Legal'S Standing of Cyber Crime in International Law Contemporary

Maskun[1], Alma Manuputty[2], S.M. Noor[3], Juajir Sumardi[4]

1. Doctoral Candidate at Legal Science, Post Graduate Hasanuddin University, Indonesia and, International Law Department, Hasanuddin University, Jl. Perintis Kemerdekaan Km. 10 Tamalanrea, South Sulawesi, Indonesia, 90245.
2. Professor of International Law Department, Hasanuddin University and Promotor, Jl. Perintis Kemerdekaan Km. 10 Tamalanrea, South Sulawesi, Indonesia, 90245.
3. Professor of International Law Department, Hasanuddin University and Co-Promotor, Jl. Perintis Kemerdekaan Km. 10 Tamalanrea, South Sulawesi, Indonesia, 90245.
4. Professor of International Law Department, Hasanuddin University and Co-Promotor, Jl. Perintis Kemerdekaan Km. 10 Tamalanrea, South Sulawesi, Indonesia, 90245.

*Email the corresponding of Author : maskunlawschool@yahoo.co.id, maskunmaskun31@gmail.com

Abstract

Cybercrime is a new range of international law, particularly international criminal law. The existence of cybercrime is now a fact that should be taken seriously by the international community. It creates then intersection with other crimes such as crime of aggression and other crimes. Immediate response form is needed to regulate cybercrime internationally because the fact shows that no one convention has found cybercrime internationally. The existed Convention of Cyber Crime enacts only regionally like European Convention of Cyber Crime and locally (like in Indonesia), the Law number 11/2008 concerning Information and Electronic Transaction.

Keywords: Cyber Crime, International Law Contemporary.

1. Introduction

Cybercrime can be said as the contemporary of international criminal law. The using of contemporary phrase shows that cybercrime as a part of international criminal law has grown fast, which started in 1970 and still growing until today. In its development, cybercrime has conducted with various modus. It means that is not only involving perpetrator in individual context, but also perpetrator that allegedly involving country as intellectual actor.

Some kind of cybercrime with sophisticated variety can be seen for example in 2005 when Chinese government utilized outsourcing to commit cyber piracy to United States (James P. Farewell and Rafal Rohonzinski, 2011). In 2007, Estonia got cyber-attack that allegedly done by Russia that immobilized Estonia's government and commerce networks. Approximately one million government's infected computers that distributed in form of *Distributed Denial-of-Service (DDoS)* attack. Similar case happened in 2008 when war occurred between Georgia and Russia which put Moscow as a multiple strategy for Russian Military Campaign that also done through *Distributed Denial-of-Service-DDoS (*Yoram Disntein, 2002).

Those crimes occurred in Estonia and Georgia could be stated as a whole or a part of Russian government policy. In this context, modus that done by attacking government's document was fatal in result and could threaten existence and comfort of both country citizens. Fatal phrase in this case means that it violates state sovereignty and infrastructure of Estonia and Georgia (James P. Farewell and Rafael Rohonzinski, 2011).

Another example of cyber-attack also occurred in Iran on June 2010. The attack was targeting Iran nuclear facility in Natanz. Approximately 60.000 computers infected by virus called Stuxnet. In terms of it, it did not only violate Iran's sovereignty, but it was also harmful for the Iran's civilization security.

According to Kevin Hogan (http://www.reuters.com, 2010), Senior Director of Symantec, 60 percent of infected computer worldwide are located in Iran and its main target is nuclear installation possessed by Iran's government. Russian computer security company, Kaspersky Lab, conclude that those sophisticated attack should be done "by state support" and allegedly Israel and United State may have been involved.

Different to Stuxnet whose attacked and infected computer and networks, in the end of May 2012 it found the development of new virus called "Flame" which worked as espionage device by infiltrating to computer and network and secretly issuing the information that contained in computer and network. This development of Flame was done by countries to spy the other country activity (David P. Fiddler, 2012). Latest case happened in February 2013 when United States internet security company, Mandiant, released a report that showed China activities to hack some western companies (Kompas, 2013).

