Law of War and Its Applicability in the Area of Cyber World

Zhuo Chen[1, *]

[1]*Chuo University, Tokyo, Japan*
[*]*Corresponding author. Email: a20.jghj@g.chuo-u.ac.jp*

ABSTRACT
Nowadays, computer science and technology developed rapidly and plays an crucial role of our daily life. The attack which occurred in cyberspace from a state or non-state group could make serious negative effect on huge amount of people’s lives and even threaten the national security since the popularization of Internet in all aspects of financial, political, and also strongly related to national security. For example, a cyber-attack on national financial system could not only causes huge economic losses, but also harmful to the overall trust in the system it destroyed. Though a huge amount of cyber incidents aimed at economic crime, it’s necessary for each state be awareness of the threat from cyber space based on the growing technological means and changing form of cyber-attack. Then, the debate of application of relevant of the law of war in the field of cyber-attacks appeared to the international stage. The purpose of this article is to conduct an exploratory qualitative analysis of the application of relevant of the wartime law in the realm of cyber-attacks; to gain an fundamental understanding of the attack, and to find counteractive methods and strategies each states have institutionalized to alleviate future cyber-attacks. The origin could be various such as the case study of happened cyber-attack and the Tallinn Manual which was written by some experts on the study of Internet. This study could also applies to cyber conflicts and cyber warfare. The article will raise concerns about areas where the law of armed conflicts remained unclear and imperfect in addressing this new threat emanating from the cyber world.

Keywords: *cyber-attack, cyber warfare, law of wartime, cyber space*

1. INTRODUCTION

Whether the state which has been the target of cyber-attacks has the inherent right to do self-defense based on UN Charter Article 51 became a heat issue internationally in which indicated the importance of this issue. In order to have a multiple understanding and further study of this issue, it is necessary to give cyber-attack and definition and what the practical effect of cyber-attacks could have in real war. A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim ’ s network. Furthermore, in what time a cyber-attack become an “armed attack” is also the point to be focused on this article because it means how some of the law of armed conflict principles may apply. In the last decades, the growing consensus on the recognize of cyber-attack to be an “armed attack” developed quickly [1].

Basically, the term cyber-attacks are used to describe a variety of harmful activities taking place in the cyberspace. Though, under the debate of whether the same principle of self-defense could be applied to cyber-attacks, the most essential part is in what time a cyber-attack could be confirmed as an armed attack. Then, the specific state could take positive actions to do the self-defense instead of taking proportional and non-forcible countermeasures. Secondly, the attribution of cyber-attacks also become essential for state to have a practical target to fight back. In addition, there are several differences between personal attack and the attack attributed to another state. The feature of anonymity of cyber-attack makes the trace back process extremely difficult because attackers can hide their identities easily. The high possibility of operators from lots of different countries which were under different legal jurisdiction also brings problem and force the international society to have a standard to regulate those kinds of attacks.

This article will also have an overview of several key developments in the law governing cyber-attacks. In the season of Spring, Estonia was under a cyber-attack action from Russia lasting a period of 22 days. During this period of time, Estonia suffered from temporary degradation and loss of service in area of commercial and government servers due to the advanced e-Estonia system. In 1991, Estonia restored its independence as a sovereign nation, defeating the Soviet occupation and oppression [2]. Following independence, the first Prime Minister Mart Laar helped push the country through a period of modernization, establishing the foundation needed to bring the country into the digital age. Since the development and expansion of computer and network infrastructure in Estonia, the system of e-Estonia was formed in 1998 with the function of which allows medical personnel immediate access to patient medical records and also the tax could be payed on e-Estonia. Since 2002 about 1.2 million of these credit-card size personal identification documents have been issued allowing citizens to digitally identify themselves and sign documents or actions. Those series of convenient functions lead to the widely use of e-Estonia in rural region. Therefore, the cyber-attack on Estonia's network by Russia has significant impact on Estonia's public service which arouse controversy of whether it could be confirmed as "armed attack". Based on the case of Estonia, it will be easier to understand the urgency of demarcate the line between cyber-attack and armed conflict.

2. PROBLEM OF ATTRIBUTION

Cyberlaws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices.

The increase in Internet traffic has led to a higher proportion of legal issues worldwide. Because cyberlaws vary by jurisdiction and country, enforcement is challenging, and restitution ranges from fines to imprisonment.

2.1. Different types of cyber-attack

Cyber-attacks hit businesses every day. Former Cisco CEO John Chambers once said, "There are two types of companies: those that have been hacked, and those who don't yet know they have been hacked." According to the Cisco Annual Cybersecurity Report, the total volume of events has increased almost fourfold between January 2016 and October 2017.

There are many different types of cyber-attacks which could be divided by different purpose. In the case of cyber-attacks between states, the purpose of attackers are always being destructive. For example, Russian government use the type of Distributed Denial of Service attack which unlike attacks that are designed to enable the attacker to gain or increase access, DDoS doesn't provide benefits for attackers directly. Another type of cyber-attack is aiming to gain the information which contains trade secrets, password and confidential information in military zone. Attackers are available to use multi-attacks to achieve the purpose and it's difficult to trace back because attackers are located in different geographic locations which means attackers are always located in different states. For example, Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks. These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations [3].

