J. East Asia & Int'l L. Vol. 13/No.2 (2020); 397-418
Publication type : Research Article
Section : Regional Focus & Controversies
DOI : http://dx.doi.org/10.14330/jeail.2020.13.2.08

# Qualifying Cyber Crime as a Crime of Aggression in International Law

Maskun, Achmad, Naswar, Hasbi Assidiq, Armelia Syafira, Marthen Napang, Marcel Hendrapati*

*Today's technological developments have resulted in the emergence of various new crimes threatening the international community. In recent decades, there have been various forms of cybercrimes targeted at the communication networks and defense systems of countries by other countries, known as cyber warfare. Unfortunately, international law has not specified this as a crime, but its impact has caused violations of sovereignty and disruption of national security, resulting in material loss, breakdown of communication networks and obstruction of social and public services based on the internet, such as what happened in Estonia in 2007. This article is a normative study that analyzes the elements of cybercrime relating to threats to a country's security. The modification of the cybercrime concept is necessary to designate cybercrimes as crimes of aggression amid technological development to maintain stability in the international community.*

**Keywords**
Cybercrime, Crime of Aggression, Cyber Warfare, NATO Cyber Defense Action Plan, Violation of Sovereignty

* Maskun, Achmad, Naswar, Hasbi Assidiq, Armelia Syafira, Marthen Napang, Marcel Hendrapati, all the authors are lecturers in the Law Faculty of Hasanuddin University, Indonesia, with the exception of Armelia Syafira and Hasbi Assidiq, who are both Research Assistants at the Law Faculty of Hasanuddin University, Indonesia. The corresponding author is Marcel Hendrapati. He may be contacted at: mhendrapati@yahoo.com/Address: Jl. Perintis Kemerdekaan Km.10 Makassar, 90245. Sulawesi Selatan, Indonesia.
All the websites cited in this article were last visited on October 20, 2020.

# 1. Introduction

In recent, the development of technology is happening very rapidly. This has an impact on social interaction which facilitates the provision of human needs. In addition to the positive impact, however, it creates a new form of crime known as "cybercrime," which is threatening the harmony of the international community. In general, cybercrime is defined as any activity that uses computers or networks as tools for criminal activities.[1]

Cybercrime has become very complex and is beginning to spread to the areas that threaten national security and sovereignty. This is known as cyber warfare. Cyber warfare is the use of cyber technology to attack various public facilities that are related to the national security and sovereignty of a country by another country, either directly or through an established proxy.[2] The last 35 years has shown the involvement of countries in cyberattacks against other countries, such as Operation Orchard involving Israel and Syria, the cyberattack on Estonia in 2007 allegedly carried out by Russia, and Operation Olympic Games (Stuxnet case) involving the US and Iran in 2010. In CASCON records, there have been 85 cases of "kinetic" warfare,[3] which means the "utilization of technology as a tool to attack one state."

Indonesia is facing a growing number of cyberattacks. Based on data from the Indonesia Security Incident Response Team on the Internet Infrastructure/ Coordination Center (ID-SIRTII) in 2015, there were 28,430,843 cyberattacks and this number increased to 135,672,984 in 2016. 47% of these cases were malware attacks, 44% fraud cases, and the rest are various cybercrimes, such as website defacement, data manipulation activities, and data leakage.[4] However, the scale of cyberattacks on Indonesia is not comparable to those on Iran and Estonia, which paralyzed various social activities and Internet-based public services. Nonetheless, cyberattacks against Indonesia are very detrimental. Therefore, an effective strategy is needed,

1 M. Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, International Telecommunication Union, (Sept. 2012), http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

2 M. Gazula, *Cyber Warfare Conflict Analysis and Case Studies* (MIT Sloan School of Management CISL Working Paper No. 2017-10, May 2017), https://dspace.mit.edu/handle/1721.1/112518. *See also* E. Turrini & S. Ghosh, *A Pragmatic, Experiential Definition of Computer Crimes*, *in* Cybercrimes: A Multidisciplinary Analysis (E. Turrini & S. Ghosh eds., 2011).

3 *Id.* at 13.

4 Kementerian PPN/Bappenas, *Policy Paper/Policy Brief: Development of National Cyber Security Budget Year 2018* [Pengembangan Keamanan Siber Nasional Tahun Anggaran 2018] at 44 (The Council of Information Technology and National Communication 2018), http://www.wantiknas.go.id/wantiknas-storage/file/img/kajian/POLICY%20PAPER%204%20-%20Cyber%20Security.pdf.

both internally and externally, in facing this challenge.

The development of international law is very dynamic, showing that there is a relationship between cybercrime and the crime of aggression. This relationship has contributed to the development of international law, especially in the form of perfecting international legal rules that specifically regulate cybercrime. Until today, no international convention or agreement on cybercrime has been adopted.[5] At this time, there is only a draft manual from NATO that is used as guidelines for cyberattacks regarded as crimes of aggression, cyber operations against important infrastructure of a country, and cyberattacks targeting enemy commands and control systems.[6] It is thus very important to provide a general international legal instrument with binding force on issues related to cybercrime, which are threatening the existence of countries. It could increase awareness and caution in dealing with the challenges of cybercrime by encouraging various forms of international cooperation.

This research aims to conceptualize cybercrime as a developing phenomenon in international law that can be categorized as a crime of aggression. In this article, the authors will chiefly examine the current development of cybercrimes. The paper will also include a brief history and definition, as well as the elements of crimes of aggression. Then, the authors will compare both crimes to understand the development of cybercrimes which threaten sovereignty and obstruct social activities and public services of countries.

