Jambe Law Journal
ISSN 2598-795X (online); 2598-7925 (print)
Vol. 4 No. 2 (2021): 131-150, DOI: 10.22437/jlj.4.2.131-150

Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with It

Maskun, Irwansyah,** Ahsan Yunus,*** Armelia Safira,**** Siti Nurhalima Lubis******

Faculty of Law, Universitas Hasanuddin, Makassar - Indonesia
**maskunmaskun31@gmail.com*
***irwansyah@unhas.ac.id*
****ahsanyunus@unhas.ac.id*
*****maskunmaskun31@gmail.com*
******maskunmaskun31@gmail.com*

Abstract

The development of technology brings changes in human life, and the shift of most human activities to cyberspace is now a challenge for every country in the world. Cyber-attacks are crimes that have developed rapidly with the development of information communication and technology (ICT). Due to its impact, cyber-attacks can be considered as a crime called a crime of aggression. The focus of this paper is to determine the urgency of regulating cyberattacks as a crime of aggression and to find out the extent to which the international community has made cybercrime the focus of contemporary crime research, which is referred to as a crime of aggression. This paper shows that international cooperation is needed to create an international regime that is respected and universally accepted by the international community in relation to cyber-attacks, which can also be referred to as crimes of aggression. It is because cyber-attacks in its nature are transnational crimes and need a cooperation such as the framework of ASEAN to deal with.

Keywords: ASEAN Cooperation; Aggression Crime; Cyber Attack; International Law

A. Introduction

The development of this era has its implications on every aspect of human life. The advance in technology and information has brought humanity to a new standard of living: the standard of living of modernization. The advance has also implied in the resilience of a state. Currently, information and technology are a media to interfere the state security and state defense. Most of the crimes that uses technology relies on computers and the internet, so this kind of crime generally happens in cyberspace. The term of cyberspace appeared for the first time in 1984, used by William Gibson.[1] William Gibson describes his understanding on the internet, resulting in a stable landscape, having a resident easily navigate, and having the exact size or even more significant.[2] In cyberspace, the users can communicate under anonymity, without limitation by the borderline and even the scope of trans-country.[3]

One of the crimes that always happen in cyberspaces is cybercrime. The perpetrators of the cybercrime do not only target the government object or critical national infrastructures, but also has endanger the state security and have a potential of cyber warfare, a form of threat that is very vulnerable to national security defense.[4] The impact can be experienced from a cyber-attack such as the destruction of state facilities, a functional disruption, a remote system control, information abuse, a riot, fright, violence, chaos, and a conflict that has the potential of cyber warfare.[5] Therefore, this needs

1 Cyberspace is a term first used by William Gibson in his novel Neuromancer, London, Voyager/Harper-Collin, 1995.

2 Andrew D. Murray, *The Regulation of Cyberspace, Control in the Online Environment*, New York: Routledge-Cavendish, 2007, p. 5.

3 Kornelia Trytko, *The Politic of Anonymity: Poland's Media Discourse on Anonymous Communication Online*, Thesis, United Kingdom: Nottingham Trent University, 2016, p. 26.

4 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan. William Perdue, and Julia Spiegel, "The Law of Cyber -Attack", *California Law Review*, Vol. 100, Num. 4, 2012, p. 818.

5 Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton, "A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate", *Journal of Cyber-*

to be noticed by the international community as a crime that is indicated as aggression crime.

The importance of awareness of cyber problems as a crime can be indicated as aggression crime and can be harmful to the security of a state. Thus, to deal with this issue, international cooperation should be initiated by one region such as ASEAN to anticipate and overcome this kind of crime. As it might be understood, a cyber-attack with an indication of aggression crime has characteristics to be not limited by region.

