Proceedings of the 3rd International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/69/20240165

The Cyber Attack in the Use of Force

Yanna Li[1,a,*]

[1]*Law School, Shenzhen University, Shenzhen, 518052, China*
a. 1677647581@qq.com
**corresponding author*

Abstract: It is controversial whether cyber attacks can constitute the use of force, and it is also difficult to reduce cyber attacks in the use of force. This article will start from arguing the definition of using force, then discuss how can cyber attacks be interpreted as a form of using force and how to regulate cyber attacks from three orientations, which is a cyber attack that attributable to individuals, attributable to organizations, and attributable to countries. Finally, this article will focus on finding out a recommendation on how to identify a cyber attack with the one that can attributed to a country with the purpose of reducing the cyber attack in the use of force, that is, reverse the burden of proof in the investigation of an international cyber attack. This method aims at increasing the possibility of bearing state responsibility. And this article will explore the feasibility and improvement path of this method in order to make the idea more practical.

Keywords: Cyber Attack, International Law, Use of force: State Responsibility, Burden of Proof.

1. Introduction

With the continuous development of network technology and the increasing dependence on networks, the harm of network attacks is becoming greater and greater, ranging from causing a cyber war that endangers peace and stability to invading an ordinary computer, which can cause varying degrees of damage to people and property. The rules of using force in international law are inadequate to reduce the cyber attacks in the use of force, we can solve this question in three situations which are cyber attacks that can be attributed to individuals, organizations and countries. This article will classify and discuss the objects of responsibility for international cyber attacks, and explore solutions to reduce the use of cyber attacks in the use of force in each situation. But it is still inadequate.

In order to combat cyber attacks, international law should put forward higher requirements for dealing with the use of force in cyber attacks. The difficulty in solving this problem lies in the fact that many cyber attack incidents are difficult to attribute to the state, and cyber attacks, due to their secrecy and opacity, are extremely easy to evade responsibility, leading countries to be quite willing to use cyber attacks to achieve their military or political goals. This article will put forward a solution aim at this problem, which is revers the burden of proof in investigation, and will focus on the feasibility of such special regulations and attempt to address potential challenges that may arise.

The first part of this paper is an introduction of the question and the background. The second part is the literature review about the argument of the definition of using force, which is a fundamental question of the research. The third part is the hypothesis and case study analysis, there are three cases:

DOI: 10.54254/2753-7048/69/20240165

the Estonia Cyber War, the Lazarus Group and the Stuxnet Cyber War, which represent the cyber attack attributed to individuals, organizations and countries. Some existing system will be proposed in this part. The fourth part is recommendation. In this part, the specific implementation of reversing the burden of proof in international cyber attack incidents will be proposed. The last part is the conclusion which will summarize this paper.

2. Literature Review

Whether a cyber attack can be regarded as a use of force of international law is widely concerned by many scholars. The first question we have to answer is: What is a use of force? [1]Schmitt emphasized that "What is a use of force?" and "To whom does the prohibition apply?" both have had a significant impact on the legitimacy of cyber operation, which did not exist when countries adopted the United Nations Charter in 1945. [2]Waxman mentioned that Article 2(4)'s view to the use of force looks at its purpose and general effect, which is it prohibits coercion.

No matter there is a cyber attack or a armed attack, it's merely a form. So if we want to find out if adopting cyber attacks to achieve a military goal or a political goal is a use of force, it is actually meaningless. What is the most important is the result of the action. Is it cause a damage? Is it poses a threat to international security and state sovereignty?

As [3]Jamal et al. stated, regardless of the means of threat used by one party, international law enforcement agencies should determine whether there is a violation or threat to the international stability order, or even an act of aggression, based on hostile intent.

de Souza Dias, T. and Sagoo R. also said, "Crucially, international law is technology neutral. This means that its rules and principles apply to old and new technologies." [4] It is not important whether the method used in the attack is conventional or unconventional. The most important factor in whether it constitutes the use of force is the damage caused by the attack, that is, whether it poses a threat to international security and national sovereignty.