## 2. Cyber Crime and its Development as an International Crime

The rapid development of technology aims to improve human life by providing easy interaction between people. A form of human interaction is the use of information and communication technology (ICT). At this time, there are various social networks that facilitate social interactions by the exchange of information through the Internet. In a society where computerized information is transferred ubiquitously, the

5 Maskun, Intersection between Cyber Crime and Crime of Aggression in the Context of Contemporary International Law 22 [Interseksi antara Kejahatan Siber dan Kejahatan Agresi dalam Hukum Internasional Kontemporer] (Fakultas Hukum Universitas Hasanuddin, 2015), http://digilib.unhas.ac.id/uploaded_files/temporary/DigitalCollection/NDdiMGZhZTViOTNhNzIyMzdiY2JhYjkwZmY0ZmIxZThjZmU3ZGQwNA==.pdf.

6 M. Schmitt (ed.), Tallin Manual on the International Law Applicable to Cyber Warfare (2013), https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

normal functioning of the society is severely degraded or altogether impossible if computerized systems no longer function correctly.[7]

The environment in which social interaction over computer networks takes place is known as "cyberspace."[8] This space is used daily by billions of people to communicate, find information, and conduct business transactions.[9] The high level of social interaction in this space and all its benefits, however, have indirectly led to negative consequences caused by the abuse of cyberspace. These abuses are known as "cybercrime."[10] There was a very significant increase in the number of internet users between 1995 and 2017. In 1995, the estimated number of internet users was only 16 million, while in 2017 the estimated number of users around the world reached 3.5 billion people.[11]

There are various types of cybercrimes: (a) offences against confidentiality, integrity, and availability of computer data and systems, such as illegal access (hacking/cracking), illegal data acquisition (data espionage), illegal interception, data interference, and system interference; (b) computer-related offences, such as computer-related fraud act, computer-related forgery, phishing, identity theft and misuse of devices; (c) content-related offences, such as pornography, racism, hate speech, glorification of violence, religious offence, illegal gambling and online games, libel and false information, spam and related threats; (d) copyright-related offences.[12] The classification of cybercrimes is given below in Figure 1.

7 Peeter Lorents, Rain Ottis & Raul Rikk, *Cyber Society and Cooperative Cyber Defence in* Internationalization, *in* Design and Global Development 182 (Nuray Aykin ed., 2009).

8 Shalhoub Zeinab Karake & Lubna Al Qasimi, Cyber Law and Cyber Security in Developing and Emerging Economies (E. Elgar ed., 2010).

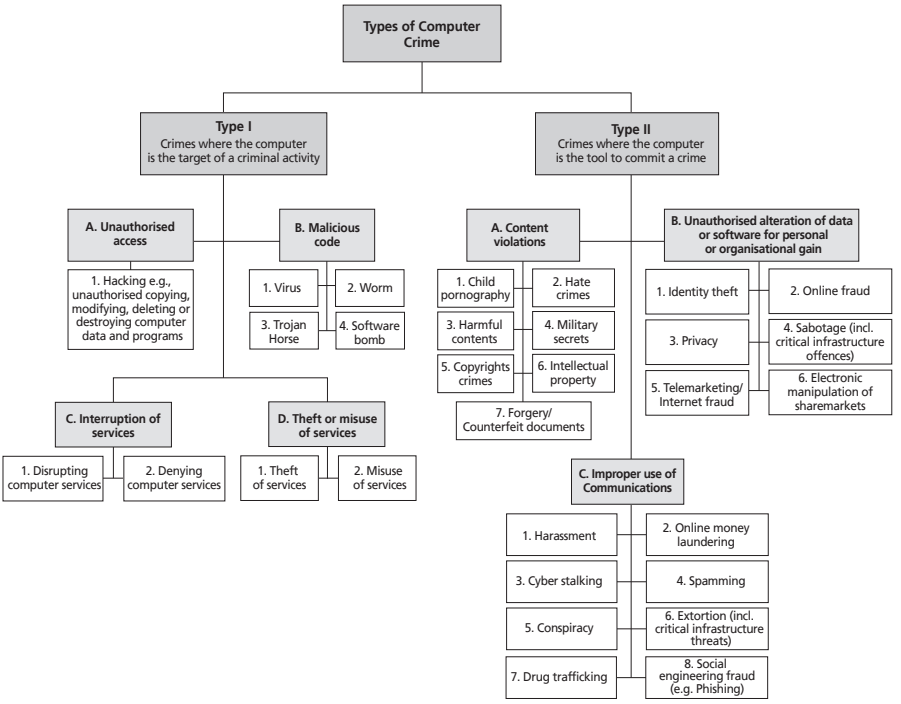
9 M. Eilstrup-Sangiovanni, *Why the World Needs an International Cyberwar Convention*, 31 Phil. & Tech. 379-407 (2018).

10 Maskun, et al., *Legal Standing of Cyber Crime in the Development of Contemporary International Law*, 42(3) Legal Probs. (Masalah-Masalah Hukum Jilid) 511-9 (2013), https://ejournal.undip.ac.id/index.php/mmh/article/view/13126/9949.

11 *Id.* at 13.

12 *Id.*

Figure 1: The Classification of Cybercrime[13]




Meanwhile, there are various motives of cybercrime, which can be categorized as (a) terrorism, (b) military espionage, (c) economic espionage, (d) targeting national information infrastructure, (d) vendetta/revenge, (e) hate (national origin, gender, and race), (g) notoriety, (h) greed, and (i) ignorance.[14] It is very important to understand these motives in order to know the cause of a cyberattack and, possibly, to calculate its scale and impact. A comprehensive analysis of the scale and impact of cybercrime can identify the responsibility pattern of the perpetrators.