Due to the nature of cyber-crime is anonymous and borderless, which has caused cyber-crimes, especially cyber-attacks, it becomes a new topic and issue in legal studies. Besides, there is a fact showing that there is no understanding between countries in an international agreement regarding the standard norms of cyber-attacks. In addition, in relation to the crime of aggression, the standardization of cyber-attacks will be increasingly important because the crime of aggression does not yet have the same standard in the practice of countries regarding the crime of aggression. The development of information, communication and technology is a certainty; it is crucial to settle a cyber-attack standardization that is universally applicable, at least within ASEAN countries. This article, therefore, will be a reference in formulating definition and regulation of cyber-attacks that are acceptable in countries, including ASEAN.

This article addresses two problems; is cyber-attack regulation can be associated as a crime of aggression? To what extent the international community, such as ASEAN, can cooperate on dealing with cyber-attacks? To support the statement on these problems, several studies conducted by several experts have demonstrated the urgency of regulation and the urgency of cyber-attacks, such as the one conducted by Hathaway, et.al,[6] whose research results say that regulations of cyber-attacks should begin by clarifying what is meant by cyber-attacks and how cyber-attacks are regulated in various laws

security, Vol. 0, Num. 0, 2018, p. 3.

6 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan. William Perdue, and Julia Spiegel, *op. cit.,* p. 818.

such as the law of war, international treaties and the national criminal law of each country. Another study was conducted by Moynihan, whose research results say that the majority of cyberattacks between countries consist of persistent low-level intrusions that occur below the threshold for the use of force international law in general, including the principle of non-interference in the internal affairs of other countries and the principle of sovereignty, can be applied to these cyber operations.[7] The research results conducted by Hathaway and Moynihan showed a positive correlation with the object of study in this article which is to establish international norms regarding cyberattacks and what countries should do to deal with them.

B. Cyber Attack and Its Regulation

1. Defining Cyber-Attack

Cyber-attack is every form of act, expression, thought either done intentionally or unintentionally by every party, with any motive and goal, it is committed in any location, targeting electronical systems or contents (information) as well as equipment that depend on technology and network in any scale, toward the vital object or non-vital in scope of military and non-military, threating the sovereignty of a country, territorial integrity and safety of a nation.[8] Cyber-attack happens when the intensity and scale of a cyber-attack increase and change from a potential threat to a factual one. A cyber-attack aims to enter, control, modify, steal, damage, destroy or disable a system or information asset.[9] There are several categories such as:

---

7 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Research Paper on International Law Programme, Chatham House: The Royal Institute of International Affairs, 2019, p. 3.

8 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan. William Perdue, and Julia Spiegel, *op. cit.,* pp. 822-823.

9 Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat To National Security And What To Do About It", in *Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan. William Perdue, and Julia Spiegel*, "The Law of Cyber -Attack", *California Law Review*, Vol. 100, Num. 4, 2011, p.

a. Cyberwar is every action that is committed intentionally and coordinated to interfere with the sovereignty of a state. Cyberwar could be in the form of cyber terrorism or cyber espionage that can interfere national securities. A cyberattack is large-scale active activity that are done intentionally.
b. Cyber violence is a passive cyberattack on a small scale, and it is done unintentionally.

Cyber-attack once happened in Estonia in 2007, and resulted in the disruption of public service and material loss. The attack allegedly carried out by Russia has deactivated the government network and trade belonging to Estonia's government. Around a million of government computers are infected by the *Distributed Denial of Service (DDoS) attacks.*[10] In 2010, Iran experienced a cyber-attack that attacking Iran nuclear facility in Natanz. It was approximately 60.000 computers at nuclear facility were infected by the virus called Stuxnet.[11] The target for uranium procurement infrastructure in Iran is very dangerous. It violates the sovereignty of Iran and the impact it causes is very dangerous for the safety of humanity.[12] A cyberattack could disable the nuclear centrifugal, air defence system, and electricity network. A cyber-attack is a severe threat to national security.[13]

Other cases happened in Iran in early 2020. The armed conflict between Iran and United States was triggered by the alleged cyber-attack that had occurred before. A new attack between two countries used Drone MQ Reaper 9. The United States Military operates a drone with the ability to run for 14 hours when fully charged with ammunition, various weapons, a solid visual sensor to hit the target,

