Cyber Attack - The Burden of International Crime Proof: Obstacles and Challenges

Maskun[1], Naswar[2], Achmad[3], Hasbi Assidiq[4], Armelia Safira[4], Siti Nurhalima Lubis[4]
[1]International Law Department, [2]Constitutional Law Department, [3]Civil Law Department, [4]Assistant Researcher Faculty of Law, Hasanuddin University, Makassar - Indonesia
Email : maskunlawschool@yahoo.co.id/maskunmaskun31@gmail.com

Abstract--Cyber-attack is a negative impact of the development of technology in the modernization era. This attack utilizes technology to attack telecommunications networks. According to international law, cyber-attacks can be categorized as international crimes. Cyber-attacks took place in Estonia and Iran resulted in material losses, violations of sovereignty, disruption of public facilities and threatening the security of a country, and can even be considered as the initial signal of other international crimes that could threaten world peace and security. However, until now, burden of proof of cyber-attack has still obstacles and challenges in the international world. The focus of the research is to find out international legal arrangements related to burden of proof of cyber-attacks as international crimes by using technology as a tool in realizing crimes. To get it, very important to explore some law and cases. The type of the research is normative legal research by using legal materials such as some law and case. The data are then analyzed qualitatively. The results show that there are challenges in proving of cyber-attacks, namely the nature of borderless and anonymous attacks, the difficulty in determining the place and time of the attack, variations in attack techniques, and political power.

Keywords- Burden a Proof; Cyber-attack; International Crime; International Law.

I. INTRODUCTION

Globalization promotes the development of information technologies around the world. This development creates a new world order based on modernization in all aspects of life. When human activity is compared with pre-globalization, it is still conventional and limited by distance, time, and technology, although these limitations are not a problem in today's world. The majority of developments in information technology is closely related to internet use, namely the *Internet of Thing (IoT)*. Furthermore, most human, business, and event management activities, are separately converted into cyberspace.

The term cyberspace first appeared in 1984 and was used by William Gibson. Cyberspace is an Internet movement resulting in a stable, populated, easy to navigate platform in country size or even larger landscape. In cyberspace, users communicate by disguising their identity, without being limited by regional boundaries, and even across countries [1].

Technology promotes the creation of global information and communication networks as an integral part of modern government methods, business, education, and economic operation [2]. However, this development brought both positive and negative impacts. Currently, crime has also transformed into the realm of cyberspace. Meanwhile, cyber-attack harms the development of information technology in this modernized era. It utilizes computer technology development, especially the internet, as a tool to attack telecommunications networks and even a country's defense system.

The cyber-attack occurred in Estonia in 2007, disrupted public services, and caused material losses. The attack, which was reportedly performed by Russians, paralyzed the government and trade networks of the Estonian Government. Approximately one million government computers have been infected and distributed in the form of *Distributed Oenialof Servise (DDoS) attacks* [3]. The most recent case occurred in Iran in early 2020. One of the weapons conflicts between Iran and the United States was triggered by allegations of a previous cyber-attack. The latest attack uses the Drone MQ Reaper 9, operated by the US military, as well as with various weapons and powerful visual sensors [4]. This attack occurred at Baghdad Airport and killed eight people, including Qasem Soleimani Mayor General.

In 2010, Iran also faced a cyber-attack on the nuclear facilities in Natanz, and approximately 60,000 computers were infected by a virus called Stuxnet [5]. The target of Iran's uranium enrichment infrastructure is certainly very dangerous, which not only violates the sovereignty but also has dangerous effects on the security of human civilization [6]. Cyber-attacks kill nuclear centrifuges, air defense systems, and electricity networks, posing a serious threat to national security [7].

II. PROBLEMS

This study attempts to present a normative review in order to prove cyber-attacks as a crime, as well as investigating the regulations and challenges in international law by including an analysis of cases.

III. RESEARCH METHOD

The type of the research is normative legal research by using legal materials such as some law and cases to answer the burden of proof of the cyber-attacks. The data then analyzed qualitatively.