Cybercrime could have a systemic impact on a country. This depends on the technology that is used and the motives of the crime. Certain cybercrimes are committed to cripple a country's military defense, as it happened in the case of Syria. Before Israel attacked Syrian nuclear area in Diaya-al-Sahir on September 2007, they first hacked into the Syrian air defense system to render Syria blind to any incoming

13 Ali Alkaabi et al., *Dealing with the Problem of Cybercrime*, *in* Digital Forensics and Cyber Crime 6-7 (I. Baggili ed., 2011).

14 J. Migga Kizza, Guide to Computer Network Security 119-20 (4th ed. 2017).

attack. The same attack method was used by the US in cooperation with Israel when they developed a Malware called "Stuxnet" to disable the Iranian nuclear reactor in Natanz.[15]

Cybercrime can also paralyze a country's economy and social infrastructure. An example can be seen in what happened in Estonia, known as spring cyber-attack, in 2007. The effect of the spring cyber-attack was huge, because of the high number of the Internet users in Estonia; for example, 98% of banking transactions were done electronically, and transfer of information was dominated by computer systems. This attack was a response to the Estonian government's decision to move the Bronze Soldier, a statue that was installed during the Soviet Union regime. The Estonian government's decision on the statue elicited a strong response from Russia. Russia criticized the Estonian government and accused Estonia of not respecting the then Soviet Union. The cyberattack focused on the websites of banks, broadcasting organizations, the police, and the government. Eventually, this attack paralyzed the government communication network and lasted for 22 days, from April 27 to May 18, 2007.[16]

Due to the adverse impact of cybercrime on countries, international cooperation is necessary to ensure responsible use of the cyberspace without harming any parties or countries. Without cybercrime, each country can freely develop their cyber technology because cybercrime has the potential to open opportunities for cyber war and increase global uncertainty. History already teaches that formal international treaty instruments can reduce the race to develop weapons, fears and uncertainties, and the dynamics of competition through the establishment of common rules that can be accepted by each country.[17]

Defense strategies against cyber-attacks can be divided into two. The first is deterrence by denial. This is done by building a strong cyber defense that can reduce the chance of attacks. The second is deterrence by retaliation. This strategy is carried out by developing the capacity to punish perpetrators of attacks.[18] If the enemy anticipates that an attack will likely trigger a counterattack, then the benefits derived from the attack will be offset. In general, cyber experts use the second defense effort, which is simply cheaper. The main reason for this strategy is the belief that protecting public network is difficult. According to Richard Clarke, Former National Coordinator for Security, Infrastructure Protection and Counter-terrorism of the US,

15 *Supra* note 7, at 379-80.

16 *Supra* note 2, at 67.

17 *Supra* note 7, at 404.

18 *Supra* note 9, at 15-6.

deterrence by retaliation is preferred because the US is able to protect its military network but unable to protect its public network effectively.[19]

At this time, there are inadequate international legal instruments to address the problem of cybercrime. Some international agreements have been made on a regional scale and in a multilateral form. Therefore, they are only binding on the countries included in that specific regional organization. The UN has been trying to adopt an international convention to regulate cybercrime as a whole, but such efforts are not successful yet. As an effort to fill the void in international law, the EU pushed for ratifying the European Cybercrime Convention, an international instrument addressing the cybercrime problem.[20]

Indonesia as one of the countries with the highest number of the Internet users assumes a responsibility to provide high cyberspace protection. Indonesia ranks 41 out of 175 according to the Global Cybersecurity Index[21] in line with legal, technical and organizational measures, capacity building, and cooperation. Cybercrime is a global problem beyond national borders or sectoral distinctions.[22] Since 2014, Indonesia has been aware of the importance of cyber defense because it ratified the Regulation of the Minister of Defense of the Republic of Indonesia Number 82 of 2014 concerning the Guidelines for Cyber Defense.

## 3. Concept and Complexity of the Crime of Aggression as an International Crime

The crime of aggression signifies human aggressiveness, which causes damage. It has occurred throughout the history of humanity with various developments.[23] To control the damage that occurs from this kind of activity, the *jus ad bellum* principle was formulated as a legal and moral constraint to prevent arbitrariness in the use of power against another country.[24]

19 *Id*.

20 *Supra* note 4, at 165-7.

21 ITU, Global Security Index 2018, at 28-9 (2019), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

22 *Id.*

23 Maskun, *The Crime of Aggression: Complexities in Definition and Elements of Crime* 25(2) Mimbar Hukum 367-75 (2013).

24 E. Elizabeth Carrol, *Victimhood and the Crime of Aggression: Broadening Victim Status at the International Criminal Court*, University of Oslo Library - Institut for offentlig rett (2019), http://urn.nb.no/URN:NBN:no-73859.

Article 227 of the Treaty of Versailles 1919 contains the first example of bringing perpetrators to account. Although the trial never happened, the crime of aggression was continued.[25] Further, the London Agreement was the basis for the establishment of the International Military Tribunal (IMT) at Nuremberg in 1945. Article 6 of the London Agreement mentioned the prohibition of the crime of aggression against peace and the possibility of holding individuals responsible in this regard.[26] The formulation of the crime of aggression in the Nuremberg Tribunal has become the reference for the postwar world.[27]

Further, in 1974, the UN General Assembly Resolution 3314 (XXIX), which defined the crime of aggression as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the UN Charter, as set out in this Definition."[28] In 1996, the UN International Law Commission (ILC) successfully came up with a Draft Code of Crime against Peace and Security of Mankind, which states: "An individual who, as leader or organizer, actively participates in or orders the planning, preparation, initiation or waging of aggression committed by a State shall be responsible for a crime of aggression."[29]

The definition of crime of aggression is crucial and complex due to the differences in interpretation among countries and experts.[30] The Rome Statue of 1998 has not explicitly provided the definition of crime of aggression. This is ironic because one of the competences of the International Criminal Court (ICC) is to adjudicate on the crime of aggression. In 2010, however, the Review Conference of the Rome Statute gave the Special Working Group on the Crime of Aggression (SWGCA) the mandate to prepare a proposal about crime of aggression, known as the Kampala amendments on the crime of aggression.[31]

Regarding the Kampala amendments, Article 8 *bis*, Paragraph 1 of the Rome statute defines the crime of aggression as "the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to

25 *Id.* at 3.