10 Katherina C. Hinkle, "Countermeasures in the Cyber Context: One More Thing to Worry About", *YJIL Online*, Vol. 37, Num. 4, p. 13.
11 James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, Vol. 53, Num. 1, 2011, p. 23.
12 Maskun, et al., "Legal Standing of Cyber Crime in the Development of Contemporary International Law", *Legal Probs. (Masalah-Masalah Hukum*), Vol.42, Num. 3, 2013, pp. 511-9, https://ejournal.undip.ac.id/index.php/mmh/article/ view/13126/9949.
13 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan. William Perdue, and Julia Spiegel, *op. cit.,* p. 882.

so it is very accurate and deadly.[14]

2. International and National Law on Cyber-Attack

a. International Law on Cyber-Attack

Until today, no special international legal instrument has regulated cyber-attacks as aggression crimes. The absence of this convention does not mean negating the international law norm on this issue in a modern world today. There are several norms generally that has been pushed by several groups or countries concerned about the development of cyber usage and its threat as aggression crime. Wibisono, cited by Iskandar, explain five norms of cyber that are encouraged to be an international law such as (a) Tallinn Manual by NATO; (b) Microsoft Norm Paper by Microsoft Corp.; (c) Code of Conduct by China, Russia, and other several groups on its axis; (d) U.S Government Policy by the United States; and (e) 11 Cyber Norm by United Nations Group of Governmental Expert of Information Security (UN GGE).[15] However, only four them are relevant to accommodate the development of international law in the scope of cyber, as follows:

a) Tallinn Manual

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations is an international organization, NATO, to push an international norm regarding cyberattack. The existence of this manual is judged as a move to regulate and ensure the security and stability of cyberspace in a peaceful state or in a certain incident that can trigger the use of violence or armed conflict. Tallinn manual has initially been established by the Cooperative Cyber Defense Center of Excellence (CCD COE) NATO in 2013. Then this manual was

14 Erwin Prima, "Bunuh Soleimani Drone MQ-9 Reaper AS Paling Ditakuti di Dunia (Tempo Online)" https://tekno.tempo.co/read/1294958/bunuh-soleimani-drone-mq-9-reaper-as-paling-ditakuti-di-dunia/full&view=ok, accessed on January 13, 2020, accessed August 20, 2020.

15 I. Hamonangan, and Z. Assegaff, "Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital". *Padjadjaran Journal of International Relations*, Vol. 1, Num. 4, 2020, pp. 342-363.

updated in 2017 with Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.[16]

b) Microsoft Norm Paper

In 2014, Microsoft Corporation, one of the giant technology companies in the United States, has pushed an International Cyber Security norm. It is not much different from other international norms. This norm focuses on the responsibility of a country to avoid or prevent a cyberattack that is launched from a territory. This cyber security norm is essential to reducing international conflict based on a cyber[17]

c) Code of Conduct

In 2011, Shanghai Cooperation Organization (SCO) which consist of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, has filed an international code of ethics for information security on the 66 United Nation General Assembly Session. In 2015, from General Assembly Resolution A/66/359 various comments and suggestions from many parties were considered to revise this code of ethics document.

This code of ethics is considered to identify the rights and responsibilities of a state in the information space, promote constructively and responsible behavior in dealing with a threat and challenge in cyberspace, and build a peaceful, safe, and open information environment that is established based on cooperation and to ensure the comprehensive usage of cyber and network for social development and community welfare, which does not conflict with the goal on ensuring the international peace and security.

There are 13 points of norms that are included in this code of ethics. Compliance with it is voluntary and open to all countries. The main idea of this code of ethics lies in the responsibility of a state on improving information security systems and systems in their territories. According to McK-

16 *Ibid.*
17 *Ibid.*

une, the norms on this code of ethics raises a severe concern about human rights.[18]It is inseparable from the code's emphasis on state and territorial sovereignty in the digital space above everything, which is dominated by intelligence, national security, and imperative for regime stability.[19]

d) United Nations Group of Governmental Expert on Information Security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE ICT's), one of the institution experts is formed by United Nations to answer the challenge on cyber world development. This group is formed based on the General Assembly Resolution 68/243 that encourage mutual understanding and to identify a potential threat on cyberspace, and possibility of mutual act to solve it, including norm, regulation, or responsibility principle of state behavior, and a step to build trust with the intention to strengthening international security in cyberspace.[20] In its report in 2015, GGE agreed and determined 11 norms that is voluntary and not binding. It is a responsible behavior of a state that aims to encourage an open, safe, stable, can be accessed, and peace ICT environment.