Schmitt proposes that whether a cyber attack constitutes military force depends on various characteristic factors of military attacks, including immediacy, severity, measurability, directness, presumptive legitimacy, and invasiveness[5]. A cyber attack that causes repairable physical damage has no long-term consequences and does not cause harm to humans, therefore it is not considered a use of force or armed attack. [6]

Therefore, in the view of [7] Gill and Tibori-Szabó, if a cyber attack does not cause direct personal injury, but is clearly aimed at preventing the state from performing its basic functions for a long period of time and cannot be easily reversed, and can be attributed to states or organized armed groups, it may indeed constitute a use of force. If the damage caused by an attack is severe enough to result in casualties and property damage, then it certainly constitutes a military attack that can be regulated through the use of force rules. But if the damage only causes non physical harmful consequences, further definition is needed. [7].

3. Methodology

This paper will use the case study analysis as well as comparison analysis to confirm the hypotheses, and due to the complexity of the research subject, quantitative analysis will not be considered.

4. Hypotheses & Case Study Analysis

This paper tests 3 hypotheses as potential answers to my research question, they are, H1: The international cyber attacks can be attributed to individuals, organizations and countries; H2: The international cyber attacks that can be attributable to individuals and organizations can be regulated

DOI: 10.54254/2753-7048/69/20240165

by current rules, but countries cannot be attributed to an international cyber attack; H3: The countries can be attributed to an international cyber attack by reversing the burden of proof.

The case study analysis will present three typical cases of international cyber attacks, each corresponding to the international cyber attacks that can be attributed to three types of objects: individuals, organizations, and countries. And the hypotheses will be tested by the case study analysis.

4.1. Estonian Cyber War

Estonia faced a large-scale cyber attack at the end of April 2007, which websites of banks, government departments, Congress and media suffered varying degrees of attacks. The attacks are widespread and deep, this incident has attracted widespread attention from the international military community, and military experts generally believe that it is the first national level cyber war. Estonia believes that it's Russia implement this action and Russia's initiation of this cyber war aims to express the dissatisfaction with Estonia's accession to NATO and the anger over Estonia's transfer of the Bronze Soldier, which is a memorial commemorating the Soviet liberation of Estonia from the Nazis. This cyber war is a threat to Estonia's sovereignty and political independence [8]. However, the exact perpetrators are hard to find, because they are mainly some individuals and they even don't know each other. Experts generally believe that Russia and "hacker activists" among Russian expatriates around the world jointly carried out these attacks. [9] But Many investigative experts, including American investigators, were unable to find conclusive evidence that the Russian government was involved in this operation. This is a case that a cyber attack is attributable to individuals.

If a case is found to be attributable to an individual after investigation, the accountability of the individuals can be pursued through the following methods:

4.1.1. Through international criminal law

The Hague Convention stipulates the principle of extradition or prosecution, and many domestic laws also regulate cybersecurity crimes. If a cyber attack cannot be attributed to a country or an organization, but can be traced back to certain individuals, the perpetrator can be held criminally responsible based on the criminal laws of their country of nationality, location, and victim country, as well as bilateral or multilateral extradition treaties.

4.1.2. Through International Criminal Court (ICC)

If an international cyber attack can be classified as genocide, endangering humanity, war, or aggression, while countries and organizations cannot be held accountable, then individuals who have been identified as perpetrators can be held accountable under the provisions of genocide, crimes against humanity, war crimes, and aggression. The specific approach is for the International Criminal Court to hear and make judgments on cases transferred by contracting states and the United Nations Security Council in accordance with the provisions of the Rome Statute, and then hand them over to the contracting states for execution.

Furthermore, whether an international cyber attack constitutes one of the four crimes under the jurisdiction of the International Criminal Court should be determined based on the provisions of the Rome Statute regarding the constituent elements of these four crimes.