26 Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, signed at London (London Agreement), Aug. 8, 1945, 82 U.N.T.S. 279.

27 A. Cassese, *On Some Problematical Aspects of the Crime of Aggression*, 20(4) Leiden J. Int'l L. 841-9 (2007).

28 G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (XXIX) (Dec. 14, 1974).

29 U.N. International Law Commission-Draft Code of Crimes against the Peace and Security of Mankind with Commentaries 1996, art. 16, https://legal.un.org/ilc/texts/instruments/english/draft_articles/7_4_1996.pdf.

30 *Supra* note 18, at 369.

31 J. Trahan, *The Rome Statute's Amendment on the Crime of Aggression: Negotiations at the Kampala Review Conference*, 11(1) Int'l Crim. L. Rev. 49-104 (2011).

direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations."[32] In the meantime, the act of aggression is "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[33] Whether an act is a crime of aggression or not depends on (a) objective and (b) subjective element. The objective element is based on the descriptions that are stated in the Kampala amendments on the crime of aggression and the descriptions stated in the United Nation Resolution 3314 (XXIX) of December 14, 1974. These can be divided into seven points:[34]

① The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof.
② Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State.
③ The blockade of the ports or coasts of a State by the armed forces of another State.
④ An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State.
⑤ The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement.
⑥ The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
⑦ The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

The subjective element is based on the criminal intent in the form of participation in the planning of the crime. The intention should be based on the awareness of the crime and the consequence of the aggression act. In this case, the responsibility is not

32 Amendments on the Crime of Aggression to the Rome Statute of the International Criminal Court, June 11, 2010, U.N. RC/Res. 6 of the Review Conference of the Rome Statute, art.8.

33 *Supra* note 31, at 1.

34 *Id.*

only laid on the country, but it also could involve the chief of military or the officials of a country if they are aware of the plan of the crime of aggression.[35]

In relation to the ICC, Article 30 of the Rome Statute also recognizes the subjective element as the "mental element." The mental element refers to the responsibility of a person for the crimes in the jurisdiction of the court if the material element is carried out with intent and knowledge. "Intent" is defined in relation to the conduct and consequences (the actor knows the consequences), while "knowledge" is defined as an awareness of the existence of the crime or the consequences that will arise from it. Both elements must be fulfilled for a crime to be categorized as a crime of aggression under the jurisdiction of the ICC.[36] Although aggression against another country is prohibited under international law by the General Assembly Resolution 2625 (1970), this provision does not eliminate the right of self-defense if threatened by armed attacks from outside. Even the UN allows a country to wage war as a defense mechanism against foreign military attacks. This right to self-defense is often used by a country to use armed measures against another country.[37]

## 4. The Development of Cyberwarfare towards Kinetic Warfare

Cyberwarfare is described as "transnational cyber offences"[38] with anonymity and borderlessness. "Anonymity" means that the Internet protocols allow a person to operate virtually anonymously. For instance, a popular cartoon depicts a dog sitting behind a computer and talking to a cat standing in front. The caption reads, "On the Internet, no one knows you're a dog."[39] The Internet offers valuable opportunities to disguise people and their identities. They can present themselves under false aliases or steal the identity of other unsuspecting and innocent person for the purposes of committing offences.[40] "Borderlessness" means that Internet technology has grown

35 *Supra* note 4, at 69.

36 *Id.*

37 Thalis Noor, *Aggression and Crimes against Peace* [Agresi dan Kejahatan Terhadap Perdamaian], 3(1) Supremasi Hukum. 44 (2014), http://ejournal.uin-suka.ac.id/syariah/Supremasi/article/view/1946.

38 Kartini Eliva, *The Differences between Cyber Attack, Cybercrime and Cyber Warfare,* [Perbedaan Cyber Attack, Cybercrime dan Cyber Warfare], 2(2) Jurist-Diction L. J. 539-54 (2019), https://e-journal.unair.ac.id/JD/issue/view/1092.

39 M. Rogera, *The Psyche of Cybercriminals: A Psycho-Social Perspective*, *in* Ghosh & Turini eds. *supra* note 2, at 217-34.

40 Majid Yar, Cyber Crime and Society 90 (1st ed. 2006).

rapidly and changed almost every aspect of human life. Whereas the Internet used to be accessible only through desktop computers that were permanently located and traceable, wireless devices are now abundant. The advent of cloud computing, where data is stored in private or public third party clouds rather than local computers, further emphasizes the borderless nature of the Internet.[41]

In theory, transnational cyber offenses share three defining features. First, they are deliberate offenses, requiring some willful acts that result in reasonably foreseeable harm. Second, transnational cyber offenses are quintessential cyber offenses, taking advantage of the design characteristics of the Internet as described above. Third, transnational cyber offenses are borderless, like other transnational offenses, such as environmental crime and illicit traffic of drugs and arms. They involve more than one country in their "inception, perpetration and/or direct or indirect effects." Infectious malware and denial-of-service are two common examples of transnational cyber offenses.[42] Table 1 shows a few attacks that happened in the real world in cyberspace.

