on who or which country that inserted Stuxnet to the said Iranian nuclear facilities. Iranian government only confirmed that there were several spies that did the deed (Shakarian, Shakarian, & Ruef, 2013, pp. 224-239). This particular illustration demonstrates that cyber-attacks have entered the Global South as well, not necessarily the North only in which technologies mainly come from.

This potential can also be read from the trend of Artificial Intelligence (AI) development which facilitates activities such as processing a large volume of data quickly and mimic behaviour of people (Shuja, 2019). AI is often being used in machines to detect algorithm, biometric, etc. It is also possible for AI being used as weaponry. The design for autonomous weapon such as killer robots lets the machine select and engage the targets with insignificant human controls. Fully autonomous weapon will be dangerous as it might cause catastrophe with accidents such as killing the wrong targets and at the same time violate rule of war (Human Rights Watch, n.d.). The utilization of autonomous weapon will be the traditional war as commonly known, but with a more sophisticated technology. Thus, anticipating cyber warfare as a form of technological disruption in international affairs

is essential and steps to prevent or resist the threats should be formulated.

The Needs for Cyber Diplomacy

Cyber Diplomacy: Cooperation on Cyberspace

The dawn of cyber-attacks has risen and cyber warfare is haunting the global security. However, there is no framework or authority regulating cyberspace which is now perceived as the jurisdiction of country. The absence of such urgent instruments has caused confusions and ineffectiveness to combat such technological disruptions, specifically in international relations. Some cases have been hung without resolution, because there is no international law regulating this matter, yet (Lacy & Prince, 2018). The emergence of cyber diplomacy begins with the understanding that cyberspace is like air, water, and land to countries. Countries have jurisdiction over the mentioned space. It is a territory, thus regulations and establishment of international norms and values regarding it should be started. However, cyberspace is a little bit distinctive. Despite the fact that the government possesses some portions of the space, cyberspace comprises of many technology companies (e.g. Facebook, Twitter, Google as storage cloud, etc.) in which they have the say in it. Approach through policy enforcement might not be effective but this is currently the best attempt to the cyber protection. Thus, the needs of international cooperation increase and only through cyber diplomacy that such matters can be taken care of (Barrinha & Renard, 2017).

Because the cases involved several countries, therefore talks and discussion need to take place to solve them. It is also important to cooperate to anticipate future cyber-attacks and cyber warfare. Cyber diplomacy may be the alternative to create such cooperation in combating and preventing cyber-threats. Cyber diplomacy is known as using diplomatic resources to maintain national interest regarding cyberspace (Riordan, 2016). Nonetheless, there is misconception of cyber diplomacy when it is come face-to-face with e-diplomacy or digital diplomacy. To date, digital diplomacy/ e-diplomacy is different from cyber diplomacy because digital diplomacy/e-diplomacy is the use of technology tools to conduct traditional diplomatic activities (Riordan, 2016).

Diplomats' roles are needed to involve in the matter because firstly, it requires a transnational communication as a cyber-threat may have spill-over effects to other states thus international cooperation should be encouraged. Secondly, diplomat will be helpful in mainstreaming the idea of cyber security and cyber threats to existing international agenda such as through human rights aspect, development policy, trade, intellectual property rights. Thirdly, a diplomat that knows how new technologies work will be of help in disseminating the issues of cyber security and cyber threats in national government, as well as the society (Tiirmaa-Klaar, 2013, pp. 509-510). However, as the nature of technologies are commonly owned by private, hence an effective cyber diplomacy should be inclusive for private actors too such as individuals, experts, and technocrats, creating a public-private partnership. The function of cyber diplomat will be similar to diplomat in nuclear era. Although nuclear weapon was famous for being used for mutually assured destruction, no

nuclear expert represented a particular country in regards to nuclear diplomacy. The same should apply to the current situation with cyber threat going around. Private actors should not become the ones to drive cyber diplomacy, but the diplomats themselves (Tiirmaa-Klaar, 2013, p. 513).

The Rise of Cyber Diplomacy and Its Dynamics in Indonesia

The history of cyber diplomacy has started ever since 2009 when a Cyber Security Workshop was conducted in Vienna following Estonia's leadership in Organisation for Security and Co-operation in Europe (OSCE) Forum for Security Cooperation. In the workshop, heads of national cyber agencies from different countries acted as diplomats to understand what cyber security really is. It was followed with several meetings throughout 2009-2010 to discuss about behaviour and norms in cyberspace and increase states capacity to fight against cyber-attacks (Tiirmaa-Klaar, 2013, p. 519).