4.2. The Lazarus Group

Lazarus Group is a well-known APT (Advanced Persistent Threat) organization with a wide range of activities, including infiltration attacks on countries such as South Korea and the United States, as well as attacks on global financial institutions. The organization's earliest activities can be traced back

DOI: 10.54254/2753-7048/69/20240165

to 2009, when it used DDoS technology to attack South Korean government websites. Since its first appearance in 2007, Lazarus Group has been engaged in large-scale cyber espionage activities, including attacks on South Korean government websites, Sony Corporation websites, and intrusions into Bangladeshi Bank. In 2014, Sony Pictures suffered an famous cyber attack by Lazarus Group because of sony's release of a comedy, which is about an assassination of the president of North Korean, Kim Jong un. [10] This is a case that the cyber attacks are attributable to organization.

If a case is found to be attributable to an organization after investigation, we need to first determine whether these organizations are funded and encouraged by the state, then identify the primary person in charge of the organization. Then classify and regulate them.

4.2.1. To the primary person in charge of the organization

Refer to the above discussion about individuals.

4.2.2. To the organization that may constitute a terrorist organization

There is no unified standard or neutral organization for identifying terrorism in international law, and the identification of terrorism is usually done by domestic law.[11] However, if an organization is widely recognized as a terrorist organization by multiple countries, then countries can strike the terrorist organization through friendly consultation, strengthened international cooperation, or military means authorized by the Security Council.

Lazarus Group is widely regarded as a terrorist organization and has faced global resistance. However, it is still uncertain whether the organization can be considered sponsored by the North Korean government.

4.3. Stuxnet Cyber War

A network worm called "Stuxnet" attacked the Iranian nuclear facility located in Natanz in June 2010, leading to the self explosion of Iran's nuclear centrifuges. Although this news has not been officially acknowledged, many media outlets and officials have hinted or acknowledged that the incident was orchestrated by the United States and Israel.[12] This incident has dealt a serious blow to Iran's nuclear development process and significantly reduced its military capabilities, which can be considered a serious harm to Iran's sovereignty and political independence. [6] And this is a case of a cyber attack that is attributable to countries for the obvious military goal of the US and Israel which is destroying Iran's nuclear development.

We can take the following measures to respond to international cyber attacks carried out by a country or funded by a country:

4.3.1. From the perspective of preventive measures

If there are some pre signed treaties or conventions between the countries concerned, these countries can hold accountable for international cybersecurity incidents based on the provisions of treaties or conventions, as well as United Nations documents and its subordinate agencies. The Ad Committee on Cyber Crime and the Global Digital Compact and OEWG exist in the United Nations, apart from these, the Oxford Process on International Law Protections in Cyberspace and the Tallinn Manuals on International Law Applicable to Cyber Operations also play an important role in governing the cyberspace. [4]

However, treaties and conventions on cyber attacks in current international law are far from sufficient to effectively regulate cyber attacks. For this, we can refer to the Convention on the Prohibition of Bacterial (Biological) and Toxic Weapons and Convention on the Prohibition of the

DOI: 10.54254/2753-7048/69/20240165

Development, Production, Storage and Use of Chemical Weapons and on Their Destruction to regulate cyber attacks.As [13]Picker stated, technology itself is the subject of law. It is wise for policy makers to refer to the Weapons of Mass Destruction Act when considering new regulations to regulate cyber attacks.

4.3.2. From the perspective of remedial measures

4.3.2.1. Hold state responsibility

If an international cyber attack committed or sponsored by a country against another country constitutes the use of force, it naturally constitutes a wrongful act of the state, and should be regulated by the International Law Commission's articles on state responsibility, including but not limited to the responsibility of continuing duty of performance, cessation and non-repetition, and reparation. It is also necessary to compensate the injured country in accordance with the provisions of the relevant compensation chapter.