Table 1: Models of attacks that happened in the world[43]

| No. | Name | Countries | Model of Attack |
|---|---|---|---|
| 1 | Nuremberg | German – WW II | Non-cyber-attack |
| 2 | Tokyo | Japan – WW II | Non-cyber-attack |
| 3 | The Love Bug | Launched in Philippines & appeared in Hongkong, (2000) | Cyber-attack |
| 4 | Titan Rain | USA vs China (2005) | Cyber-attack |
| 5 | | Estonia vs Russia (2007) | Cyber-attack |
| 6 | | Georgia vs Russia (2008) | Cyber-attack |
| 7 | Stuxnet | Iran vs US (2010) | Cyber-attack |
| 8 | | Burma (2010) | Cyber-attack |
| 9 | Flame | Iran vs US (2012) | Cyber-attack |
| | | USA vs China (2013) | Cyber-attack |
| | | USA vs China (2013) | Cyber-attack |
| 10 | | Russian vs Ukraine | Cyber-attack |

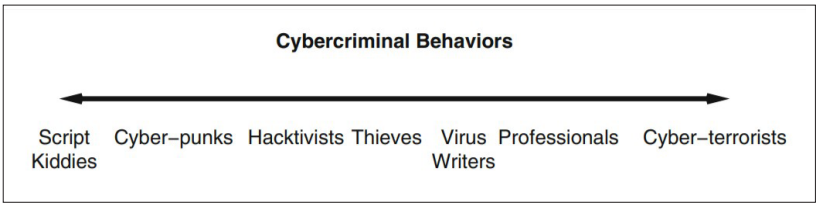
41 A. Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 Yale J. Int'l L. 191-226 (2018).

42 *Id*. at 191-226.

43 *Supra* note 5, at 222.

Table 1 shows that wars are still happening between states in the form of cyber-attacks. Due to technological development, a state can wage war with another state through the Internet. As shown in the figure below, cybercrime can be divided into seven classifications.

Figure 2: The Taxonomy of Cybercriminal Behavior[44]

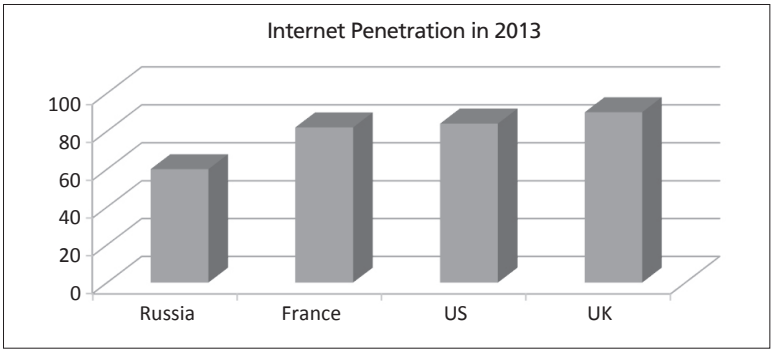



Script Kiddies refer to individuals with limited technical knowledge and abilities; they run precompiled software to create mischief, without truly understanding what the software is accomplishing "under the hood." The second group (Cyber-punks) extends the real-world "punk" into cyberspace. These individuals have a clear disrespect for authority and its symbols, and a disregard for societal norms. The third group is the Hacktivist. The inclusion of a hacktivist category has been somewhat controversial. It is unclear whether the individuals constitute a unique group or are merely individuals from other categories who are simply trying to hide their actions behind semantic camouflage, namely, employing morally neutral terms to disguise aberrant behaviour. The fourth group is the Thief. This category includes criminals. These individuals commit cybercrimes and hide behind labels to deflect their feelings of guilt. The fifth group is the Virus Writer. This category may in fact represent a continuum within a continuum. This category of individuals may include both the technically proficient as well as the "Click Kiddies." The sixth group is the Professional. This category is the most elite of the cybercriminal groups and is often linked with the terms competitive intelligence and white and grey activities. These individuals may be involved in sophisticated swindles or corporate espionage. The seventh group is the Cyber-Terrorist. On the surface, this group's activities mimic those of other categories. They may be part of the military or paramilitary of a nation and are viewed as soldiers or freedom fighters in the new cyberspace battlefield.[45]

44 *Supra* note 39, at 218-19.

45 *Id.* at 218.

Figure 3: Internet Penetration in 2013[46]




In the analysis of the offense-defense theory with respect to Russian cyber capability, Medvedev and Sergei explained that even though Russian internet penetration lags behind those of France (82%), the US (84%), and the UK (90%) in 2013, Russian internet users are more of patriotic users, hackers, and cyber-criminal. These patriotic users, hackers, and cyber-criminals are used as militias that can be mobilized to support the national interest.[47] For example, during the period when the cases of Russia v. Estonia and Georgia occurred, the hacktivists still enjoyed a semi-permissive internet environment, and the rest of Russia's population enjoyed liberal internet experience. During the 2011 parliamentary election, however, the opposition used the Internet to campaign against the regime. Thereafter, the Russia government made changes to the Russian internet architecture, which curtailed Russian internet freedom. However, the curtailment improved its defensiveness and also made cyber-attack from Russia much more difficult. In conclusion, the aggression happened in Russia due to the semi-permissive internet at that time.[48]

Regarding this kind of attack, the weapon is designed to threaten or cause physical, functional, or mental harm to structures, systems, or living things. This general definition is an essential building block for developing a more precise understanding of cyber-weapon and by extension cyber-conflict.[49] The cyber-weapon usage also causes harm like the regular weapon, *e.g.*, the incident at Sayano-Shushenskaya hydroelectric plant in Russia. Keith Alexander, head of America's

46 Sanja Kelly et al., Freedom on the Net 2014: Russia, Freedom on the Net 300, 877 & 858 (2014), https://freedomhouse.org/sites/default/files/resources/Russia.pdf.