IV. DISCUSSION

International Crime

The international world has declared its readiness to maintain peace and security through consensus on the fundamental goals of the United Nations (UN). However, there have been actions by the international community that destroy and violate this agreement. These entail committing international crimes since it is the study object of criminal law on a global scale. International Criminal Law was originally introduced and developed by legal experts from Europe such as Friederich Meili in 1910 (Switzerland), Georg Schwarzenberger in 1950 (Germany), Gerhard Mueller in 1965 (Germany), JP Froncois in 1967, Rolling in 1979 (Netherlands), Van Bemmelen in 1979 (Netherlands), then followed by legal experts from the United States such as Edmund Wise in 1965 and Cherif Bassiouni in 1986 (United States).

Theoretically, M. Cherif Bassiouni divides the international crime level into three. First, as part of *jus cogens,* related to peace and security as well as fundamental human values [8]. Eleven crimes occupy the top hierarchy as international crimes, such as:

a. *Aggression.*
b. *Genocide.*
c. *Crimes against humanity.*
d. *War crimes*
e. *Unlawful possession or use or emplacement of weapons.*
f. *Theft of nuclear materials.*
g. *Mercenaries.*
h. *Apartheid.*
i. *Slavery and slave related practices.*
j. *Torture and other forms of cruel, inhuman, or degrading treatment.*
k. *Unlawful human experimentation.*

Second, as international delicts, it relates with the protected interests, which include more than victims and losses incurred from one country. There are thirteen crimes included in international delicts, such as:

a. *Piracy.*
b. *Aircraft hijacking and unlawful acts against international air safety.*
c. *Unlawful acts against the safety of maritime navigation and safety of platforms on the high seas.*
d. *Threat and use of force against internationally protected persons.*
e. *Crimes against United Nations and associated personnel.*
f. *Taking of civilian hostages.*
g. *Unlawful use of the mail.*
h. *Attacks with explosives.*
i. *Financing of terrorism.*
j. *Unlawful traffic in drugs and related drug offenses.*
k. *Organized crime*
l. *Destruction and/or theft of national treasures.*
m. *Unlawful acts against certain internationally protected elements of the environment.*

Third, as an international infraction. In normative criminal law, international infrastructure is not included in the category of crime and delicts. There are only four crimes included in International Infraction, such as:

a. *International traffic in obscene materials.*
b. *Falsification and counterfeiting.*
c. *Unlawful interference with submarine cable.*
d. *Bribery of foreign public officials*.

Furthermore, according to Bassiouni, three elements need to be fulfilled before posing as an international crime [9]. These elements are as follows:

a. *The international element* includes direct and indirect threats to world peace and destabilizing human feelings.
b. *The transnational element* includes the impact on more than one country, on citizens, as well as the facilities, infrastructure, and methods used to transcend the territorial boundaries of a nation.
c. *The need element* includes the demand for cooperation between countries to carry out countermeasures.

Cyber Attack

Before discussing cyber-attacks further, the general explanation of its existence needs to be known. It is a crime in cyberspace and generally defined as "*any activity in which computers or networks are a tool, a target or a place of conducting its criminal exercise"* [10]. In the Convention on Cybercrime, the activities were classified as follows: *The criminalization of conduct, ranging from illegal access, data, and systems interference to computer-related fraud and child pornography* [11] Cyber-crime continues to develop significantly to become a potential threat in the security sector since it is the most serious challenge of the 21st century [12]. Currently, this

crime extends to the territory of the military and resilience of a country, for example, the development of militaria crime, the use of space and non-kinetic weapons on the ground, maritime, or air platforms used to influence satellite or sensor operations without physical contact [13].

The encounter between cybercrime and the military is considered a contemporary crime. This was influenced by time, and the use of weapons or tools. The crime focuses on the existence of an attack using cyber technology during operation. This is a type of offensive maneuver used by countries, individuals, groups, or organizations that target computer information systems, infrastructure, networks, and/or personal devices, with various malicious actions. These are usually from anonymous sources, which steal, modify, or destroy specified targets by hacking vulnerable systems [14]. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Rule 92 defines cyber-attacks, "*as an offensive or defensive operation that is reasonably expected to cause injury or death to persons or damage or destroy objects"*. [15]

An attack is often associated with destruction or damage. In the case of cyber-attacks, there is no formal definition of destruction in international humanitarian law [16]. In a battle, the destruction of an object is definitely due to an attack. However, this is now widely doubted since attacks are not always synonymous with destruction, which is physically and directly visible. In conducting cyber-attacks, for example, the use of weapons does not necessarily cause damage and destruction immediately, but the opposite may occur relating to human life.