4.3.2.2. Exercise the right of self-defense

If a cyber attack can be classified as the use of force, it may lead to the exercise of the right of self-defense. The exercise of the right of self-defense, as a private remedy for the victim country, can be used to protect the victim country as soon as possible when the tortious act occurs, minimize the losses of the victim country as much as possible, and impose appropriate punishment on the victim country. However, in order to reduce the abuse of the right of self-defense, the exercise of the right of self-defense in the use of force must follow the principle of proportionality to prevent the unreasonable use of the right of self-defense from causing more serious damage to peace. As [14] Gardam, Gail stated, “Proportionality as an element of self-defense is uncontroversial.” It is obvious that if a country receives a cyber attack on its military system from another country, it cannot have a self-defense with a nuclear weapon attack.

4.3.2.3. File a lawsuit to the International Court of Justice

The International Court of Justice operates in accordance with the Statute of the International Court of Justice and its own Rules of Court, resolving legal disputes submitted to it by States in accordance with international law. The International Court of Justice operates in accordance with the Statute of the International Court of Justice and its own Rules of Court, resolving legal disputes submitted to it by States in accordance with international law. When an international cyber attack occurs, the parties involved can submit the dispute to the International Court of Justice for review, but given that the Court's compulsory jurisdiction is not recognized by many contracting states, the effectiveness of this approach may not be high.

4.3.2.4. Seeking international assistance

As a form of public remedies, when the victim country is unable to resolve a cyber attack on its own, it can seek assistance from the international community. In addition, in order to raise the threshold for violating international law in the use of force, efforts should be made to increase the sanctions against the offending country, especially the great powers.

DOI: 10.54254/2753-7048/69/20240165

4.4. Cross-case analysis & comparison analysis

4.4.1. Cross-case analysis

Both these three cases have some commonalities, including but not limited to the damages they caused, the potential culpable objects are countries and both of them cannot be held accountable to the relevant countries (Table 1).

Table 1: Comparison of three cases

Cases	The consequence	Potential Attribution Subject's purpose	The result
Estonian Cyber War	Critical infrastructure destroyed and the country cannot function normally	Russia's political purpose	Russia cannot be attributed
The Lazarus Group	Sony Corporation has been unable to operate normally for a long time	The North Korea's political purpose	The North Korea cannot be attributed
Stuxnet Cyber War	Iran's nuclear facilities destroyed	The UK and Israel's military purpose	The UK and Israel cannot be attributed

If it can be determined that cyber attacks can be attributed to the state, in order to address the above cases, United Nations General Assembly Resolution 56/83, which states that the responsibility of states for internationally wrongful acts, can be applied. But from this chart we can notice that both these three cases cannot attribute an international cyber attack to a country, this is due to the difficulty of investigation and proof. To solve this problem, the rules of investigation and proof should be changed. This will be discussed in the fifth part of this paper.

4.4.2. Comparison analysis

As mentioned earlier, cyber attack is just a form of using force, and its essence is more similar to a weapon. We can compare and analyze it with the regulations on biological weapons, chemical weapons, and other weapons of mass destruction.

First of all, both the biological weapons, chemical weapons and other weapons of mass destruction are capable of devastating strikes. The international law has made prohibitive provisions on this because these weapons can bring uncontrollable harmful consequences. The same goes for cyber attacks. So for the international cyber attacks, a treaty or a convention that similar to the Convention on the Prohibition of Bacterial (Biological) and Toxic Weapons and Convention on the Prohibition of the Development, Production, Storage and Use of Chemical Weapons.

Some counter arguments might consider that some types of cyber attacks have less damage than some weapons of mass destruction, but these types of cyber attacks are unqualified to constitute a use of force, thus will be excluded from the scope of this paper.

5. Recommendation

5.1. Background and the proposal of recommendation

The paper believes that special provisions can be made to the burden of proof during the investigation process by the International Law Commission to prevent the state from evading its responsibility, that

DOI: 10.54254/2753-7048/69/20240165

is, by reversing the burden of proof, allowing the highly suspected state to prove its innocence during the investigation process. If the state cannot prove its innocence, it is presumed that it has committed a cyber attack. But this recommendation has a lot to improve until it turns doable.