Complexity of type and modus variant of cybercrime, in practice as mentioned above, is not followed by adequate regulation or legal instrument especially in context of international law (Maskun, 2013). Some current enacted regulation that applies in international practices is European Cybercrime Convention (ECC) and some other national regulation. The existence of some provision on cybercrime as if ECC indeed are still in regional scope Hence, the need of legal framework in cybercrime context is a new challenge in legal world. Availability and limitation of the current regulation are "pushing" law enforcement officer and policy makers to make law in this field (emerging norms/laws) so verdicts that related to cybercrime issues can fulfill the aspect of justice, expediency, and rule of law (Dedy Nurhidayat, 2006), (Abdul Wahid and Muhammad Labib, 2005). Realizing the cybercrime discourse as explained above therefore in this paper, cybercrime will be focused on its intersection to crime of aggression in contemporary international law.

2. Methodology

2.1. Type and Approach of Research

The research was categorized as a normative research. The research was intended to formulate the best solution to deal with the real problems was being faced. To get the goal of it, the research employed some approaches such as conceptual, historical, statute, comparative, and cases approaches.

2.2. Type and Source Data

The data of the research was classified as primary and secondary data. The primary data was collected directly to the main source (respondents). The respondents were: 1) some experts of cybercrime and crime of aggression; and 2) some governments and organization websites officially. The secondary data furthermore was collected via primary, secondary, and testier of legal documents. Those documents could be from statute, laws, jurisprudence, draft regulation, results of research, and encyclopedia.

2.3. Technical of Collected Data

The collected data technically was applied library study, observation, and interview. The library study was a prior technique of legal research. This methodology brought a plenty of advantages of the research without disturbing the research objects (Jonathan Sarwono, 2006). The observation was the next method to collect the data via observing and writing some phenomena of the research objects systematically (Cholid Narbuko and H. Abu Achmadi, 2004). The interview itself applied unstructured interview where the researcher provided merely some main questionnaires.

2.4. Data Analysis

The analysis was based on the data that came from the primary and secondary data. Technically, the analysis was theoretically-rationally that applied deductive method to elaborate both the primary and secondary data (Milles Mattew and A. Michael Huberman, 1982). The data has been analyzed then keeping the objective of this research.

3. Results and Discussion

3.1 The Meaning of Cybercrime

Before elaborate the definition of cybercrime in detail, it will be explained first that the core of cybercrime actually is cyberspace. Cyberspace is seen as computer-based communication world. In this case, cyberspace is considered as a new reality in human being life which is in daily life recognized as an internet. This new reality is formed by computer network that connecting countries or continents based on transmission control protocol/internet protocol. It can be said in its working system that cyberspace (internet) has transformed distance and time to be unlimited. Internet is being described as set of computer network consist of numbers of smaller networks with varying network system (Kenny Witson, 2002).

In the subsequent development, the presence of advance computer technology with internet network has brought great benefits for human beings. Its utilizations are not only in government, private sector/corporate, but it has also reached all sector of life including household needs (personal). Computer (internet) has been able to open up new horizon in human life, both in context of communication and information facility that promises transcend national boundaries as well as dissemination and exchange of knowledge and ideas amongst scientist all around the world (Widyopramono Hadi Widjojo, 2005). However, advances in information technology and all kind of benefits in it, bring its own negative consequences where the criminal contender will be easier to commit crime that increasingly disturb the public. The abuse of cyberspace is then known as cybercrime or in the other literature mentioned as computer crime.

In several literatures, cybercrime is often identified as computer crime. According to US Department of Justice, computer crime described as "any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution" (www.usdoj.gov). Another opinion proposed by Organization for Economic Cooperation Development (OECD) stipulates that use "computer related crime" phrase means any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmission data" (Obsatar Sinaga, 2010).

Cybercrime on the other hand, not only uses advance computer technology but also it involves telecommunication technology in its operation (Ari Juliano Gema, 2000). It can be seen in Indra Safitri's view

(1999) which proposed cyber crime as type of crime related to the use of unlimited information technology and also has a strong characteristic of technology engineering that rely on high level security and credibility of information that delivered and accessed by internet consumer.