Referring to Tallin Manual Rule 103, *Cyber Weapon* was defined as "*a means of warfare used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that result in the consequences required for qualification of a cyber operation as an attack.*"[15]. Some experts agreed that an attack becomes armed when confronted with humanitarian law. According to Jean Pictet, armed attacks are related to sufficient duration and intensity. However, many experts responded that the duration and intensity as a benchmark are still not sufficient. Furthermore, Michael N. Schimitt stated that there are six criteria to qualify as an attack [17];

1. *Severity*, was seen from the scope and intensity of the attack, such as the number of casualties caused, the area affected and the number of objects damaged.
2. *Immediacy*, it was seen from the attack duration, such as the duration of the effects,
3. *Directness,* it was seen from the wound or damage caused,
4. *Invasiveness*, it was seen from the locus of the attack, it entails its country border crossing process,
5. *Measurability*, as a result of the attack by interpreting and measuring,
6. *Presumptive Legitimacy* was seen from the assessment and legitimacy of the attack based on the practice of States, and the norms which exist in the international community. Also, an act obtains legitimacy under the law when accepted by the international community.

There are several types of cyber-attacks commonly used, such as [18]:

1. *DoS (Denial of Service),* this type aims to hinder or disable the service work. Therefore, authorized or interested users are not allowed to use the service. DoS attacks target the bandwidth and connections of a network to accomplish its mission [19]. These repeated attacks performed to prove shut down of the site. An intense attack caused complete paralysis of the website.

2. *Malware,* this attack is conducted using a software with high danger level. When the software has successfully entered the device used, it can quickly destroy the system and steal important data. Usually, this malicious attack enters the device when uploading a file prior to installation. This makes Malware one of the most dangerous forms of a cyber-attack. Several types are commonly known to attack computer systems such as Viruses, Worms, Trojan Horses, Backdoors, Keystroke Loggers, rootkits, or Spyware.

3. *Phishing attacks devices and steals the relevant information on the system*. Usually, the data stolen is important, such as PIN, password, and username.

4. *Credential Reuse*, this type of cyber attack occurs when a similar or identical username, password, and PIN are present in multiple accounts. It becomes an easy target, and the concept of this attack is to reuse various important information previously obtained.

5. *SQL Injection*, in practice, hackers manually enter code in the form of marks such as dots, single quotes, and dashes. When the code is successful, all data in a database will be deleted and it is used by hackers to perform other actions, which may harm the company.

6. *Cross-Site Scripting (XSS)*, this type of attack attempts to damage or take over a particular website, especially in government agencies or companies in the banking and

financial sectors. Hackers obtain information such as usernames, passwords, and PINs by entering HTML or client script code on a site.

7. *Man in the Middle,* this type of attack puts the hacker in the middle of a communication between two people. During communication, various important information exchanged between them are stolen by the mediating hacker.

Sample case

Estonia - Russia

Estonia as a former Soviet Union state has a very close historical background with Russia. In 2007, the Estonian Government announced that it will move the Bronze of Soldier statue, which was built as a liberation symbol of the Soviet Liberation of Estonia from Nazi Germany. Therefore, this statue has a historical relationship with Russia and Estonia as a unit within the Soviet Union. This policy triggered severe riots by ethnic Russians in Estonia in the region that did not accept the policy [20].

The conflict eventually spread after cyber-attacks from April 27 to May 18, 2007, for 22 days, attacking various servers for public facilities owned by the government, parliament, police, banks, internet service providers, online media, and many businesses. Cyber-attacks were conducted through computers in various countries, such as Egypt, Russia, and the United States, and were used against servers and routers in Estonia with email and ping spam as well as datagram on the user protocols.

The cyber-attack was performed in the form of a DDoS. Websites that normally handled 1000 hits per day crashed receiving 2000 per second. Furthermore, online banking, credit card, and ATM transactions were stalled, while government websites became difficult to access due to damage, and online media were unable to upload news. This is exacerbated by the very high level of internet usage in Estonia, where 60% of residents were internet users, and 97% of banking transactions were already using electronic media [21]. The cyber-attack caused various public services to not function properly, costs and the human life continuity was disrupted.