47 S. Medvedev, *Offense-Defense Theory Analysis of Russian Cyber Capability*, Naval Postgraduate School NPS Calhoun Institutional Repository (2013), at 37, https://calhoun.nps.edu/handle/10945/45225.

48 *Id.*

49 T. Rid & P. McBurney, *Cyber-Weapons*, 157(1) RUSI J. 6-13 (2012).

National Security Agency as well as the US Cyber Command used the incident in a speech to highlight the potential risks of cyberattacks. Regarding the incident, the cyberattack caused an unusually high vibration, which made the turbine to rip out and caused the transformer to explode.[50]

The cyberattack on Estonia in 2007 opened the world to the threat of cybercrime as one of the modern developments of the crime of aggression. In response to the cyberattack that happened in Estonia, the NATO member countries were encouraged to adopt "NATO Policy on Cyber Defense" in 2011. Finally, at NATO summit in Wales 2014, "NATO Cyber Defense Action Plan" was approved. The cyberattack in Estonia in 2007 formed the basis for one of the most fundamental questions underlying this agreement: "If a member state's communications center is attacked with a missile, you call it an act of war. So, what do you call it if the same installation is disabled with a cyber-attack?" Finally, the NATO secretary-general Fogh Rasmussen after the meeting in Wales said: "Today we declare that cyber defense is part of a collective defense."[51]

This viewpoint from the NATO secretary-general was concretized in the Tallin Manual on the International Law Applicable to Cyber Warfare prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence. This document specifically lays emphasis on cyberattacks, such as the targeting of important infrastructure of a country or cyber-attack targeting enemy command and control system.[52]

A cyberattack can have a great impact on the society. For example, if such an attack occurs in a nuclear facility it could have dire consequences, such as nuclear explosion and other dangerous effects. A cyber-attack can also trigger a kinetic war. As a consequence, cyberattacks can be judged as violating Article 2, Paragraph 4 of the UN Charter.[53]

The cyberattack against Iran in 2010 could be designated as a crime of aggression because it is a kind of war maneuver aiming to make an opponent lose its ability to launch a counterattack. This cyberattack, known as Stuxnet, targeted the nuclear facility in Natanz, which had a factory for enriching uranium in Iran. To enrich uranium, centrifugal motion is needed to control the pressure and temperature precisely. Stuxnet was designed to change the direction of the centrifugal motion

50 *Id.*

51 J. Valuch, T. Gábriš & O. Hamul'ák, *Cyber Attacks, Information Attacks, and Postmodern Warfare,* 10(1) Baltic J. L. & Pol. 63-89 (2017).

52 *Supra* note 7, at 18.

53 G. Lilienthal & N. Ahmad, *Cyber-Attack as Inevitable Kinetic War*, 31(3) Comp. L. & Security Rev. 390-400 (2015).

silently. The Stuxnet virus caused excessive vibration until it was enough to damage the centrifugal motion. This cyberattack caused great material losses.[54]

In the authors' view, the material loss fulfills the condition needed for an action to be categorized as a crime of aggression. The cyberattack carried out by the US against Iran was a war maneuver to weaken Iran's power to respond to any embargo policy carried out by the US. Such activity is referred to in the definition of aggression in the Kampala Amendments; it fulfilled the element of attack by using force in another way, which is against the UN Charter, because it caused material loss due to the damage to an existing Iranian nuclear facility.

It appears that the ICC's jurisdiction needs to be amended in order to cover persons "in a position effectively to exercise control over or to direct the political or military action of a State."[55] By limiting the potential for error (*culpa*) to those with direct political or military control, the so-called "leadership clauses" exclude most transnational cybercrimes. A cybercrime rarely occurs in the context of a tight chain of command. In general, it is committed "by individuals with only weak affiliation with a collective," and collectively may or may not be affiliated with, or sponsored by, a State.[56] In the case of cybercrime as mentioned above, a distributed denial of services (DDoS) attack fulfills the requirements of a leadership clause insofar as the attacker effectively controls the victim state, such as the Russian DDoS case whose attacker crippled the Georgian government's ability to act or communicate with its own country. In many cases, however, limiting the ICC's jurisdiction to high-level state actors prevents regulation of even cyber breaches with major international impact.[57]

# 5. International Law to Reduce the Gap between Cybercrime and Cyber aggression

## A. The UN Charter

In the context of intersection between cybercrimes and the crimes of aggression, cyber-warfare raises its own debate, especially to determine whether cyber acts are

54 *Id.*

55 Rome Statute of the International Criminal Court, 2187 U.N.T.S. 90, entered into force July 1, 2002, art. 8(1).

56 J. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 9(3) Duke L. & Tech. Rev. 1-28 (2010).

57 *Supra* note 40, at 221.

armed attacks for which States have the right to self-defense. Self-defense carried out by a country in response to cyberattacks will be subject to both Article 2, Paragraph 4 and Article 51 of the UN Charter. Acts of self-defense can be carried out by a country according to international law, as mentioned in Article 39, 41, and 42 of the UN Charter. In the context of Article 51, basically, the phrase "...the inherent right of individual or collective self-defense if an armed attack..." is a separate analytic material when connected with cyberattacks. This is because Article 51 emphasizes armed attacks in the sense of traditional understanding, which include traditional weapons and certainly does not include cyber-weapons.[58]

