THE URGENCY OF INTERNATIONAL REGULATION REGARDING CYBER ATTACK WITH AN INDICATION OF AGGRESSION CRIME IN ASEAN

MASKUN[1], NASWAR[2], ACHMAD[3], HASBI ASSIDIQ[4], ARMELIA SAFIRA[4], SITI NURHALIMA LUBIS[4]
International Law Department [1],Constitutional Law Department[2] ,Civil Law Department[3], Assistant Researcher[4]
Universitas Hasanuddin, Makassar - Indonesia
maskunlawschool@yahoo.co.id / maskunmaskun31@gmail.com

Abstract *– The development of technology brings change to human life, the change of most human activity to cyber is a challenge for every country in the world today. Cyber-attack is one of a crime that developed rapidly along with the development of information, technology, and communication (ICT). Based on the impact, cyber-attack can be seen as a crime that is indicated as an aggression crime. The main focus of this research is to determine the urgency of cyber-attack regulation as a crime that is indicated as aggression, and to find out to what extent the international community has made cyber-crime as the focus of contemporary crime studies that are indicated as a crime of aggression. This type of research is a normative legal study with a qualitatively data analysis which contain the urgency of international regulation regarding on cyber attack with an indication of aggression crime. The conclusion of this research is that an international cooperation is needed in order to realize an international regulation that are respected and universally recognized by international community regarding on cyber attack and their handling as a crime that can be indicated as a crime of aggression. Because cyberattack are cross-border, the cooperation expected in this research is a regional based cooperation, such as cooperation in a scope of ASEAN*

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

Table of Contents

INTRODUCTION

The development on this era has its own implication on every aspect of human life. The advance in technology and information has bring humanity to the new standard of living that is the standard living of modernization. This advance is also implicated on the resilience of a state. Currently, the threat on a state security and defense have used information and technology as the media of crime. Most of crime that using technology are relying on computer and internet, so this kind of crime generally are happening in the cyberspace. The term of cyberspace, appeared for the first time on 1984, used by William Gibson. William Gibson describe his character moving on the internet, resulting a stable landscape, have a resident, easily to navigate, have the same size of a country or even bigger. In cyberspace, the user can communicate under anonymity (anonymous), without limitation by the borderline (borderless) and even trans-country (transnational).[1]

One of a crime that could be happened on cyberspace is cybercrime. The perpetrators of cybercrime are not only targeting the government object or the critical national infrastructure, but their attack also have an ability effectively to endanger the state security and have a potential of cyber warfare which is a form of threat that is very vulnerable to national defense. The impact that could be experienced from a cyber attack such as the destruction of state facilities, a functional disruption, a remotely system control, the information abuse, a riot, fright, violence, chaos, a conflict which have a potential of cyberwarfare. This need to be noticed by the international community as a crime that is indicated as aggression crime.

The importance of awareness about this cyber problem as a crime that indicated as aggression crime and could harmful to the security of a state, to encourage an initiation for made an international cooperation. Considering that a cyber attack with an indication of aggression crime has characteristics that are not limited by region, it is necessary for the awareness of ASEAN community to create a regional cooperation that is capable to anticipate and overcoming this kind of crime.

This research is divided into fiveparts, introduction on section I, section II about the problems that will be the question, section III about the research method. The result of this study will be explained on section IV then the conclusion will be explained on section V.

1. PROBLEMS

The fundamental problem on this article is the urgency of cyber attack regulation that are indicated as a crime of aggression? and to what extent the international community is able to create cyber-attack as the focus of contemporary crime study with indication of crime aggression?

2. RESEARCH METHOD

The type of method used in this research is normative legal study with qualitatively data analyzation that contain the urgency of international regulation related to cyber attack that is indicated as aggression crime.

3. DISCUSSION

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 done in any location, it is targeting electronical system or the content (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. Cyber attack happened when the intensity and scale of cyber attack is increased and changed from a potential threat into factual threat. A cyber attack is aiming to entering, control, modify, stealing or damaging, or destroying or disabling a system or information asset, that have several categories such as:

a. Cyber war, is every action that is done intentionally and coordinated in order to interfere a sovereignty of a state. Cyber war could be in form of cyber terrorism or cyber espionage that can interfere a national security. Cyberattack is a large-scale of active activities that is done intentionally.
b. Cyber violence, is a passive cyberattack on a small scale and it is done unintentionally.