Iran- AS

The history of conflict between Iran and the United States (US) occurred in the pre and post-Iran Islamic revolution in 1978. At the end of the Shah Reza Pahlavi regime in 1978, the president fled with the assistance of the US government. The elected government then detains US citizens at their embassy in Tehran. This relationship worsened after the US shot down an Iranian plane in 1988. In 2002, the US censured Iran as the axis of world crime and accused the country of developing a nuclear weapons program secretly [20]. To ensure Iran does not develop nuclear weapons, the US made various efforts, both diplomatically, through negotiations and intelligence operations. The Olympic Games program or commonly referred to as Stuxnet is part of an effort to disrupt Iran's nuclear development program.

Stuxnet is a virus that attacked Iran's nuclear infrastructure in Natanz. According to Stefano Mele, Stuxnet can be categorized as a Cyber Weapon, on the assumption that it refers to the context of its use in conflict situations between countries, such as Iran and the US. The use of Stuxnet was specifically aimed at attacking Iran's nuclear infrastructure. Cyber operations were performed using viruses developed with sophisticated information and communication technology [21]. Stuxnet was designed to change this centrifugal motion silently until it was quickly increased before slowing down. The result of this virus attack caused excessive vibrations until the centrifuge was damaged. Therefore, the Cyber-attack caused severe material losses to Iran as a nation [22].

The Case of Qassim Solaimani

On January 3, 2020, the United States proceeded to another maneuver by adopting key measures to assassinate the commander of the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), General Qasem Soleimani, one of the most influential generals in Iran. This plan was conducted by the US with a cyber-attack using emasculated drones. Based on an official statement from the US Defense Department, this action was considered a "Defensive Action", because Qasem Soleimani was responsible for the deaths of hundreds of US people and members of the coalition forces. Furthermore, the coalition forces that executed the blockade agreements went to the US embassy in Baghdad, and actively developed plans to attack US diplomats and soldiers in Iraq and across the Middle East region [23].

In this attack, the US military operated MQ Reaper 9 drone at a speed of 14 hours when loaded with ammunition, weapons, and powerful visual sensors to hit the target. This happened at Baghdad Airport and succeeded in killing eight people, including General Qasem Soleimani. This heightened tensions between the United States and Iran [4]. This situation also led the international world to start measuring the threat to global security.

Cyber Attack as an International Crime

Based on the representation and the elements of criminal activities, one can construct that cyber attacks are international crimes. The description of the related elements can be constructed as follows:

a. International elements, defined as the existence of threats to world peace, either directly or indirectly. In this context, cyber-attacks have the potential to threaten world peace. The cases in Estonia and Iran show that they disrupt a country's public service s ystem which is a vital facility designated for more than one balance, such as the banking sector and cross-border trade. In the case of Stuxnet (2010), the attack becomes very dangerous because a person and/or country can easily control any activities. Ralph Lagner described Stuxnet as a cyber weapon that was used to attack the entire Iranian nuclear program [5]. This weapon will be very easy to use today considering the massive development of information and technology. Therefore, the occurrence of cyber-attacks can directly or indirectly have the potential to threaten world peace and security.

b. Transnational element, which means that the scope of the cyber-attack is cross-border. As previously explained, this attack utilizes cyberspace as a domain or place to become borderless. According to Hata, the attack showed that the sovereignty of the country is very easy to penetrate since its traditional power was weakened [24]. Furthermore, when referring to the "Convention Against Transnational Organized Crime", it can be categorized that cyber-attack is a transnational crime. Article 3 of the convention categorizes a transnational crime as follows: *For paragraph 1 in this article, an offense is transnational when*:

i. *It is committed in more than one State*
ii. *It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another;*
iii. *It is committed in one State but involves an organized criminal group that engages in criminal activities for more than one; or*
iv. *It is committed in one State but has substantial effects in another.*

d. ***The need element*** means that international cooperation between countries is required in the process of prosecuting cybercriminals, within an international court framework. In this context, an interpenetration aspect is needed to describe the urgency of cooperation with the international treaty law formula. Also, the alternative solution in law enforcement against transnational crimes is based on the belief of all countries participating in the convention. According to the convention, law enforcement against these crimes cannot be conducted optimally and successfully on the assumption that only one country is committed. This is a new strategy by applying the principle, "No Safe Haven", which is aimed at narrowing the space for transnational criminal activities [26].