According to Katherine C. Hinkle, however, cyberattacks can be categorized as armed-attacks on the condition that cyber-attacks use armed force weapon.[59] Hinkle's interpretation is based on the extension of the meaning of cyberattacks. This interpretation leads to discussion and debate (gaps) in view that harm caused by cyberattacks remains outside the scope of an armed attack under international law. It has been shown that cyberattacks are very dangerous and have the potential to destroy a country's infrastructure. The intended loss not only is in financial terms, but also involves the security and defense of a country. A concrete example took place in Myanmar in October 2010.[60] The loss caused by the attack reached billions, even trillions of rupiah, whose damage was very devastating, affecting Myanmar's sea-carrying communications cables among others. Then, the question that arises regarding cyberattacks, like that of Myanmar, is whether retaliatory action can be carried out by a country (an injured state) against other countries according to international law.

The answer to this question is a point of contention in international law, because "taking countermeasures" is not necessarily the right action considering that cyber-attacks are new in international legal literature. Retaliation is limited under international law. The intended retaliation is not a "revenge." Article 49 of the ILC's Draft Article on Responsibility for States for Internationally Wrongful Acts has regulated countermeasures "against a State which is responsible for an internationally wrongful act …"[61] As implied in Article 49 of the Draft Article, the purpose of carrying out the "countermeasures" is only to encourage the offending

58 *Id*. at 202.

59 K. Hinkle *Counter Measures in the Cyber Context: One More Thing to Worry About*, 37 Yale J. Int'l L. (online) 11-21 (2010).

60 L. Seltzer, *DDoS Attack on Myanmar Takes the Country Offline*, PC Mag. (Nov. 7, 2010), https://www.pcmag.com/archive/ddos-attack-on-myanmar-takes-the-country-offline-256531.

61 UN International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Nov. 2001, Supp. No. 10 (A/56/10), ch. IV.E.1, art. 49(1).

country to fulfill its obligations regarding its acts that have caused losses to another country. The form of the obligation is "compensation" without the use of force. According to the Draft Article, in carrying out retaliation, two important conditions should be met: "necessity and proportionality." Article 52 of the Draft Article states:

> "Conditions relating to resort to countermeasures:
> 1. Before taking countermeasures, an injured State shall:
>  (a) Call on the responsible State, in accordance with Article 43, to fulfill its obligations under Part Two;
>  (b) Notify the responsible State of any decision to take countermeasures and offer to negotiate with that State.
> 2. Notwithstanding paragraph 1 (b), the injured State may take such urgent countermeasures as are necessary to preserve its rights.
> 3. Countermeasures may not be taken, and if already taken must be suspended without undue delay if:
>  (a) The international wrongful act has ceased; and
>  (b) The dispute is pending before a court or tribunal which has the authority to make decisions binding on the parties."

Article 52 shows the meaning of necessity regarding the need to take retaliatory action for the damages inflicted by another country. Basically, the fundamental problem of cyberattack carried out by a state is the issue of sovereignty. In this case, a rapid response is needed from the disadvantaged country when cyberattack occurs within its territory.[62]

In the case of Estonia and Russia,[63] if the perpetrators of the attack (incursion) are Russians, then the most important thing that must be proven is that Russia directly carried out and/or sponsored the attacks. In the context of customary international law, the perpetrators that directly carried out and/or sponsored the attack are not considered to have carried out unlawful acts; they are categorized as 'illicit' acts.

Responding to the case of Estonia and Russia, NATO immediately revised its cyber defense policy to include the category of cyberattacks within the scope of territorial integrity, independence and security.[64] It is stipulated in Article 4 of the North Atlantic Treaty, which state as follows: "The Parties will consult

62 C. Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights,* 26 Emory Int'l L. Rev. 825-919 (2012).

63 J. Andress & S. Winterfield, Cyber Warfare: Techniques, Tactics and Tools for Security 13 (2d ed. 2014).

64 J. Valo, *Cyber Attacks and the Use of Force in International Law* 92 (Master's Thesis at the Faculty of Law, University of Helsinki, 2014), https://helda.helsinki.fi/bitstream/handle/10138/42701/Cyber%20Attacks%20and%20the%20Use%20of%20Force%20in%20International%20Law.pdf?sequence=2.

together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened." The expansion of the meaning and scope of Article 4 of the North Atlantic Treaty is a strategic step taken by NATO to anticipate the danger of cyberattacks that could occur within the scope of the North Atlantic defense, particularly in the concept of state sovereignty.[65]

## B. The Law of Armed Conflict

Traditionally, armed conflict is governed by the Geneva Conventions, The Hague Conventions, and a collection of relevant treaties and laws. These rules are binding on those who have signed, ratified, or acceded to them. Although not every country is a party to the conventions or agreements, the rules referred to in these treaties should be obeyed by every country in the context of customary international law to avoid grave acts or activities during the war.[66] Therefore, the treaties and conventions serve as deterrence against cruelty that often occurs in war (atrocities of war), and are meant to set the correct procedure for war.