Those eleven norms namely: (1) Maintaining international peace and security in line with the United Nations objective; (2) Considering all relevant information, including

18 Sarah McKune, "An Analysis of the International Code of Conduct for Information Security", https://citizenlab.ca/2015/09/international-code-of-conduct/, accessed on September 28, 2015, accessed 5 September 2020.

19 United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security, UN Document A/69/723, 13 January 2015", https://www.un.org/disarmament/publications/library/69-ga-ga-sc/, accessed on January 2015, accessed September 27, 2021.

20 United Nations for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security", https://www.un.org/disarmament/ict-security/, accessed on December 2018, accessed January 10, 2021.

context, challenge, and consequences from ICT case incident; (3) Not using their territory for an activity that is prohibited internationally; (4) Considering the best way to overcome an ICT threat for criminal acts; (5) Ensuring the safe usage of ICT, respecting human rights, including the right to privacy and freedom of expression; (6) Avoiding taking action or supporting ICT activities that are contrary to its obligations under international law; (7) Taking appropriate action to protect their critical infrastructure from ICT threats; (8) Responding to request for assistance from other countries related to the protection of critical infrastructure from ICT threats; (9) Taking a reasonable step to ensure the safety of ICT products and preventing the spread of harmful ICT tools and techniques; (10) Promoting a report responsible for ICT vulnerabilities and sharing information on the best solution in limiting or eliminating potential ICT threats, and (11) prohibiting to support activities for damaging information systems from official emergency response teams of other countries. As well as avoiding the involvement of the official emergency response team of its country to be involved in a dangerous international activity.[21]

From these several norms, it is learnt that there is a common spirit to improve security in cyberspace and avoid the practice of using force in retaliating against the cyber-attack. Historically, the process of making these international law norms, firstly from the view of NATO with their Tallin Manual in 2013. They were then responded by Shanghai Cooperation Organization Group with their Code of Ethics in 2015. All of these norms were then accommodated with 11 norms that were filed by GGE ICT's in 2015. However, they did not

21 United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Document A/70/174, 22 Juli 2015". https://www.un.org/disarmament/ict-security/, accessed on September 27, 2021.

agree on the next meeting, so GGE ICT's to improve cyber security were quite hampered. Until the United Nations established a new GGE known as Open-Ended Working Group (OEWG) to continue the discussion during 2019-2020 and 2020-2021.[22]

b. National Law on Cyber-Attack

Several countries have made an institution or organization specifically to deal with cyber problems in their respective state defense. United States established United States Cyber Command (US CYBERCOM) under United States Strategic Command (US STRATCOM). North Atlantic Treaty Organization or NATO established NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) as a cybersecurity agency to increase NATO's cyber defense. Other countries in Asia and Australia also make this cyber problem a severe problem that will possibly affect the state defense. Through the Australian Signals Directorate of Australia Department of Defense, Australia established an institution called Cyber Security Operations Center (CSOC) responsible for detecting and preventing a cyber-crime threat toward the interest and the Australian government. [23]

China also formed a "Blue Army" force; this force protects China's defense from cyber-attack. This force has its home base in Guangzhou Military Area, in the south of China.[24] England also build their own cyber defense. The system called Cyber Security Operations Centre (CSOC) under the Government Communications Headquarters (GCHQ) England, in Cheltenham, around 160 Kilometers from northwest of London.[25]

---

22 *Ibid*.

23 Australia Signal Directorate, "History of Australia Signal Directorate", https://www.asd.gov.au/about/history, accessed on December 2020.