Evidence Analysis of Cyber Attack Cases

Since the development of Information and Communication Technology (ICT), human beings have been introduced to cyber space as a new dimension or space. As a new dimension, ICT has potential to create a conflict as a negative impact of it [26]. Theoretically, there is fifth spatial dimension of ICT and it is very different in comparison to the above enumerated examples. It has a global reach, which blurs the physical boundaries between countries (*borderless*), and allows for operating regardless of the political system, with an extremely wide range of actors –from individuals, through various groupings, up to states [27].

Cyber-attack can be qualified as contemporary crime to use technology as a tool to create crime in cyberspace. However, the most important problems on it is there is no international legal instrument universally regarding burden a proof of cyber-attacks that has connection to responsibility of attack. Article 14 and 21 Convention on Cybercrime only allows for the creation of procedural regulations and international cooperation related to investigations and the gathering of evidence in cyber-crime cases. The explanation regarding the possibility of international cooperation is regulated in Article 23 of this convention, namely "*General principles relating to international co-operation The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence*".

In general, this convention gives authority to the country's domestic law to create legal instruments in the form of domestic law and cooperation agreements in dealing with cyber-crimes, including variations of cyber-attack techniques. This is the basis for proving efforts against cyber-attacks that occurred within the European Union region, for example in the case of Estonia 2007. This cooperation can be established only when we have reached a consensus from the parties involved. Meanwhile, for the making of procedural rules and domestic regulations of a country based on the interests and wishes of that country.

Proving is needed at the investigation stage. In proving cyber-attacks, there are obstacles and challenges. **First**, the nature of the borderless

and anonymous attacks. Cyber-attacks are carried out through the dimensions of cyber space without limitations on area and area, so that cyber-attacks are borderless. This poses a challenge in proving the origin of the attack. In the Estonian case as many as 1-2 million previously infected 'bots' in 175 jurisdictions were set up to launch coordinated attacks against Estonian targets by flooding websites with data. However, at the research stage, Estonia could only prove that an Estonian student of Russian origin, Dmitri Galushkevich, was arrested, indicted and convicted for targeting political party websites its scale shows that many people are likely to be involved in planning and implementation but not can be proven. Dmitri can be proved as an attacker because he did it inside Estonia, so that tracking is easier. The nature of anonymity is possible in cyber-attacks. This is also done by the attacker as a tactic so that it is not easily traced for proof.

Second, it is difficult to determine the place and time of the attack. The difficulty in determining the place and time of attack is also related to the borderless and anonymous nature of the attack. The use of technology in cyber-attacks makes these attacks more sophisticated. Technological developments can disguise time and place. This challenge occurred in the case of Estonia, of the total number of attacks that Estonia received, only one attack was able to prove by the Estonian Court regarding its place and time. This is because most of the malicious network traffic data cannot be obtained, thus not allowing investigators to chase down the large number of people who carried out the attack [28].

Third, variations in attack techniques. Several types of cyber-attacks techniques have been explained, including DoS (Denial of Service), Malware, Phishing attacks devices and steals the relevant information on the system. Credential Reuse, SQL Injection, Cross-Site Scripting (XSS) and Man in the Middle. However, driven by technological developments, currently cyber-attacks can have a relationship with armed militarian activities that are indicated as acts of aggression. A variation of this attack technique can be seen in the Iran-United States case. The use of cyber as a weapon can be seen from the use of drone technology to attack Baghdad air bases. According to Tallinn Manual 2.0 On the International Law Applicable To Cyber Operations Rule 68 related to the Prohibition of the threat or use of force, which stated that "*A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations, is unlawful"* [15].