Therefore, it can be said that cybercrime and computer crime are two different things. The difference can be seen in Nazura Abdul Manaf's opinion (Agus Rahadjo, 2002) which marks off cyber crime and computer crime, as follows:

> *"Defined broadly, computer crime could reasonably include a wide variety of criminal offences, activities or issues. It also knows as a crime committed using a computer as a tool and it involves direct contact between the criminal and the computer. For instance, a dishonest bank clerk who unauthorizedly transfers a customer's money to a dormant account for his own interest or a person without permission has obtained access to other person's computer directly to download information, which in the first place, are confidential. These situations require direct access by the hacker to the victim's computer. There is no internet line involved, or only limited networking used such as the Local Area Network (LAN).Whereas, cyber crimes are committed virtually through internet online. This means that the crimes could extend to other countries, which is beyond the Malaysian jurisdiction. Anyway, it causes no harm to refer computer crimes as cyber crimes or vice versa, since they have same impact in law".*

Basic difference between cyber crime and computer crime as defined by Nazura Abdul Manaf is the existence of connected computer unsure by telecommunication device in form of internet online as medium for someone or group of people to commit violence and or cyber crime. Whereas, computer crime committed by someone by using computer as medium to do offense without involving internet network.

3.2. Legal's Standing of Cybercrime in International Law Contemporary

International law is a law of integration between the different legal systems of different countries. Integration shows cooperation between states in international community (Magdalena Petronella Ferreira-Synman, 2009). In legal approach, international law regulation cannot be protected and promoted individually, but it should be pursued by all countries around the world.

The development of International law occurred today has influenced by various issues such as human rights, democracy, poverty, environment conservation, and threat to security and peace. The development shows that those various issues have been intersection to each other. This intersection is influenced by the development of information and technology which has created a new crime as a consequence of international character that attached to those various forms and modus.

Intersection of cybercrime and international crime has put cybercrime as one of contemporary international law variants. Contemporary meanings that cybercrime as a consequence of the development of international law had also expanded scope and coverage of international criminal law. It can be proved by seeing the type of international crime in historical context that have not qualified cybercrime as a kind of international criminal law.

Theoretically, M Cherif Bassiouni (Eddy O.S. Hiariej, 2009) divides the stage of international crime in to three stages. First, international offence called "international crimes" which is a part of *jus cogens.* Type and character of international crime is related to peace and security as a fundamental value of humanity. There are eleven offences that placed in highest hierarchy as international crime, as follows:

1. Aggression.
2. Genocide.
3. Crimes against humanity.
4. War crimes
5. Unlawful possession or use or emplacement of weapons.
6. Theft of nuclear materials.
7. Mercenaries.
8. Apartheid.
9. Slavery and slave-related practices.
10. Torture and other forms of cruel, inhuman, or degrading treatment.
11. Unlawful human experimentation.

Second, international offense called International Delicts. Type and character of the international delicts is related to protection of international's interests that covered more than one state or victim and the emerged detriment comes from one state. There are thirteen international offenses that categorized as international delicts, as followings:

1. Piracy.
2. Aircraft hijacking and unlawful acts against international air safety.
3. Unlawful acts against the safety of maritime navigation and safety of platforms on the high seas.
4. Threat and use of force against internationally protected person.
5. Crimes against United Nations and associated personnel.
6. Taking of civilian hostages.

7. Unlawful use of the mail.
8. Attacks with explosive.
9. Financing of terrorism.
10. Unlawful traffic in drugs and related drug offenses.
11. Organized crime
12. Destruction and/or theft of national treasures.
13. Unlawful acts against certain internationally protected elements of the environment.

Third, International offense called as international infraction. In international law as a normative, international infraction is not including into international crime and international delicts category. There are four offences that classified as international infraction, as following:

1. International traffic in obscene materials.
2. Falsification and counterfeiting.
3. Unlawful interference with submarine cable.
4. Bribery of foreign public official.