24 Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations", *China Leadership Monitor*, Num. 42, pp. 1-3, https://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf.

25 Optimists CSOC, "Cyber Security Operation Center: Foresee, monitor, detect and react", https://www.optimesys.com/cyber-security-operations-center, accessed on 22 December 2020

The President of the Republic of Indonesia has signed Presidential Decree (Perpres) No. 53 of 2017 concerning State Cyber and Code Agency (BSSN) on 19 May 2017,[26] and it is revised through Presidential Decree No. 133 of 2017. State Cyber and Code Agency is a non-ministerial government agency which is under and directly responsible to the President. In addition to State Cyber and Code Agency, Indonesia State Army (TNI) also has a role on establishing a cyber unit (Satsiber) of Indonesia State Army to carry out the activities and cyber operation in the environment of Indonesia State Army to support the primary duty of Indonesia State Army.

Indonesia has also experienced a "black-mirror" of cyberattacks. Several governments owned sites have been hacked. One of which was the General Election Commission (KPU) site from infopemilu.kpu.go.id that served information of temporary real count of regional election in 2018. Irresponsible and anonymous person has reported to have massively attacked the site. The same also happened on other government institution which is the site of Directorate General of Taxation (Ditjen Pajak), Ministry of Finance from pajak.go.id. The site was hacked on 10 June 2018 by a person who claimed as Anonymous Arabe. The cyberattack incident may take form such as the changing of the view of a page (deface). In 2020, the number of cyberattacks in Indonesia throughout the first semester of 2020 reached 149,78 million times. The number was increased five times compared to the same period last year, reaching 29,63 million times. The monitoring result of the National Cyber Security Operations Center shows that the COVID-19 pandemic that has hit the world has a significant impact on online activities and affects the number of traffic attacks that occur.

26 National Cyber and Crypto Agency, "Presidential Decree (Perpres) No. 53 of 2017 concerning on State Cyber and Code Agency (BSSN)", https://jdih.bssn.go.id/arsip-hukum/presidential-regulation-of-the-republic-of-indonesia-number-133-year-2017-concerning-amendment-to-presidential-regulation-number-53-year-2017-concerning-national-cyber-and-crypto-agency, accessed on December 16, 2017, accessed 23 December 2020.

Some legal basis of cyber-attack in Indonesia can be seen in some laws, as follows:

a) Article 30 Paragraph (1), (2), and (5) concerning on National Defense and Security the Constitution of Republic of Indonesia 1945;
b) The Law No. 3 of 2002 Concerning on National Defense;
c) The Law No. 34 of 2004 Concerning on Indonesia National Army;
d) The Law No. 11 of 2008 Concerning on Information and Electronic Transaction as amended to the Law No. 19 of 2016 Concerning Amendment of The Law No. 11 of 2008 Concerning on Information and Electronic Transaction;
e) The Law No. 13 of 2008 Concerning on Public Information Disclosure;
f) Regulation of the Minister of Defense No. 57 of 2014 Concerning on Strategic Guidelines for Non-Military Defense; and
g) Regulation of the Minister of Defense No. 82 of 2014 Concerning Cyber Defense Guidelines

C. ASEAN Regional Cooperation

ASEAN is an international organization and a regional organization in South East Asia, established on 8 August 1957. On its declaration in Bangkok, it is stated the aim and purposes of ASEAN is to accelerate the economic growth, social progress and cultural development in the region; and to promote regional peace and stability through abiding respect for justice and the rule of law in the relationship among countries in the region and adherence to the principles of the United Nations Charter. The interaction between ASEAN members is in the form of cooperation, which is to build a relationship between two states or more to reach an agreement. The cooperation between ASEAN members in the field of social and culture, politics and security, education.