In the Kampala Amendment Article 8 bis paragraph 1 of the Rome Statute defined crime of aggression as the planning, preparation, initiation or execution, by a person in a position that can effectively exercise control on the political or military action of a State, and from an act of aggression, its character, gravity, and scale, constitutes a manifest violation on the Charter of the United Nations. Meanwhile, acts of aggression are "*the use of armed force by a State against the sovereignty, territorial integrity or political independence of another, or in any other manner inconsistent with the Charter of the United Nations*". Based on the explanation above, the potential of a cyber attack, which threatens territorial sovereignty and political independence of the United Nations, can be categorized as an act against the law. Tallinn Manual Rule 69 further explains the use of force definition as "*A cyber activity which constitutes a use of force when its scale and effects are comparable to non-cyber operations*". This new variation of attack technique is now also a challenge for parties who want to prove cyber-attacks, a humanitarian law review is required in it.

Fourth, political power. The two cases analyzed in this study were based on political conflict. This conflict is also a challenge in terms of accounting for cyber-attacks. There is a tendency to hinder proof, such as what Russia did by not accepting the "a formal investigation assistance request" to the Russian Supreme Procurator in May of 2007, which Estonia put forward can be considered evidence of the use of political force to protect itself. The element of political power is also found in the Iran-United States case. According to Miko Ardiyanto, cyber-attacks on Iran's nuclear infrastructure by the US can be categorized as an intervention against the Iranian state sovereignty. The American pretext that these actions are seen as a form of self-defense using the lessons of the pre-emptive military strike to protect against the threat of a possible nuclear attack from Iran cannot be justified. This is based on the absence of armed attack activities conducted by Iran against the US. Therefore, the element of "When an Armed Attack Occurs" as stipulated in Article 51 of the UN Charter was not fulfilled. In the opinion, a UN expert, Agnes Callamard, the results of the investigation into the killing of Qasem Soleimani by the United States with drones was illegal and contrary to international law related to the *Conduct of Hostilities.*

Apart from that, on the use cases drone attack action is only justified in response to a real threat. Information to avoid this threat is considered very vague when judged from the context of the US not showing evidence to necessitate the killing of Soleimani [28]. The existence of casualties in a cyber-attack is categorized as an aggressive crime. This is based on the fulfillment of action elements officially by the US following the statements of President Trump that conducted cyber-attacks using Drone MQ-9 Reaper, remotely controlled, and used to kill the military commander of Iran's IRGC-QF, General Qasem Soleimani, and entourage [29]. This

assassination of a military General violated Iranian sovereignty. The difficulty in proving cyber-attacks related to the Iran-US case this time is due to the hindrance of testifying the responsibility of the state and the elements of protective measures. These cannot be separated from the political power of the two countries.

V. CONCLUSION

Cyber-attacks have a negative impact on the development of information technology in the age of modernization. This attack is an international crime with the potential to cause material loss, sovereignty violation, disruption of public facilities, and threatening the country security, as well as disrupt global peace, especially when it is related to the military sector. Due to the difficulty in proving. There are obstacles and challenges in proving, namely the nature of borderless and anonymous attacks, the difficulty of determining the place and time of attack, variations in attack techniques and political power. Proving becomes more difficult because there is no universal international legal instrument that regulates it.