Cyber attack that has been happened at Estonia on 2007, resulting the disruption on public service and material loss. The attack that allegedly carried out by Russia has deactivate the government network and trade that is belong to the government of Estonia. Around a million of government computer is infected by the Distributed OenialofServise (DDoS) attacks.[2] Other cases had happened at Iran in early 2020. The armed conflict between Iran and United State one of which was triggered by the alleged cyberattack that had occurred before. A new attack that using Drone MQ Reaper 9, a drone that is operated by the United State Military, with ability to running for 14 hours when fully charged with an ammunition, various weapons, a solid visual sensor to hit the target, so it is very accurate and deadly.[3]

In 2010 Iran also experienced a cyberattack that attacking Iran nuclear facility in Natanz, approximately 60.000 computers at nuclear facility are infected by the virus called Stuxnet.[4] The target for uranium procurement infrastructure in Iran is very dangerous, not only violate the sovereignty of Iran but also the impact it causes very dangerous for the safety of humanity.[5] Cyberattack could disabling the nuclear centrifugal, air defense system, and electricity network, a cyber attack is a serious thread for national security.[6]

Cyber Attack Prevention

The cyber-attack prevention using an approach that adapts to the source and form of the attack that is faced. The form of cyber-attack prevention can be in form of:

a. Cyber defense is an attempt to prevent a cyber attack that could resulting in a disruption to the normal administration of country. Cyber defense is prepared as an attempt to preventing a cyber-attack.
b. A legal handling. By coordinate with the related security force if the perpetrator of cybercrime is found.
c. Cyber counter-attack, is an attempt of counter-attack to the source of attack with the intention to giving a deterrent effect to the perpetrators of cyber-attack

The target of cyber crime according to the purpose and target also could be differentiated. Namely:

a. Individual, public, organization, specific organization, which is a cyber-crime.
b. Vital object, national critical infrastructure, which a physical infrastructure system that is important where if this system is not functional properly, it can be weaker the defense or the security and the country economy.
c. National interest, is every aspect that is related with the national goal, state symbol, a state politics and nation interest.

International Law Regulation

Until this day, there is no special international legal instrument that is regulating about a cyber attack that is indicated as aggression crime. The absence of this convention, doesn't mean negating the international law norm regarding this challenge on a modern world today. But generally, there are several norms that has been pushed by several group or country that have concern on the development of cyber usage and its threat as aggression crime. Wibisono as it is quoted from Iskandar explain five norms of cyber that is pushed to be an international law such as: (a) Talinn Manual by NATO; (b) Microsoft Norm Paper by Microsoft Corp.; (c) Code of Conduct by China, Russia, and other several groups on it axis; (d) U.S Government Policy by United States; and (e) 11 Cyber Norm by United Nations Group of Governmental Expert of Information Security (UN GGE). But only four of norm above that is relevant except Government Policy by United States. We are judging the four norms as they have accommodating the development of international law in a scope of cyber. These are the explanation:[7]

a) Tallin Manual

Tallin Manual 2.0 on the International Law Applicable to Cyber Operations, is a move of international organization in this case is NATO that pushing an international norm regarding with cyberattack. The existence of this manual is judged as a move to regulated and ensure the security and stability of cyberspace in a peaceful state, or in certain incident that can trigger the use of violence or armed conflict. Tallin manual was originally established by Cooperative Cyber Defense Center of Excellence (CCD COE) NATO on 2013. Then this manual is updated on 2017 with Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

b) Microsoft Norm Paper

On 2014, Microsoft Corporation is one of a giant technology company in United Stated, has pushed an International Cyber Security norm. It is not much different with other international norms. The focus of this norm is on the responsibility of a country to avoid or prevent a cyberattack that is launched from a territory. This cyber security norm is important to reducing international conflict that based on a cyber

c) Code of Conduct

On 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 comment and suggestion from many parties is considered then this code of ethics document is revised.

This code of ethics is considered aimed to identifying the rights and responsibilities of a state in the information space, promoting 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 on the basis of cooperation and to ensure the comprehensive usage of cyber and

network for social development and community welfare, which doesn't conflicting with the goal on ensuring the international peace and security.