An analysis of international crime qualification as explained by Bassiouni clarifies cybercrime position which implicitly have not categorized yet as a part of international crime. Therefore, in order to qualify cybercrime as a new type of international crime, the qualification should base on elements of international crime. According to Bassiouni (Romli Atmasasmita, 2003), there are three elements to fulfill as prerequisite to be categorized as international crime. Those elements are:

1. International element, including direct and indirect threat to world peace and disturb the feeling of humanity.
2. Transnational element, including the effect that has impacted more than one country, to citizen from more than one country, and facility and infrastructure also method that used is beyond the territorial boundaries of a country.
3. Necessity element, including the need of cooperation among countries to undertake prevention.

Starting at the description of the elements of international crime as stated by Bassiouni, then cybercrime implicitly can fulfill all the elements to be categorized as a new offense in international crime literature nowadays. Description of elements in question can be constructed as follows:

a. International element, namely the existence of threat to world peace both direct and indirect. In this context, cyber crime has a potential to threat world peace. Stuxnet case (2010) and Flame (2012) as mentioned in the previous section are highly dangerous because control to nuclear activity can be done by someone and or state easily. According to Ralph Lagner, Stuxnet described as cyber weapon that used to attack the entire Iran’s nuclear program (James P. farewell and Rafal Rohonzinski, 2011). This kind application of cyber-weapon will be used easily nowadays considering massive development of information and technology that cannot be avoid.
b. Transnational element means that cyber crime’s scope and coverage is interstate. According to Hata (2012), cybercrime occurred shows that state’s traditional sovereignty is so easy to penetrate, which at the same time weakening the traditional authorization functions of a country. Hata’s statement, (2012) then can be easily proven by seeing several cases from credit card theft case, online gamble, illegal access, espionage, to cyber terrorism which has been started to develop in last couple years.
c. Necessity element means international cooperation between countries is needed to face and try the perpetrator of cybercrime in an international tribunal frame. In this context, the cooperation should form in terms of international law treaty (Maskun, 2013).

Fulfillment of international crime proposed by Bassiouni put cyber crime as sophisticated international crime which has its own legal standing. Internet as a medium (tools of crime) has facilitated international law both private and public to apply in form of international law product. International law product that regulates cyber crime specifically will enrich international law practice and literature itself. Moreover, current fact shows the absence of international law instrument that apply universally to regulate and prosecute cyber crime that occurred.

The needs of international law instrument are the basic need of international community to handle cybercrime and its intersection to other crimes including crime of aggression. Until now, there is no international law treaty concerning cybercrime. Some current cybercrime regulations are enacted regionally and domestically. Those regulation can be assumed as a part of cyber security system to protect every individuals both active and passive user.

1. European Convention on Cybercrime (ECC)

   The only binding international instrument against cybercrime nowadays is ECC. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between state parties (http://conventions.coe.int/Treaty, 2014). It has been also ratified and accessed by 41 countries and 11 countries signed without following with ratification. It has been entry into force on 1 July 2004.

It covers type of cybercrime such as illegal access, illegal interception, data and system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights (article 2-11 of ECC).

Related to those articles (2-11), the ECC explains furthermore the jurisdiction of the ECC under article 22 of the ECC.

"1.Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or
b on board a ship flying the flag of that Party; or
c on board an aircraft registered under the laws of that Party; or
d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution".

2. The Law Number 11 Year 2008 Concerning Electronic Information and Transaction (UU ITE)

UU ITE is the only of the Indonesian Law against to some cybercrime issues. It has been entry into force a year after enacting (2009). The law applies to the development of interoperability for data exchange occurs given in between information system is an electronic system. It is covering some issues such as electronic transaction, domain name, intellectual property rights, and protection of privacy rights.

Those legal instruments as mentioned above are samples of legal instruments. However, those instruments are enacted only in one region and state. They cannot be enforced to other states that do not being ratified or accessed. Some other weaknesses of those instruments are scope of the cybercrime. The scope of it is expanded to other crimes that have intersection to cybercrime such as war crime, crime of aggression, and cyber of espionage. Those expanded type of cybercrime will be a new challenge of international criminal law to be governing internationally.