The purpose of cooperation in the political and security field is to create safety, stability, and peace among ASEAN countries. Coop-

eration in the field of politics is a concern of ASEAN. Some of the concrete examples of cooperation on politic and security of ASEAN such as Treaty on Mutual Assistance in Criminal Matters (MLAT); ASEAN Convention on Counter-Terrorism (ACCT); Defense Ministers Meeting (ADDM) which aims to promote peace and stability of region through a cooperation dialog and a cooperation in field of defense and security; South China Sea resolution dispute; cooperation in eradicate transnational crime which includes the eradication of terrorism, drugs, money laundering, smuggling and trafficking of small arms and human beings, pirates, internet crimes, and international economy crimes; Cooperation in the field of law, migration, and consular affairs, as well as the inter-parliamentary institution.

Regionally, ASEAN has made various attempts to promote awareness and joint commitment in enhancing cybersecurity. These attempts can be identified from multiple cooperation documents, such as on ASEAN Leaders' Statement on Cybersecurity Cooperation on the 32nd ASEAN Summit in Singapore in 2018. Moreover, in Manila, ASEAN Declaration to Prevent and Combat Cybercrime was agreed in the year before. In 2016, at Brunei Darussalam, the ASEAN nation was aware of the importance of personal data protection through ASEAN Framework on Personal Data Protection. Then furthermore, in 2012, on the 19thASEAN Regional Forum (ARF) in Cambodia, the foreign affairs minister in ASEAN have agreed on increasing cooperation in guaranteeing cyber security through the ARF Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security.[27]

In 2017, ASEAN conducted a 2nd International Security Cyber Workshop Series that aimed to conserve and enrich cyber stability in the regional area of ASEAN. This workshop generally discussed the opportunity and challenge in the context of peace and security in cyberspace. There are four main topics that is discussed in this workshop such as (a) The 2017 GGE and Issues for International Agree-

27 Muhammad Aris Yunandar, *Laporan Utama Kerja Sama Keamanan Siber di ASEAN dalam Menyambut Industri 4.0, Masyarakat ASEAN*, Jakarta: Dirjen Kerjasama ASEAN, 2019, p. 12.

ment; (b) The sovereignty and global perspective on international law regarding cyberspace; (c) Regional perspective on norm and act of building trust; (d) the next step on international cooperation. Those topics explanation can be seen, as followings:[28]

a. The 2017 GGE and Issues for International Agreement

The failure to reach an agreement at the GGE's 2017 Council does not mean that the report and recommendation to the United Nations General Assembly that existed before must be ignored. The failure of GGE's in reaching agreement is due to the geopolitical environment after the success of GGE's in 2015, which established 11 norms in regulating information, communication, and technology. The expert on the forum considered it difficult to reach an agreement in terms of threat analysis, the binding strength of the agreement, and capacity building and mutual trust-building. The main reason they disagreed is to implement international law on ICT's and how the norms that are not binding can make a state responsible.

The eleven GGE's norms cannot prevent a conflict and is difficult to enforce those norms in state's practice. One of fundamental questions related to the GGE is the definition of the use of force in the context of cyber-attacks. In this case, the countries tend to take defensive action in responding to force usage in the cyber context because of misunderstanding to the definition of use of force.

The state needs another approach to create the various bilateral agreements, regional and international, to assist each country in increasing trust among them. An open multi-stakeholder approach is required to increase regional unity in advancing a multilateral process. The speakers on the forum also gave special attention to information asymmetry among the 25 of the members and those involved in its making. They need to be get involved and more active in various ICT's discussions related to international security issues.

28 UNIDIR, *Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in ASEAN*, Singapore: UNIDIR, 2017, pp. 1-14.

b. The sovereignty and global perspective on international law regarding cyberspace

In the context of sovereignty is focused on the urgency of the state participation in the broader area of the regional level to make a more expansive space for the involvement of countries internationally. In practice, International Humanitarian Law does not explicitly mention cyber-attacks. Still, the principle of International Humanitarian Law regulates Distinction, Proportionality, and Military Necessity and various arrangements related to hostility act of a state in a conflict that occurs in cyberspace.

The biggest challenging on cyber operation for the state is to ensure whether the cyber operation is still in line with the doctrine and international law. In this context, the usage of ICT's for military purposes has to be in line with the principle of state sovereignty. In practice, on several states with sophisticated cyber equipment doesn't place the principle of state sovereignty as something that must uphold within the norm and international law framework. Increasing each country's transparency and cyber capability is the initial stage in building trust and stability in cyberspace in international life.