There are 13 points of norms that is included in this code of ethics. Compliance with this code of ethics 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 system and system in their territories. According to McKune, the norms on this code of ethics raises a serious concern about human rights, this 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

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) which is one of an institution expert that 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. In its report in 2015, GGE agreed and determining 11 norms that is voluntary, not binding, is a responsible behavior of a state that aimed to encourage an open, safe, stable, can be accessed, and peace ICT environment.

Those eleven norm namely:

(1) Maintain international peace and security inline with United Nation objective;
(2) Consider all relevant information, including context, challenge, and consequences form 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 right to privacy and freedom of expression;
(6) Avoid taking action or supporting ICT activities that is contrary to its obligations under international law
(7) Take an 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 steps to ensure the safety of ICT products, and preventing the spread of harmful ICT tools and techniques;
(10) Promoting a report that responsible on ICT vulnerabilities and share information on the best solution in limiting or eliminate potential ICT threats;
(11) A prohibition to support activities for damaging information system from official emergency response team of other country. As well as avoiding the involvement of official emergency response team of its country to involved in a dangerous international activity.

If we seen several norms that have a common spirit to improve security in cyberspace, avoiding the practice of using force in retaliating against the cyber attack that still remain on the corridor to realizing the United Nation Goals. Historically, the process of making this international law norms, firstly from the view of NATO with their Tallin Manual in 2013. Then responded by Shanghai Cooperation Organization Group with their Code of Ethics on 2015. All of this norm then accommodated with 11 norm that is filed by GGE ICT's on 2015. However, they didn't agree on the next meeting, then the step of 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 the period 2019-2020 and 2020-2021.[7]

National Law Regulation

Several countries have made an Institution or Organization that is specifically to dealing with cyber problem in their own 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 agencies in order to increasing the cyber defense of NATO. Other countries in Asia continent and Australia also make this cyber problem as a serious problem that will be happen and possible to affect the state defense. Australia, through Australian Signals Directorate, Australia Department of Defense established an institution called Cyber Security Operations Center (CSOC) that is responsible to detect and prevent a cyber crime threat toward the interest and Australia government. China also formed a "Blue Army" force, this force is in charge on protecting China defense from cyberattack. This force has its own home base in Guangzhou Military Area, in south of China. England also build their own cyber defense. The system called Cyber Security Operations Centre (CSOC) under the Government Communications Headquarters (GCHQ) England, in Cheltenham, round 160 Kilometers from northwest of London. The President of Republic of Indonesia, has signed Presidential Decree (Perpres) No. 53 of 2017 concerning on State Cyber and Code Agency (BSSN) on 19 May 2017. Then 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 president. Other than State Cyber and Code Agency, Indonesia State Army (TNI) also have a role on established a cyber unit (Satsiber) of Indonesia State Army in order to carry out the activities and cyber operation in the environment of Indonesia State Army to support the main duty of Indonesia State Army.

Indonesia have a serious history regarding cyberattack. It can be proven from several government owned site hacking incident, one of the case was the hacking of General Election Commission (KPU) site from infopemilu.kpu.go.id that served an information of temporary real count of regional election in 2018. The site is massively attacked by irresponsible person. This also happened on other government institution which is the site of Directorate General of Taxation (DitjenPajak), Ministry of Finance from pajak.go.id. The site was hacked on 10 June 2018. The site was hacked by a person who claimed as Anonymous Arabe. The cyberattack incident such as changing the view of a page (deface). In 2020, the number of cyberattack in Indonesia throughout the first semester of 2020 is reaching 149,78 million times. The number was increased five times compared to the same period on last year that is reaching 29,63 million times. The monitoring result of 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.

The threat of cyberattack is a real possibility that happened in this globalization and technology development era and knowledge in this world today. Those thread could come from overseas or within the state. Stephen M. Walt argued where counties face a threat by applying a balance where the behavior of the country alliance is determined by the threat that endangers them from other countries. Walt argued that a state generally will balancing its armed force in alliance to counter threats in the form of an alliance or defense pact. With the presence of an increasing threat, a countries that have a weak armed forced will more likely to join an on an alliance in order to protect their own security.

Walt Theory identify 4 (four) criteria that used to evaluate other country threat:[8] aggregate power (size, population, and economy capability), geographical proximity, offensive capability, and offensive intention.

Cybersecurity is collection of tools, policies, security concepts, security protection, guideline, risk management, actions, training, best practices, guarantees, and technology that can be used to protect the cyber environment and organization and user assets.