In addition, Malware is a specialized type of application that has the ability to perform a variety of malicious tasks. Some strains of malware are designed by attackers to create persistent access to an Internet network, some are designed to spy on the user in order to gain credentials or other valuable information, while some are simply designed to cause disruption. Some kinds of malware are produced to extort the victim in some way. Perhaps the most notable form of malware is Ransomware-a program designed to encrypt the victim's files and then ask them to pay a ransom in order to get the decryption key. In the case of Sony hack in 2014, this method was used to attack an American corporation.

2.2. Attribution

To activate the right of self-defense, which could also mean to have an specific target whom self-defense action will be taken, is important in the counteractive strategies. Attribution is thus essential but is a very demanding and blurry exercise in the context of conventional attacks and even more so in the case of cyber-attcaks, based on the multi-aspects of methods of each attack. It's the lack of government resources in the situation of responding to a blurry cyber-attack which could be from an individual or organization. In addition, the conservative and the insufficiency of traditional passive defenses led to the outcomes which make governments pay extra cost. The mechanism of activating the positive self-defense action relies to the effective attribution process. However, the traditional techniques of attribution are always associated with positive cyber actions which called "hack back".

As there isn't any universally accepted standards to define an clear line between active cyber defense and passive cyber defense, the process of attribution become problematic. The urgency and importance of attribution during the wartime are definitely differ with the usual cyber intrusions which take personal companies as targets. Thus, the standard of define "hack back" action as an active cyber defense should be more relax.

Otherwise the difficulties of attribution and the strict standard of the confirmation of whether the attack is dangerous or not will let the state lose the control of the situation [4]. The outcome could be destructive as modern society heavily relies on the Internet and there are also giant amounts of data concerned with national security.

In order to obtain relief from a cyber-intruder - whether by technical means of mitigating or disrupting the attack or by non-technical means like litigation, diplomatic engagement, military force, or otherwise - there must first be some knowledge of the attacker's identity or location, even if it is only an intermediate location (Wheeler & Larsen, 2003). The "attribution problem" is caused by the architecture of the Internet itself, complex governance and administrative matters, and destruction of evidence. What degree of certainty is afforded by current means of attribution? Will better attribution increase the ability to influence attackers? Which active defense countermeasures are viable means of improving the accuracy of attribution 9 through private-sector or individual contribution? What is the proper framework for the private sector to engage with the government for the purposes of implementing, de-conflicting, and reporting the use of active defense countermeasures? The Institute for Security Technology Studies at Dartmouth University researches and investigates cyberattack issues facing law enforcement investigations and focuses on the continuous development of IP tracing, data analysis, real-time interception and national data sharing. These questions are worth to be discussed though it's difficult to find out all the answers in this one article.

3. APPLICATION OF WARTIME LAW IN CYBER WORLD

The principle which called proportionality prohibits attacks against military objectives which are "expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated". In other words, the principle of proportionality seeks to limit damage caused by military operations by requiring that the effects of the means and methods of warfare used must not be disproportionate to the military advantage sought. On one hand, the state which want to do self-defense will meet the legal challenge under this principle [5]. On the other hand, Proportionality also prohibits attacks that are expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated. The applicability of this principle in cyber world could be evaluated. In this situation, the standard to confirm the proper use of this principle in cyber world should be rethink. Proportionality will require an assessment of the effects of cyber weapons on military and civilian personnel or infrastructure, the physical destruction that cyber-attack may occurs, and also the potential effects of such an attack on civilian objects, including civilian computers that may be linked to computers that are considered to be lawful military objects. Despite this urgency of cyber-attacks, a unified international cyber-warfare agreement which adequately applies the current laws of proportionality principle, does not exist. Consequently, governments are always facing the difficulties to apply a jus in bello proportionality analysis to these potentially offensive cyber-strikes [6]. The principle of proportionality is a basic element and for testing the legitimacy of the reason for launching an armed conflict and the legitimacy of the use of force (jus in bello). Unfortunately, the utilize of the principle of proportionality has some practical problem when solving the disputes and conflicts between states because there are some difficulties in the quantification of the standard of the principle of proportionality. State practice shows that the legitimacy of countries resorting to the reasons for armed conflict affects their cognition as to what degree of force should be used to achieve the purpose of armed conflict during an armed conflict. Which means the reason for advocating resorting to force the strength and urgency of legitimacy often determine the type and intensity of the use of force, as well as the overall consideration of comprehensive military interests and the purpose of war. Therefore, the legitimacy and legality of the use of force has a more or less subtle influence on what kind of force should be used. Although there are still some basic rules to regulate each states, it is still necessary to determine whether it conforms to the norms of on a case-by-case basis. Regardless of whether the use of force or the initiation of an armed conflict is contrary to the principle of proportionality, the military intention adopted by it shall not be legitimized because the reason for asserting the use of force is self-defense or other justifiable reasons, which means violate proportionality in hostilities principle, also constitutes a war crime. Based on the situation above, a state will meet the legal test of proportionality when it limits the use of self-defense to defeat the ongoing attack or deter a future attack.