The provisions on the reversal of the burden of proof in various countries' laws are very cautious, as it involves a balance between public and private interests. As the statement of [15] Hamer, "... a balance is sought between the defendant's right not to be wrongly convicted and the community's broader interest in law enforcement."

5.2. Reasons for using the reversal of burden of proof

The adopting of the reversal of the burden of proof usually happens in domestic law to balance individual rights and public interests. The reason for applying it to international law is similar, that is, to balance the national interests of the countries concerned and higher international interests such as international peace and security.

A major challenge to the current rules of the use of force in cyber attacks is that compared to traditional use of force, cyber activities have the characteristics of anonymity and confidentiality. Even if we can trace the source of the attack based on IP addresses, attackers can easily use fake or encrypted addresses to conceal the true source of the attack, making cyber attacks more difficult to trace and attribute. Because cyber attacks are easy to evade responsibility, they can easily become an effective way for countries to achieve their military or political goals.

Taking the Estonian cyber war as an example, even though many pieces of evidence point directly to the possibility that the Russian government led the cyber attack, investigative experts still find it difficult to find ironclad evidence of the Russian government's involvement or funding of the cyber attack. The Russian side only denies the Kremlin's involvement in this incident without bearing any burden of proof, while the Estonian side, which has suffered damage, has to invest a lot of resources to investigate the cause of this incident. For an internationally wrongful or criminal act, the burden of proof borne by both parties is completely unequal and cannot reflect fairness.

5.3. Improvement suggestions

5.3.1. The premise of reversing the burden of proof

Although the author believes that reversing the burden of proof in international cyber attacks is feasible, it does not mean that any suspected country must bear the responsibility of proving its innocence.

Firstly, the cyber attack should constitute a use of force, that is, it poses a threat to international Security and State Sovereignty. Secondly, the prerequisite for assuming the responsibility of self-proving innocence must be through investigation, a country being highly suspected of involvement in the incident. That is to say, the reversal of the burden of proof must have a relatively strict pre procedure to initiate. Last but not least, investigators must provide certain evidence as a clue pointing to the suspicious country, which does not need to be conclusive evidence, but needs to be able to raise reasonable doubts about the pointed country. These prerequisite procedures aim to prevent major powers from using other countries as scapegoats or maliciously framing other countries in order to achieve their political goals.

Taking the Stuxnet cyber war as an example, if Iran believes that the United States and Israel led the cyber war, it must first provide strong evidence pointing to the United States and Israel as clues to initiate an investigation. The United States and Israel can provide certain evidence to prove that they are not involved in the incident. If they cannot prove their innocence, they are presumed to be involved in the incident and bear corresponding national responsibilities, such as compensation and restoration of the original state.

DOI: 10.54254/2753-7048/69/20240165

5.3.2. The burden of proof for the suspected perpetrator country

In an international cyber attack, the party initiating the investigation first presents evidence as a clue, and then the suspected perpetrator country proves its innocence. At this time, the burden of proof for the suspected perpetrator country should be based on the preponderance rule (or a requirement of proof beyond a reasonable doubt). "... In contrast, if there is little prospect of chilling beneficial activity and the pertinent harmful acts impose extreme damage and might readily be deterred, a low threshold should be employed." [16] He mentioned a "Chilling Effect" to find out if a case should use the preponderance rule or optimal evidence threshold. This reminds us that when using the reversal of the burden of proof in international law, we should pay attention to the degree of the burden of proof that can be considered as fulfilling the burden of proof for proving innocence.

That is, the burden of proof for the suspected perpetrator country is a proof beyond a reasonable doubt. The reason of the adopting of the preponderance rule is obvious. The IP addresses and physical addresses used in modern cyber attacks can come from all over the world, and the victim country can suspect any country for its own political purposes, making many countries possible targets of suspicion. In addition, it is quite difficult to prove that a country has not sponsored any hacker organizations or substantial participate in a certain cyber attack, so its burden of proof only needs to exclude the reasonable doubt. But if it cannot finish the burden of proof to exclude the reasonable doubt, it has to undertake the unfavorable legal consequences of being presumed to be related to the cyber attack.