In 2010, USA encouraged the conference to formulate a Confidence-Building Measure (CBM) on cyber security (Tiirmaa-Klaar, 2013, p. 519). CBM is a tool for parties to build trust with each other to achieve the willingness to exchange information with adversary—it is a part of preventive diplomacy (Harman, 2016). At the same time with OSCE development, discussion about cyber security has started in the UN. In 2009, UN resolution on ICT in the context of international security was released. The resolution stressed the importance for states to enhance cyber talks and dialogues, as well as creating UN Group of Governmental Expert (GGE) of which its main task is to raising states' awareness on cyber security.

One year after that, such GGE was established. They published a report which stated that International Humanitarian Law applies in cyberspace in terms of attacks and warfare. At Seoul Conference in 2012, cyber capacity building was the agenda for states in the effort of mitigating cyber threats. Cyber capacity building in this context is limited to equalise the capacity of all countries for their cyber securities. Often known is that developing countries tend to be less prepared than developed countries. Hence, one of the strategies to diminish such inequality is by creating national Computer Emergency Response Team (CERT) which enables developing nations to enhance their cyber capacities consisting of trainings, transfer of technologies, and best-practices sharing with the CERT networks (Tiirmaa-Klaar, 2013, pp. 520-523).

In Indonesia's case, as a matter of fact, internet penetration has increased by 10% in 2018 with around 171 million people have access to the internet (Indonesia has 171 million internet users: Study, 2019). The data implies that Indonesia's society has deep interdependence with the internet, thus problems related to the internet and cyberspace most likely to arise. Therefore, cyber security becomes a new agenda that should be prioritised in response to the development.

The precedence in Indonesia showcased the increase in fake news, as well as utilisation of disinformation for political purposes that even threatens national security (Paterson, 2019). (In Facing CBRNE and Cyber Threats, Indonesia - US Intensify Military Cooperation, 2020)

The example of censorship in Indonesia has happened recently by the government action to take down several social media platforms as a response to the hoax and disinformation following 2019 Presidential election. Instagram, WhatsApp, Facebook, and Twitter were down for several hours (Indonesia blocks social media as election protests escalate, 2019). This proves that Indonesia has been lacking of any other options apart from censorship. In international arena, especially in conducting cyber diplomacy, Indonesia will be in a difficult position for this country will be seen as disrespecting the nature of the Internet because the restrictions on social media platforms back in May 2019 has impacted not only the spreader of hoax, but also all of the civilians. However, being involved in cyber diplomacy forums will certainly benefit Indonesia in the sense that Indonesia will gain transfer technology of tools used to enhance cyber security. Such forums will also be benefitting Indonesia in terms of the exchange of information that will increase capability of stakeholders of cyber security in Indonesia as individuals (e.g. managerial skills of the Internet, updated information in regards of cyber security).

For Indonesia's case, cyber diplomacy has been conducted by the establishment of its CERT in 1998. As explained above, CERT is a community which has linked to CERTs in every other country. Indonesia establishing CERT was considered early in Asia, because the development of CERT in Asia was started around that time too. Unlike CERT in South Korea, Japan, and Australia, Indonesia's CERT is a community-built instead of government-endorsed. Indonesian CERT was initiated by an individual who is also an expert in internet security, Dr. Budi Rahardjo, and is currently by professionals and volunteers for its operations (Pitoyo, 2013).

Indonesian government has attempted to provide an ecosystem that will be suitable for the development of cyber security by establishing a body specifically addresses the issues on cyber and information security in 2017, which is the National Cyber and Crypto Agency (Tentang BSSN, n.d.). Through Presidential Regulation of the Republic of Indonesia Number 133 year 2017 (Sejarah Pembentukan BSSN, n.d.). This particular agency will act as a think tank, as well as the one who promulgates strategies against cyber threats and cybercrimes.

Apart from that, Indonesia has secured a cooperation with South Korea in capacity building to increase research and skills on cybercrimes investigation. This agreement involved Korea International Cooperation Agency (KOICA), Indonesian Police, and Institute of Technology Bandung in it. The agreement has taken into effect in 2018 and will end in 2021 (Memorandum of Understanding among the Indonesian National Police and the Korea International Cooperation Agency and the Bandung Institute of Technology on Cybercrime Investigation Capacity Building).

Conclusion

To conclude, technology advancement has brought about positive impacts to humankinds, yet it also brought along its downsides. The disadvantages can be found in the forms of technological disruptions. Technological disruptions have also impacted politics, government, even international

relations. Technological disruptions in international relations prominently matter to discuss about, reminiscing that cyber-attacks and future inevitable cyber warfare are threatening national security.