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

[1] Murray Andrew D, *The Regulation of Cyberspace, Control in the Online Environment*, London: Routledge-Cavendish, 2007.
[2] Purna Cita Nugraha, "Konsepsi Kedaulatan Negara dalam Borderless Space", Jurnal Opinio Juris, Volume 13, 2013.
[3] Katherina C. Hinkle, "Counter measures in the Cyber Context: One More Thing to Worry About", The Yale Journal of International Law Online, Volume 17 No. 4, 2011.
[4] E. Prima, "Bunuh Soleimani, Drone MQ-9 Reaper AS Paling Ditakuti di Dunia", Tempo, 2020. [Online]. Available: https://tekno.tempo.co/read/1294958/bunuh-soleimani-drone-mq-9-reaper-as-paling-ditakuti-di-dunia/full&view=ok. [Accessed: 14- Jan- 2020].
[5] James P. Farwell and Rafal Rohonzmskl, "Stuxnet and the Future of Cyber War", Journal Survial, Volume 53, 2011.
[6] Maskun, Alma Manuputty, S.M. Noor, Juajir Sumardi, "Kedudukan Hukum Cyber Crime dalam Perkembangan Hukum Internasional Kontemporer", Jurnal Masalah-Masalah Hukum, Volume 42 No. 4, 2013.
[7] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, "The Law of Cyber-Attack", California Law Review, Volume 100 No. 4, 2012.
[8] Eddy O.S. Hianej, *Pengantar Hukum Pidana lntemasional*, Jakarta; Airlangga, 2009.
[9] Romli Atmasasmita, *Pengantar Hukum Pidana lnternasional*, Bandung: Refika Aditama, page. 58, 2003.
[10] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response of Telecommunicatoin Development Sector*, Telecommunication Development Sector; International Telecomunication Union (ITU), 2012.
[11] "The Budapest Convention on Cybercrime: International Criminal Law and the use of Treaties | Lexology", Lexology.com, 2020. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=4220b287-ac07-4a33-a711-bee235721d9f. [Accessed: 29- Jul- 2020].
[12] Paul Meyer, "Norms of Responsible State Behaviour in Cyberspace", The International Library of Ethics, Law and Technology, Volume 21, 2020.
[13] Todd Harrison, *International Perspectives on Space Weapon,* The Center for Strategic and International Studies (CSIS), 2020.
[14] Tom. C. W. Lin, "Financial Weapon of War", Minnesota Law Review, Volume 100, 2016.
[15] M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
[16] Nobuo Hayashi, "Requirement of Military Necessity in International Humanitarian Law and International Criminal Law", Boston University International Law Journal, Volume 28, 2010.
[17] Jeffrey Carr, *Inside Cyber Warfare*, California: O'Reilly Media, Inc., 2010.
[18] G. Ong, "7 Jenis Cyber Attack yang Mengancam IT Perusahaan dan Solusinya – Mitra Teleinformatika Perkasa", Mtp.co.id, 2020. [Online]. Available: https://mtp.co.id/project/7-jenis-cyber-attack-yang-mengancam-it-perusahaan-dan-solusinya/. [Accessed: 25- Oct- 2020].
[19] Cse.wustl.edu, 2020. [Online]. Available: https://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar.pdf. [Accessed: 27- Oct- 2020].

[20] Mohan B. Gazula, *Cyber Warfare Conflict Analysis and Case Studies,* Cybersecurity Interdisciplinary Systems Laboratory (CISL), Cambridge: Massachusetts Institute of Technology, 2017.
[21] Stephen Herzog, "Ten Years after the Estonian Cyberattacks Defense and Adaptation in the Age of Digital Insecurity", Georgetown Journal of International Affairs Fall, Volume XVIII (3) (III), 2017.
[22] Gary Lilienthal and Nehaluddin Ahmad, "Cyber attack as Invitable Kinetic War", The Computer Law and Security Review XXXI. 3, 2015.
[23] Clayton Thomas et.al, "U.S Killing of Qasem Soleimani: Frequently Asked Questions", Congressional Research Service, 2020.
[24] Hata, *Hukum lntemasional: Sejarah dan Perkembangan hingga Pasca Perang Dingin,* Malang: Setara Press, 2012.
[25] *Pusham.uii.ac.id*, 2020. [Online]. Available: https://pusham.uii.ac.id/upl/article/id_Hukum%20Pidana%20Internasional.pdf. [Accessed: 25- Oct- 2020].
[26] Cf. Michaela Melková and Tomáš Sokol, *Cyber Space as the New Dimension of the National Security*, Banska Bystrica: Belianum, 2015.
[27] Rain Ottis, "Analysis of the 2007 Cyber Attack Against Estonia from the Information Warfare Perspective", Published in Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth in 2008, Reading: Academic Publishing Limited, 2018.
[28] "The Killing of Qassim Suleimani Was Unlawful, Says U.N. Expert", Nytimes.com, 2020. [Online]. Available: https://www.nytimes.com/2020/07/09/world/middleeast/qassim-suleimani-killing-unlawful.html. [Accessed: 9- -Jul 2020].
[29] "The Killing of Gen. Qassim Suleimani: What We Know Since the U.S. Airstrike", Nytimes.com, 2020. [Online]. Available: https://www.nytimes.com/2020/01/03/world/middleeast/iranian-general-qassem-soleimani-killed.html. [Accessed: 3- Jan- 2020].