Legal Basis of Cyber Attack in Indonesia

a. The Constitution of Republic of Indonesia 1945, Article 30 Paragraph (1), (2), and (5) concerning on National Defense and Security
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
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
g. Regulation of the Minister of Defense No. 82 of 2014 Concerning on Cyber Defense Guidelines
h. The Information and Electronic Transaction Law

Establishing an International Regulation

To establishing an International Law, we need to look at the definition and scope of the international treaty such as Vienna Convention of the Law of Treaties 1969 and Convention on the Law of Treaties Between States and International Organization or Between International Organization and International Organization 1986.

Article 2 Paragraph (1) letter a, of Vienna Convention on the Law of Treaties 1969 explained that:

"treaty" means an international agreement concluded between States in written from and governed by international law, whether ambodied in a single instrument or in two or more related instruments and whatever its particular designation"

On the positive law of Indonesia which is the Law No. 24 of 2000 Concerning on International Treaties on the Article 1 Paragraph (1) stated that:

International Treaties is an agreement, in certain form and name, which are regulated in international law which is made in writing and creates a rights and obligations in the field of public law;

Then, it is also stated in the Article 4 Paragraph (1):

The Government of Republic of Indonesia made an International treaties with one state or more, international organization, or international legal subject according to the agreement; and both parties are obliged to carryout the treaties in a good faith.

From several regulations above it showed that every treaties that applied is binding the parties who agree about the treaties and must be done in a good faith on both related parties. This is universally recognized as a general principle of law.

According to SumaryoSuryokusumo, the good faith principle is a moral requirements so the treaties can be done in earnest. Because good faith is a moral requirement for the treaties so it can be done in earnest. Because good faith also one of the essence of pacta sunt servanda concept where overall it is held on many legal and arbitration decision.[9]

According to Vienna Convention 1986 it is stated: Treaties is an international treaties that is regulated by international law and defined in a written form: (i) between one state or more, and one or more international organization; or (ii) between international organization, both agreement in form of an instrument or more that one instrument that is relating each other. Therefore, there are several element or qualifications that need to be fulfill on a treaties so it can be said as international treaties namely: agreement, international law subject, in a written form, regulating on a specific object, and it is obeying international law.

In forming an international treaty, it is sometimes done by an approach both formal or informal between diplomats or state officials that want to made a treaties of several problem. The approach also can be done on an international organizational forum in globally or regional such as ASEAN. The result from the approach then made an ideas that will be followed up into a bilateral or multilateral international treaties. The process on making international treaties has been regulated on the Vienna Convention 1969 and Vienna Convention 1986 which refer the representative of the parties that is given a duty or obligation to hold a negotiations, submission of full powers attorney by the representative of each parties, a negotiation to made an agreement clause, adoption of the text, creating an authentic treaties manuscript (authentication of the text), a consent regarding the treaties (consent to be bound by a treaty), determining the entry into force of an international treaty (entry into force of a treaty), depository of a treaty, and registration and publication of the treaty.[10]

In order to made an international treaties into positive international law, then the related countries need to declare their agreement to be strictly bound on the agreement concerned. Several ways to express an agreement on a treaties in accordance with Vienna Convention namely by signature, exchange of instruments constituting a treaty, ratification, acceptance, approval, or other ways that is agreed in the agreement.

Different with other scope, the cyberspace has its own special characteristic with a difficulty in timing and the venue. Therefore, in determine the norm in this space, at least three things according to Lessig, as described by Edi Atmaja, which must be considered, namely: (a) who is regulated; (b)

where are they; (c) what they did. According to Lessig, if a state cannot know for sure who is regulated, where are they, and what they did, then a state cannot regulate a norm in a cyberspace.[11] To find out which individual are regulated, location and actions, of course it need a qualified infrastructure so it can be properly regulated and keep relationship in cyberspace safe and smooth.

ASEAN Regional Cooperation

ASEAN (Association of South East Asian Nation) is one of international organization which is 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 member of ASEAN is in form of cooperation. Cooperation, in this case is by having relationship between two states or more in order to reach an agreement. The cooperation between ASEAN member in field of social and culture, politic and security, education.

The purpose of cooperation in politic and security field is to create a safety, stability, and peace between ASEAN country. Cooperation in the field of politics is a concern of ASEAN. Some of concrete example 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 inter-parliamentary institution.