The Sony hack which happened in 2014 is related to the first instance of the U.S. government publicly blaming a foreign government for the reason of cyber-attack against an American corporation [7]. The Guardians of Peace claimed credit for unleashing the Nov.24 wiper malware attack against Sony Pictures that reportedly compromised 6,000 employees' computers and landline phones, after which attackers leaked high-quality digital copies of unreleased movies, as same as sensitive and embarrassing corporate data [8].

Following this cyber-attack, G.O.P. said it would stop the leaks if the studio promised to never release "The

Interview", which features a plot to assassinate North Korean leader. The FBI officially attributed the attack to North Korea and President Obama followed with a speech stating that the U.S. would "respond proportionally ... at a time and place that we choose". Although U.S. officials said the attack against Sony was of a "destructive" nature, it did not meet the traditional definition of a "destructive attack" under international law, which involves death, injury, or damage or destruction of physical objects, such as computers. The attribution process also has lots of disputes. The FBI states that technical analysis of the data-deletion malware used in the attack revealed links to other malware the FBI had linked to North Korean hackers. There are some similarities are found in specific lines of code, encryption algorithms, data-deletion methods and compromised networks [9]. Initially, the process of attribution was criticized by security researchers for its shortage of unambiguous information. In addition, security firm Norse proposed an alternative theory in which the hack was the work of insiders unrelated with North Korea. Although there are some who still doubt its legitimacy, the accuracy of FBI's attribution was confirmed by other private sector actors. Shortly after the confirmation of attacker, U.S. government compulsory sanctions on a group of North Korean individuals and three entities connected with the North Korean government. The U.S. government emphasize the fight back action would follow the principle of proportionality. And the legitimacy of the action would be located in the aspects of the violation of U.S. sovereignty because the aim of hackers could be seen as the beginning of imposing censorship in the United States [10].

4. CONCLUSION

In this article, the author intended to give the current cyber-attack a proper standard which makes the discussion more persuadable and reasonable. The clear standard will be helpful not only in problem solving of the dispute on the confirmation of armed attack but also promoting the accuracy of the concepts which have been discussed in this article such as the apply of wartime law principle in definitive situation which is the attack occured in cyber space. Then, through the case of Estonia's cyber-attack, the importance for governments to recognize the dangerousness of cyber-attack has been emphasized and it forces the international society to have an universal consensus when facing the risk of cyber wartime. Naturally, the proper use of some principles of wartime law became the key elements for solving the problem in cyberspace. Although it's almost impossible to have a universal standard and use the acceptable standard to constraint each state, the discussion of the characteristics of cyber-attack and the related analysis could be helpful in the future deter of the attack.

The structure of this article is formed of two main parts which are the attribution problem and the use of the principle of proportionality. And it's all based on one premise that is the inherent right of use of force when a state is under an armed attack. In what situation could a cyber-attack become an armed attack is necessary to be discussed under the legal frame of wartime law, especially the UN Charter Article 51. Also, the attempt of using the logic of wartime law principle is a bold but reasonable thinking process.

REFERENCES

[1] Davis, George Dewey, III. The Digital Fog of Cyber: Case Study of the 2007 Cyber Attack on Estonia, Northcentral University. ProQuest Dissertations Publishing, 2017. 10618770.

[2] Tian lipin, examining the legitimacy of the reasons and means of armed conflict by the principle of proportionality, military law special issue, military law special issue, 201310 (59:5), 180-192 pages

[3] Hodgkinson, Sandra L, The international lawyer; Crossing the Line: The law of war and cyber engagement--Applying the existing body of law to this new national security threat; Chicago Vol, Iss.3, (2018); 613-628.

[4] Nicholas Tsagourias, Cyber-attacks, self-defense and the problem of attribution, Journal of Conflict&Security Law© Oxford University Press 2012

[5] Kristjan Vassil, Estonian e-Government Ecosystem Foundation, applications, outcomes, Institute of Government and Politics University of Tartu

[6] HENSEY A. FENTON III, PROPORTIONALITY AND ITS APPLICABILITY IN THE REALM OF CYBER-ATTACKS, Copyright © 2019 Hensey A. Fenton III

[7] Kevin A. Elliott, ACTIVE CYBER DEFENSE AND ATTRIBUTION IN CYBER ATTACKS, Published by ProQuest LLC (2018). Copyright of the Dissertation is held by the Author.

[8] Hathaway O A, Crootof R , Levitz P , et al. The Law of Cyber-Attack[J]. Social Science Electronic Publishing, 2012, 100(4):817-885.

[9] Blank L R. Cyberwar versus Cyber Attack: the Role of Rhetoric in the Application of Law to Activities in Cyberspace[J]. Social Science Electronic Publishing, 2014.

[10] Tromp J. Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-attacks. ©2005-2020, Small Wars Journal publishing, Thu, 01/28/2016 - 4:30am