There are several cases of cyber threats against international harmony such as happened in Iran in 2009 that targeted centrifuges of their nuclear-making machines, the attacks to Sony Pictures as retaliation of their controversial movie on North Korean leader, as well as interception in diplomatic cable of European Union. However, although cyber-attacks affected different countries, these technological disruptions were left unsolved because of the lack of international instruments and frameworks addressing the issues.

On that account, there should be cooperation between countries to enforce stability on global cyber security. It may start with state-to-state discussion attempting for capacity building or technicalities on preventing cyber-attacks. For instance, the initiative between Indonesian National Armed Force with the US Government to increase cooperation on cyber security training (In Facing CBRNE and Cyber Threats, Indonesia - US Intensify Military Cooperation, 2020). However, to note that every country has different technology capacity and complexity hence established framework should be in line with the distinctive features of each country. To bridge the differences, thus cyber diplomacy is needed to communicate between states. Good cyber diplomacy is measured by how government can work together on cooperation in fighting against cyber threats—which are transnational, but still respecting the value of Internet which is for freedom of expression.

For Indonesia's case, cyber threats are still in the subject of information and communications governance. The cases of hoax and disinformation are commonly found, probably because of the lateness in technology advancement compared to other North countries in which technologies are mostly coming from. Indonesia has been receiving generous amount of cyberattacks. However, several attempts done to respond to the problems have been authoritarian such as social media platforms limitation and censorship. This will reduce Indonesia's bargaining position in the cyber diplomacy forums. But, the needs to do cyber diplomacy is still there. Because only through cyber diplomacy Indonesia will be able to gain transfer technology, exchange of information, and capacity building. As of now, Indonesian government has maintained a cooperation with South Korea to increase the capability in investigation of cybercrimes. Yet, there is still a long way to go in order to satisfy Indonesia's needs. Particularly by understanding the nature of cyber space where many communities are involved. Thus, multi-stakeholder and multi-disciplinary approaches are highly encouraged to handle cyber-related issues.

References

Books

Barston, R. P. (2014). Modern Diplomacy. New York: Routledge.

Bueger, C. and Stockbruegger, J. (2018). Actor-Network Theory: Objects and actants, networks and narratives. In Daniel R. McCarthy (Eds.), Technology and World Politics: An

Introduction (pp. 42-59).

Deibert, R. J. (2002). Hyper-Realities of World Politics: Theorizing the Communication Revolutions. In E. H. Potter, Cyber-Diplomacy: Managing Foreign Policy in the Twenty-first Century (pp. 27-47). Canada: McGill-Queen's University Press.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2007). Digital era governance: IT corporations, the state, and e-government. New York: Oxford University Press.

McCarthy, Daniel R. (2018). Introduction: Technology in world politics. In Daniel R. McCarthy (Eds.), Technology and World Politics: An Introduction (pp. 1-22).

Shakarian, P., Shakarian, J., & Ruef, A. (2013). Introduction to Cyber-Warfare: A Multidisciplinary Approach. Massachusetts: Elsevier.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.

Tiirmaa-Klaar, H. (2013). Cyber Diplomacy: Agenda, Challenges and Mission. In K. Ziolkowski, Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (pp. 509-529). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Winterfeld, S., & Andress, J. (2013). The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. New York: Syngress.

Journal Articles

Abebe, D. (2016). Cyberwar, International Politics, and Institutional Design. The University of Chicago Law Review, 1-22.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 353-364.

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. Global Discourse, 1-16.

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

Online sources

Beauchamp, Z. (2014, December 19). The Sony hack isn't cyberwar — and the US can't really punish North Korea for it. Retrieved from Vox: https://www.vox.com/2014/12/19/7417363/sony-hack-cyberwar

Cisco. (n.d.). What Are the Most Common Cyber Attacks? Retrieved from Cisco: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

DAKA Advisory. (2013). Meeting the cyber security challenge in Indonesia: An analysis of threats and responses. Retrieved from https://dokumen.tips/documents/meeting-the-cyber-security-challenge-in-indonesia.

html

European Union diplomatic communications 'targeted by hackers'. (2018, December 19). Retrieved from BBC News: https://www.bbc.com/news/world-europe-46615580?intlink_from_url=https://www.bbc.com/news/topics/cp3mvpdp1r2t/cyber-attacks&link_location=live-reporting-story

Feckler, M., Barnes, B., & Sanger, D. E. (2014, December 14). Sony's International Incident: Making Kim Jong-un's Head Explode. Retrieved from The New York Times: https://www.nytimes.com/2014/12/15/world/sonys-international-incident-making-kims-head-explode.html

Government, S. M. (2017, June 21). Seoul City Operates the First Digital Civic Mayor's Office. Retrieved from Seoul Metropolitan Government: http://english.seoul.go.kr/seoul-city-operates-first-digital-civic-mayors-office/?cat=29