Generally, the expert on this workshop also agrees that there is no legal vacuum on regulating malicious behavior in cyberspace. So, there is no urgency to make an international treaty or a new convention with regards to this problem. They also remind us not to apply a high standard of the norm in cyberspace than others. The main challenge for the international community is to limit the use of force and peace time activities such as what proxy has done, and organized cyberspace crime network.

In the global context, there are doubts related to one permanent institution specifically connected to ICT's. This is based on the fact that many countries are still in the early stages of developing their institutional and legal structure for the cross-border cyber issues. The current international geopolitical condition also has an impact on decreasing trust among countries which is the challenge in forming a permanent international institution

related to ICT's.

c. Regional perspective on norm and Confidence Building Measures (CBM's)

The condition of Asia Pacific region is very diverse and covers a different economic background. Of 55% of internet users all over the world, there are still real obstacles among states. More than half of the households in this region do not have internet access. Whilst, several states have done development to bridge this gap by increasing the connectivity of every citizen, an issue of cybersecurity has not a priority for those states and they ignored the cybersecurity issue.

The GGE's previous report has provided a map offering a high-level commitment of ASEAN countries that set up the expectation for responsible state behavior. Even with the high principle, existing asymmetry is in cyber technical expertise, legal and political and cyber capabilities are the limitation to increase trust among states.

d. Regional perspective and the next step on encouraging international cooperation

In 2017, at least 80 to 90 states have done a revision related to cybersecurity law. There are also 30 states actively investing in offensive cybersecurity development. There is a tendency to increase international involvement and cooperation among countries, especially in terms of using the cyber domain, which aims to build the resilience of cyber architecture, both in times of peace and during conflicts.

Pause on the GGE's stage also allow increasing participation of other countries by involving various Non-Governmental Organization (NGO), as it happened on the Tallinn Manual and Hague Process for broader participation. Even though it can be observerd that every state does not agree with the deal, it leads to international law and cyber spatial management discourses. At the end of the session, the audiences are asked to consider six potential formats with various characteristics to bring the international discussion forward with regional preference. Those six for-

mats are: (a) continued the government expert group (Another GGE's); (b) Limited Working Group; (c) Open Working Group; (d) Conference on Disarmament; (e) UN Disarmament Commission; (f) Conference of States.

In 2019 in Thailand, ASEAN Defense Ministers' Meeting Plus (ADMM-Plus) occurred to establish a Joint Statement by the ADMM-Plus Defense Ministers on Advancing Partnership for Sustainable Security. This joint statement is a positive step in developing an international legal norm in the scope of cyber. Indonesia was particularly active in making international law norms in the field of cyber on *an Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security* (OEWG ICT's). Indonesia is also one of the special members of the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (GGE ICT's) for period 2019-2021.[29] It would not impossible if Indonesia take significant action in determining the regulation on International Law regarding Cyber in the future.

D. Conclusion

Contemporary crime is developed along with globalization in the form of cyberattacks indicated with aggression crime which need special attention by the world community. Some regulations, either international or national laws, have been imposed in Tallinn Manual by NATO, Microsoft Norm Paper by Microsoft Corp., Code of Conduct by China, Russia, and other several groups on its axis, and 11 Cyber Norm by United Nations Group of Governmental Expert of Information Security (UN GGE). The ASEAN cooperation is one of the initiations to realize an international law that is universally respected and recognized by the international community related to cyberattack and its handling as a crime that can be indicated as an

29 Anonym, "Indonesia Suarakan Stabilitas Siber di PBB", https://kemlu.go.id/portal/id/read/1327/view/indonesia-suarakan-stabilitas-siber-di-pbb, accessed on May 23, 2020, accessed January 15, 2021.

aggression crime. Therefore, it is pivotal for the international community to determine a general definition and regulation of cyber-attacks to be applied by all states. It is also needed a great cooperation among states to handle cyberattacks if it takes place transnationally.