In relation to war crimes that occur in the intersection of the cybercrime and aggression, there is need to expand the scope of the crime of aggression by including cyber warfare that has all the attributes of war into the domain of international conventions in existence. The approach that should be taken is to adopt or interpret legal events that occur and adapt them to existing legal rules regarding armed conflict. If an attack is carried out by an individual or a small group of people, it is certainly different from the concept of armed force according to the two conventions mentioned above. This causes controversy regarding cybercrime. Therefore, some concepts of war are explained to support the arguments within the framework of *bellum iustum* (just war theory). *Bellum iustum* basically provides an argumentation at the level of armed conflict (war): beginning a war (*ius ad bellum*-the right to wage war), during war (*ius in belo*-conduct during war) and ending a war (*ius post bellum* - ending a war).[67]

### 1. Jus in Bello

*Ius in bello* emphasizes how the country should act during war. It has two principles, i.e., the principle of 'distinction' and the principle of 'proportionality.' First, the

65 *Id*. at 94.

66 J. Andress, The Basics of Information Security: Understanding the Fundamentals of Indosec in Theory and Practice 228 (2d ed. 2014).

67 *Supra* note 40, at 201.

principle of 'distinction' specifically stipulates that war should not be aimed directly at civilians and neutral parties. In conventional warfare that has occurred so far, this principle is hard to apply. In comparison, it will be even more difficult to apply this principle to cyberattacks due to the mixed military and civil society systems and networks. So, it will be also hard to identify the war targets as referred to in this principle. Also, the technological systems and networks on which cyberattacks are based, are complex. This is compounded by the nature of cyberspace, where a target may be affected even though s/he is not in the country being attacked. Under this condition, it will be very difficult to apply this principle to cyberattacks. The failure of identification of the target, as in conventional warfare, results in violations of the rules of war that have been established both by the Geneva Conventions and The Hague Conventions.

Second, the principle of 'proportionality' states that the effect of the attack should correspond to the target being attacked. If the target is the military, then the intended attack should not injure or affect other targets, such as civil society, non-combatants, and neutral parties.[68] In cyberattacks, a fundamental problem is the difficulty in detecting and measuring the effects of a cyberattack. This is due to the nature of cyberattacks; i.e. the effects of some can be measured, while others cannot. For the cases of attack related to denial of services (DoS) or DDoS system, the effect can be measured. Samples that can show the effect are available in the case of Estonia and Russia, so that the effect of losses in the banking sector can be measured. In another case, however, such as Stuxnet (Iran v. the US), the effect is difficult to predict because the target of the attack is Iran's nuclear center, where the effect cannot be predicted and even imagined.[69]

### 2. Ius Post Bellum: Justice after War

*Ius post bellum* explains how to end and handle the aftermath of a war. In this case, there are three main principles: (1) seeking lasting peace; (2) holding morally-culpable individuals accountable; and (3) extracting reparations. First, the principle of "seeking lasting peace" views peace as an output that should be achieved. This principle in relation to cyber warfare is difficult to be applied because the scope of cyber warfare is not yet covered by the war conventions such as The Hague and Geneva Conventions. The perpetrators of attacks in this case therefore are

[68] Emanuela-Chiara Gillard, *Proportionality in the Conduct of Hostilities: The Incidental Harm Side of the Assessment* 6-8 (The Royal Institute of International Affairs, Research Paper, Dec. 2018), https://www.chathamhouse.org/sites/default/files/publications/research/2018-12-10-proportionality-conduct-hostilities-incidental-harm-gillard-final.pdf.

[69] *Supra* note 63, at. 48.

qualified as non-state actors (hackers, hacktivists, and organizations), in which they are qualified as unlawful combatants.[70] Second, the principle of "holding morally-culpable individuals accountable" refers to assuming offenders responsible for their actions. Due to the anonymous nature of cyber warfare, the perpetrators are difficult to prosecute since it is difficult to identify individuals.[71] Third, the principle of "extracting reparations" relates to reparations (compensations) for both individual and state actors. These reparations aim to compensate for the material and immaterial losses caused by the perpetrators.[72] However, it is realized that the damaged caused by a cyberattack is more difficult to be assessed, particular in determining the number of affected systems, the affected data value, and the effects on untested systems and society.[73]

## 6. Conclusion

Technology is developing rapidly, and if it is not properly controlled, a new form of armed attacks would threaten the peace and stability of the international community. A cyberattack is a new international crime. Since the late 1980s, cyberattacks have evolved to use ICT innovations to commit cybercrimes. In recent years, notable developments, such as the cyberattack in Estonia in 2007 allegedly carried out by Russia and the Operation Olympic Games (Stuxnet) involving the US and Iran in 2010, have sparked the need to seriously consider monitoring internet-based crimes across the world. These crimes have also caused material loss to the affected countries. Cyberattack is considered as a form of war maneuver in order to defeat the opponent and destroying their ability to counterattack. It has also been categorized as a crime of aggression, as stipulated in the Kampala Amendment. It also violates Article 2, Paragraph 4 of the UN Charter.

Responding to the increase of cyberattacks, every country including Indonesia needs to strengthen its defenses against cyberattacks that could happen in future. This could be done by developing domestic defense policy and international convention to deal with cybercrime. Governments should also encourage research

70 J. Sigholm, *Non-State Actors in Cyberspace*, 4(1) J. Military Stud. 61-71 (2016).

71 *Supra* note 39.

72 M. Cisneros, *Cyber Warfare: Jus Post Bellum*, 40 (Master's Thesis at the Naval Post Graduate School, 2015), https://calhoun.nps.edu/handle/10945/45169.

73 *Id.*

and development in cyber technology and support all domestic efforts aimed at strengthening domestic cyber defense against cybercrime. The absence of international norms to regulate cybercrime in the form of cyber war could trigger kinetic warfare. Therefore, the global community should cooperate to achieve an international agreement regarding cyber warfare in order to tackle technological development and challenges.

Received: August 1, 2020
Modified: October 30, 2020
Accepted: November 15, 2020