Harman, S. (2016, May 17). Confidence-building measure. Retrieved from Enyclopædia Britannica: https://www.britannica.com/topic/confidence-building-measure

Human Rights Watch. (n.d.). Retrieved from Killer Robots: https://www.hrw.org/topic/arms/killer-robots

Indonesia blocks social media as election protests escalate. (2019, May 22). Retrieved from Netblocks: https://netblocks.org/reports/indonesia-blocks-social-media-as-election-protests-escalate-XADE7LBg

Indonesia has 171 million internet users: Study. (2019, May 19). Retrieved from The Jakarta Post: https://www.thejakartapost.com/life/2019/05/18/indonesia-has-171-million-internet-users-study.html

In Facing CBRNE and Cyber Threats, Indonesia – US Intensify Military Cooperation. (2020, December 7). Retrieved from Indonesian Military: http://int.tni.mil.id/berita/317-in-facing-cbrne-and-cyber-threats-indonesia-us-intensify-military-cooperation.html

Kemlu_RI. (2017). Retrieved from Twitter: https://twitter.com/kemlu_ri/status/818777285629095936?lang=en

Memorandum of Understanding among the Indonesian National Police and the Korea International Cooperation Agency and the Bandung Institute of Technology on Cybercrime Investigation Capacity Building. (n.d.). Retrieved from MINISTRY OF FOREIGN AFFAIRS OF THE REPUBLIC OF INDONESIA DIRECTORATE GENERAL OF LEGAL AFFAIRS AND INTERNATIONAL TREATIES TREATY ROOM LIST OF TREATIES CONCLUDED BY INDONESIA: https://treaty.kemlu.go.id/apisearch/pdf?filename=KOR-2018-0173.pdf

Natalia, M. (2019, April 26). Proteksi

Ekonomi Digital, Serangan Cyber di Indonesia Capai 232,4 Juta Kali. Retrieved from Sindonews.com: https://ekbis.sindonews.com/read/1399048/178/proteksi-ekonomi-digital-serangan-cyber-di-indonesia-capai-2324-juta-kali-1556251619

Nugraha, R. M. (2019, February 8). 2019 Presidential Election Shrouded by Cyber Attack Threats. Retrieved from Tempo.co: https://en.tempo.co/read/1173517/2019-presidential-election-shrouded-by-cyber-attack-threats

Peraturan Menteri Komunikasi dan Informatika Nomor 27/PER/M.KOMINFO/9/2006 tanggal 20 September 2006. (n.d.). Retrieved from Jaringan Dokumentasi dan Informasi Hukum Kementerian Komunikasi dan Informatika Republik Indonesia: https://jdih.kominfo.go.id/produk_hukum/ view/id /445/t/peraturan+menteri+komunikasi+dan+informatika+nomor +27perm kominfo92006+tanggal+20+september+2006

Pernyataan Pers Tahunan Menteri Luar Negeri Tahun 2017. (2017, 10 January). Retrieved from Kementerian Luar Negeri Republik Indonesia: https://kemlu.go.id/portal/id/read/757/pidato/pernyataan-pers-tahunan-menteri-luar-negeri-ri-tahun-2017

Pitoyo, A. (2013, 25 July). Peranan ID-CERT di Asia Pasifik diakui APCERT. Retrived from Merdeka.com: https://www.merdeka.com/teknologi/peranan-id-cert-di-asia-pasifik-diakui-apcert.html

Riordan, S. (2016, May 12). CYBER DIPLOMACY VS. DIGITAL DIPLOMACY: A TERMINOLOGICAL DISTINCTION. Retrieved from USC Center on Public Diplomacy: https://www.uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

Schwab, K. (2016, January 14). The Fourth Industrial Revolution: what it means, how to respond. Retrieved from World Economic Forum: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Sejarah Pembentukan BSSN. (n.d.). Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/sejarah-pembentukan-bssn/

Shuja, F. (2019, September 11). The Digital Battleground of Cyberwarfare. Retrieved from CPO Magazine: https://www.cpomagazine.com/cyber-security/the-digital-battleground-of-cyberwarfare/

Situs KPU Kerap Diretas Lewat 'IP Address' Rusia dan China. (2019, March 13). Retrieved from CNN Indonesia: https://www.cnnindonesia.com/nasional/20190313180046-32-37 69 376980/situs-kpu-kerap-diretas-

lewat-ip-address-rusia-dan-china

Tentang BSSN. (n.d.). Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/tentang/

The Global Risks Report 2019. (2019, January 15). Retrieved from World Economic Forum: https://www.weforum.org/reports/the-global-risks-report-2019