Bibliography

Books, Journals, Reports

A. Clarke, Richard and K. Knake, Robert, 2011, "Cyber War: The Next Threat To National Security And What To Do About It", in Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan. William Perdue, and Julia Spiegel, "The Law of Cyber -Attack", *California Law Review*, Vol. 100, Num. 4.

Agrafiotis, Ioannis, *et.al.*, 2018, "A Taxonomy of Cyber-harms: Defining the impacts of cyber-attacks and understanding how they Propagate", *Journal of Cybersecurity*, Vol. 0, Num. 0.

A. Hathaway, Oona, *et.al*, 2011, "The Law of Cyber -Attack", *California Law Review*, Vol. 100, Num. 4.

C. Hinkle, Katherina, "Countermeasures in the Cyber Context: One More Thing to Worry About", YJIL *Online,* Vol. 37, Num. 4.

D. Murray, Andrew, 2007, *The Regulation of Cyberspace, Control in the Online Environment*, New York: Routledge-Cavendish.

D. Swaine, Michael, "Chinese Views on Cybersecurity in Foreign Relations", *China Leadership Monitor*, Num. 42, pp. 1-3, *https://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf*.

I. Hamonangan, and Z. Assegaff, 2020, "Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital". *Padjadjaran Journal of International Relations*, Vol. 1, Num. 4.

Maskun, et al., 2013, "Legal Standing of Cyber Crime in the Development of Contemporary International Law", *legal probs. (Masalah-Masalah Hukum*), Vol. 42, Num. 3. https://ejournal.undip.ac.id/index.php/mmh/article/ view/13126/9949.

Moynihan, Harriet, 2019, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Research Paper on International Law Programme, Chatham House: The Royal In-

stitute of International Affairs.

P. Farwell, James and Rafal Rohozinski, 2011, "Stuxnet and the Future of Cyber War", *Survival*, Vol. 53, Num. 1.

Try to, Kornelia, 2016, *The Politic of Anonymity: Poland's Media Discourse on Anonymous Communication Online*, Thesis, United Kingdom: Nottingham Trent University.

UNIDIR, 2017, *Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in ASEAN*, Singapore: UNIDIR.

Yunandar, Muhammad Aris, 2019, *Laporan Utama Kerja Sama Keamanan Siber di ASEAN dalam Menyambut Industri 4.0, Masyarakat ASEAN*, Jakarta: Dirjen Kerjasama ASEAN.

Internet

Anonym, "Indonesia Suarakan Stabilitas Siber di PBB", https://kemlu.go.id/portal/id/read/1327/view/indonesia-suarakan-stabilitas-siber-di-pbb, accessed on May 23, 2020,

Australia Signal Directorate, "History of Australia Signal Directorate", https://www.asd.gov.au/about/history, accessed on December 2020.

Erwin Prima, "Bunuh Soleimani Drone MQ-9 Reaper AS Paling Ditakuti di Dunia (Tempo Online)" https://tekno.tempo.co/read/1294958/bunuh-soleimani-drone-mq-9-reaper-as-paling-ditakuti-di-dunia/full&view=ok, accessed on January 13, 2020,

National Cyber and Crypto Agency, "Presidential Decree (Perpres) No. 53 of 2017 concerning on State Cyber and Code Agency (BSSN)", https://jdih.bssn.go.id/arsip-hukum/presidential-regulation-of-the-republic-of-indonesia-number-133-year-2017--concerning-amendment-to-presidential-regulation-number-53-year-2017-concerning-national-cyber-and-crypto-agency, accessed 23 December 2020.

Optimists CSOC, "Cyber Security Operation Center: Foresee, monitor, detect and react", https://www.optimesys.com/cyber-security-operations-center, accessed on 22 December 2020

Sarah McKune, "An Analysis of the International Code of Conduct for Information Security", https://citizenlab.ca/2015/09/inter-

national-code-of-conduct/, accessed 5 September 2020.
United Nations for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security", https://www.un.org/disarmament/ict-security/, accessed January 10, 2021.