Regionally in ASEAN, it has made various attempt to promote awareness and joint commitment in enhancing cybersecurity. Several attempts by ASEAN can be identified from various cooperation documents such as on ASEAN Leaders' Statement on Cybersecurity Cooperation on the 32nd ASEAN Summit in Singapore on 2018. Moreover, on the year before, in Manila, ASEAN Declaration to Prevent and Compat Cybercrime is agreed. In 2016, at Brunei Darussalam, the ASEAN nation have been aware on the importance of personal data protection through ASEAN Framework on Personal Data Protection. Then further more in 2012, on the 19thASEAN Regional Forum (ARF) at Cambodia, the foreign affair minister in ASEAN have agreed on increasing cooperation in guaranteed the cyber security through ARF Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security.[12]

On 2017, ASEAN has done a 2nd International Security Cyber Workshop Series that is aiming to conserve and enrich the stability of cyber in the regional area of ASEAN. This workshop generally discussed about the opportunity and challenge in the context of peace and security on cyberspace. There are 4 main topic that is discussed on this workshop such as: (a) The 2017 GGE and Issues for International Agreement; (b) The sovereignty and global perspective on international law regarding on cyberspace; (c) Regional perspective on norm and act of building trust; (d) the next step on international cooperation

Here is the explanation:[13]

a. The 2017 GGE and Issues for International Agreement

   The failure to reach agreement at the GGE's 2017 Council, doesn't mean that the report and recommendation to the United Nation General Assembly that is exist before has to be ignored. The failure of GGE's in reaching agreement because 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 was difficult to reach agreement in several things such as threat analysis, the binding strength of the agreement, and capacity building and mutual trust building. The main reason they cannot agreed is the application of international law on ICT's dan how the norms that is not binding can made a state responsibility.

Those eleven norms, cannot prevent a conflict and a state difficulty on enforce those norms in the practice. This can be seen from several fundamental question that is still about the definition of the use of force in the context of cyber. Several arguments said that they cannot defined "use of force". In this case the countries are tend to taking defensive action in responding the usage of force on the cyber context.

Other things that is need by the state, is the creation of various bilateral agreement, regional and international to assist each countries in increasing trust among them. An open multi-stakeholder approach is needed to increase regional unity in advancing a multilateral process. The speakers on the forum also giving a special attention to the information asymmetry, among the 25 of the members and those who were involved on its making. As an effort to fostering an ICT's space that is open, stable, and safe, many countries need to be included and to be heard in various ICT's discussion that is related with the international security issues.

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

In the context of sovereignty, it is focused on the urgency of the state participation in wider area of regional level in order to made a wider space, for the involvement of countries internationally. In practice, International Humanitarian Law doesn't explicitly mentioning cyberattack, but in the principle of International Humanitarian Law it is regulates Distinction, Proportionality, and Military Necessity and various arrangements related to hostility act of a state in a conflict that occurs on cyberspace.

The most dangerous thing on cyber operation for state is ensure, is the cyber operation 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 the practice, on several state with sophisticated cyber equipment doesn't place the principle of state sovereignty as something that must be upheld, within the framework of norm and international law. Increasing the transparency and cyber capability of each country, is the initial stage in building trust, and stability in cyberspace on international life.

Generally, the expert on this workshop also agree, that there is no legal vacuum on regulating malicious behavior in cyberspace. So, there is no urgency to made an international treaty or new convention regarding on this problem. They also remind to not applying a high standard of norm in the cyberspace than other. The main challenge for international community is to managing activity that is the limitation of the use of force also the activity in the peacetime such what proxy have done, an organized cyberspace crime network.

On the global context, there are doubt related to one permanent institution specifically related to ICT's, this is based on many countries are still in early stages of developing institutional and legal structure for cross-border cyber issue. The current international geopolitical condition, also have 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 regionally is very diverse, and covering a different economy background. As the home of 55% of internet user all over the world, there still a real gap between states. More than half of the household in this region doesn't have access to internet. Several state has done a development to bridging this gap, with increasing the connectivity on every citizen. This efforts also have an impact on weak cybersecurity which is not a priority. In addition, the differences in national value, government structure, a strong and diverse views relating to special issue such as sovereignty, human rights, and content control, are important aspect that shouldn't be ignored.