4. Conclusion

Cybercrime is a new fact and phenomenon in international law corridor. International law response placed cybercrime as a new kind of international crime that has not been regulated internationally. The Needs of international law instrument is highly urgent to be created. Indeed, it is considered that the regulation should be governed by international law product universally. With universal nature of arrangement, it will provide cybercrime a legal status in international law.

References

Atmasasmita, Romli. (2003). *Pengantar Hukum Pidana Internasional*, Bandung, Refika Aditama.

Dinstein, Yora. (2002). "Computer Network Attacks and Self-Defense", *76 Int'l L. STUD*, 99.

Ferreira-Synman, Magdalena Petronella. (2009). *The Erosion of State Sovereignty in Public Internaional Law: Towards a World Law?*, Afrika Selatan, University of Johannesburg.

Gema, Ari Juliano. (2000). "Cybercrime: Sebuah Fenomena di Dunia Maya", diakses pada www.theceli.com.

Hadi Widjojo, Widyopramono. (2005). "Cybercrimes dan Pencegahannya*"*, *Jurnal Hukum Teknologi*, Fakultas Hukum Universitas Indonesia, Vol 2.

Hata. (2012). *Hukum Internasional : Sejarah dan Perkembangan hingga Pasca Perang Dingin,* Malang, Setara Press.

Maskun. (2013). *Kejahatan Siber: Suatu Pengantar*, Jakarta, Prenada Kencana.

________. (2013). "Cyber Security: Rule of Use Internet Safely?*", Journal of Law, Policy and Globalization*, Vol. 15.

Mattew, Milles and Huberman A. Michael. (1982). *Analisa Data Kualitatif,* translated by Tjetjep Rohendi Rohini, Jakarta, UI Press.

Narbuko, Cholid and Achmadi, H. Abu. (2004). *Metodologi Penelitian*, Jakarta, Bumi Aksara.

Nurhidayat, Dedy. (2005). “Eksaminasi Terhadap Perkara Pidana Terkait Pembobolan Situs Komisi Pemilihan Umum”, *Jurnal Hukum Teknologi*, Vol 2. Nomor 1.

O.S. Hiariej, Eddy. (2009). *Pengantar Hukum Pidana Internasional,* Jakarta, Airlangga.

P. Fiddler, David. (2012). “Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law”, *ASIL*, Vol.16. Issue 22 .

P. Farwell, James, and Rohonzinski, Rafael. (2011). “Stuxnet and the Future of Cyber War”, *Survival*, Vol. 53.

Raharjo, Agus. (2002). *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung, Citra Aditya.

Reuters, “2-Cyber Attack Appears to target Iran-tech Firms” http://www.reuters.com/article/2010/09/24/security-cyber-iran-idUSLDE68N1OI20100924.

Sarwono, Jonathan. (2006). *Metode Penelitian Kuantitatif dan Kualitatif,* Yogyakarta,Graha Ilmu.

Sinaga, Obsatar. (2010). “Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia”, Makalah, Bogor, Institut Pertanian Bogor.

Safitri, Indra, *Tindak Pidana di Dunia Siber*, Insider, Legal Journal From Indonesian Capital and Investment Market, 1999, diakses http://business.fortunecity.com

Wahid, Abdul, dan Mohammad Labib. (2005). *Kejahatan Mayaantara (Cyber Crime)*, Bandung, Refika Aditama.

Wiston, Kenny. (2002). *The Internet: Issues of Jurisdiction and Controversies Surrounding Domain Names*, Bandung, Citra Aditya.

http://www.un.org/apps/news/story.asp?NewsID=23977&Cr=general&Cr1=debate&Kw1=general+assembly&Kw2=&Kw3=, *Estonia Urges UN Member States to Cooperate Against Cyber Crimes*, Posting 27 Sepetember 2007, diakses 05 Oktober 2012.

http://conventions.coe.int/Treaty, diakses 3 Februari 2014.