5.3.3. Protection for weak countries

Although all countries should be treated equally, weak countries usually do not have the same capabilities and resources as large countries, which makes it more difficult for them to prove their innocence. So they are more likely to be used as scapegoats by great powers. Therefore, when weak countries are trapped in the dilemma of providing evidence, more capable countries, especially major powers, should provide international assistance to them. This can not only help innocent weak countries prove their innocence, but also enhance the international reputation of great powers, thus achieving a win-win situation.

6. Conclusion

We can regulate international cyber attacks that constitute the use of force from the perspectives of individuals, organizations, and countries. However, regulating international cyber attacks that constitute physical use from the perspectives of individuals, organizations, and countries is a remedial measure to reduce the use of force. Its preventive effect is minimal because cyber attacks are more difficult to prove and attribute to the state compared to traditional use of force. Therefore, the method of reversing the burden of proof can be used to increase the possibility of state responsibility from the source for international cyber attacks that constitute the use of force.

References

[1] *Michael N.Schmitt (2010) "Cyber Operations in International Law:The Use of Force." Collective Security,Self-Defense,and armed conflicts,Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy: 679-685.*

[2] *Matthew C. Waxman (2011) "Cyber Attacks as 'force'under UN Charter Article 2(4)." Int'l L. Stud, 87: 43-57.*

[3] *Jamal Awwad Alkharman, Sonia Abed ALhamed Drawsheh, Majid Mohammad Al-Khataybeh, Zein Bassam Bani Younes, Najwa Abdel Hamid Darawsheh & Hanaadi Alrashdan(2024)"Cyber Attacks and its Implication to National security:The Need for International Law Enforcement. " Pakistan Journal of Criminology, 16(3)(July-September): 851-864.*

[4] de Souza Dias, T. and Sagoo R. (2024) "AI Governance in the Age of Uncertainty: International Law as a Starting Point", (January 2), https//Justsecurity.org.
[5] Michael N. Schmitt (1999) "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." COLUIBIA JOURNAL OF TRANSNATIONAL LAW, 37:885, 914-915.
[6] James P. Farwell & Rafal Rohozinski (2011) "Stuxnet and the Future of Cyber War." 53:1, 23-40, DOI: 10.1080/00396338.2011.555586.
[7] Gill, Terry D. and Kinga Tibori-Szabó (2023) "New Technologies of Warfare and the Law on the Use of Force." Chapter. In The Use of Force and the International Legal System, 228(46) (07 December), https//doi.org/10.1017/9781009407342.01 Published online by Cambridge University Press.
[8] Herzog, Stephen (2011) "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." Journal of Strategic Security, 4(2): 49-60.
[9] Michael Connell and Sarah Vogler (2017) "Russia's Approach to Cyber Warfare."CNA, (24 March).
[10] Joshua Park (2021) "THE LAZARUS GROUP."Harvard International Review, 42(2)(SPRING):34-39.
[11] Todd Sandler and Khusrav Gaibulloev(2012)"Determinants of the Demise of Terrorist Organizations." US Department of Homeland Security, (Nov.) http://www.utdallas.edu/~tms063000/website/.
[12] Emily Haslam (2000) "Information Warfare: Technological Changes and International Law." Journal of Conflict and Security Law, 5(2): 157-175.
[13] Colin B. Picker (2001) "A View from 40, 000 Feet: International Law and the Invisible Hand of Technology. "Cardozo Law Review, 23(1) (November): 149-220.
[14] Gardam, Judith Gail (1993) "Proportionality and force in international law." American Journal of International Law, 87(3): 391-413.
[15] David Hamer (2007) "The Presumption of Innocence and Reverse Burdens: A Balancing Act."Cambridge Law Journal, 66(1)(March):142-171.
[16] Kaplow, Louis (2012) "Burden of proof." The Yale Law Journal, 121: 738-859.