The GGE's previous report is considered have providing a map with offering a high-level commitment of ASEAN countries that set the expectation for responsible state behavior. Even with the existence of high principle, existing asymmetry in cyber technical expertise, legal and politic and cyber capabilities are the limitation in order to increasing trust between state.

d. Regional Perspective and the next step on encourage international cooperation

On 2017, at least there are 80 until 90 state that has done a revisions related with cybersecurity law. Other than that, there also 30 state actively invest on offensive cybersecurity development. There is a tendency of increasing international involvement and cooperation among

countries especially in terms of using cyber domain which is aimed to building a resilience of cyber architecture, both in time of peace and during conflicts.

Pause on the GGE's stage also giving an opportunity to increasing participation of other countries. With involving various Non-Governmental Organization (NGO), as it is happened on the Tallin Manual and Hague Process for a possibility of wider participation. Even though it can be every state is not agreed with the deal that is taken, but it leading into international law and cyber spatial management discourses.

In the end of the session, the audience was asked to consider six potential format with various characteristics to bring the international discussion forward with regional preference. Those six formats namely: (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 at Thailand, ASEAN Defense Ministers' Meeting Plus (ADMM-plus) occurred, agreed to established 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 on making international law norm in the field of cyber on Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (OEWG ICT's). Indonesia also one of the special member of UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (GGE ICT's) period 2019-2021.[14] It's not an impossible thing, if in the future Indonesia could significantly act in determining the regulation on International Law regarding on Cyber.

CONCLUSION

A Contemporary crime that is developed along with globalization in form of cyberattack that is indicated with aggression crime need a special attention by world community. Making a legal instrument in form of ASEAN regional cooperation is one of the initiation in order 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 aggression crime.

ACKNOWLEDGEMENT

The authors are grateful to the Indonesian Ministry of Research and Technology for the Higher Education Leading Basic Research Scheme in 2020. The authors are also grateful to the research assistants for helping in data collection and processing to improve the results.

REFERENCES

Murray Andrew D 2007 The Regulation of Cyberspace, Control in the Online Environment (Routledge-Cavendish)

Katherina C. Hinkle 2011 Counter measures in the Cyber Context: One More Thing to Wony About YJILOnllne 17 4 (Fall 2011)

Erwin Prima 2020 BunuhSoleimani Drone MQ-9 Reaper AS Paling Ditakuti di Dunia (Tempo Onine) https://tekno.tempo.co/read/1294958/bunuh-soleimani-drone-mq-9-reaper-as-paling-ditakuti-di-dunia/full&view=ok

James P. Farwell and RafalRohonzmskl 2011 Stuxnet and the Future of Cyber War Survial 53

Maskun; Alma Manuputty; S.M. Noor; JuajirSumardi 2013 Kedudukan Hukum Cyber Crime dalamPerkembangan Hukum InternasionalKontemporerJurnalMasalah-Masalah Hukum, Universitas Diponegoro Semarang 42 (4)

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel 2012 The Law of Cyber-Attack California Law Review 100 (4) p. 817-885, Published by: California Law Review, Inc.

Hamonangan, I., &Assegaff, Z. 2020 Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital. Padjadjaran Journal of International Relations 1 (4)

Juraeva, Asal, and KhumoyunSoyipov. "Chinese International Commercial Courts: Overview and Potential Questions Around It." Hasanuddin Law Review 8, no. 1 (2022): 1-17. DOI: http://dx.doi.org/10.20956/halrev.v8i1.3315

SumaryoSuryokusumo 2008 Hukum PerjanjianInternasional (Jakarta :Tatanusa)

Zulkifli 2012, Kerjasama InternasionalSebagaiPengelolaan Kawasan Perbatasan Negara (StudiKasus Indonesia), (Depok : tesis Universitas Indonesia)

Ap Edi Atmaja 2014 Kedaulatan Negara di Ruang Maya Kritik UU ITE dalamPemikiranSatciptoRahardjoGemaKeadilan 1(1)

Muhammad Aris Yunandar 2019 Laporan Utama KerjaSama KeamananSiber di ASEAN dalamMenyambutIndustri 4.0, Masyarakat ASEAN (edisi 22 September 2019)

UNIDIR 2017 Preserving and Enhancing International Cyber Stability : Regional Realities and Approaches in ASEAN (Singapore: UNIDIR)

Anonym, 2020, Indonesia SuarakanStabilitasSiber di PBB, dapatdiaksessecara daring melaluihttps://kemlu.go.id/portal/id/read/1327/view/indonesia-suarakan-stabilitas-siber-di-pbb