Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/19/20231391

Cyber-Attack Regulation: Issues and Advances in International Law

Heng Cai[1,a,*]

[1]*Law School, University of Exeter, Stocker Rd, Exeter, United Kingdom*
a. hc800@exeter.ac.uk
**corresponding author*

Abstract: With the development of network technology, cyber-attacks and cyber wars are likely to become new forms of warfare that endanger world peace. The current international law has difficulties in the definition of national sovereignty, the identification of national responsibility and the exercise of the right of self-defense when cyber-attacks occur. The international community needs to supplement and improve the existing rule system as soon as possible and impose stronger legal constraints on transnational cyber-attacks. Some measures can be taken to solve this problem. Firstly, countries around the world should be promoted to reach a consensus on the legal concept of "cyber sovereignty". Secondly, the applicable conditions of the current law need to be clarified. That is to say, the national responsibility for cyber-attacks and a clearer interpretation of "threat or use of force" and "armed attack" should be clarified. Meanwhile, the circumstances and methods of exercising the right of self-defense should be clarified when a cyber-attack is encountered. Thirdly, new rules of international law and relevant international soft laws should be created to solved these problems.

Keywords: cyber-attack, cyberwarfare, cybercrime, law of war, international law

1. Introduction

In the 1960s, computer networks were born in the military field, and have developed rapidly since then. In today's era, the network has surpassed the limitation of virtual space and has a great impact on people's real life. The Internet and information communication technology have been completely incorporated into all facets of human social life as a result of network technology's ongoing popularization and application. Networks are playing a vital role in government systems, public utilities, banks, communications and other sectors that involve national economy and security. In this context, the harm that transnational cyber-attack may cause to the overall operation of state agencies has become increasingly prominent. The destructive power of cyber warfare and the seriousness of its consequences may be comparable to or even surpass that of traditional warfare, so the international community must regulate it.

In late April 2007, the world's first cyber-attack that threatened the security of the entire country occurred in Estonia. The attack targeted the Estonian government, financial institutions, media outlets, and other organizations, causing widespread disruption to internet services and digital infrastructure. This cyber-attack involved a range of tactics, including distributed denial-of-service (DDoS) attacks, website defacement, and theft of sensitive information. The websites of some Estonian governments

DOI: 10.54254/2753-7048/19/20231391

and organizations were effectively shut down for several days. The Estonian cyber-attack highlighted the potential risks of cyberwarfare and raised concerns about the vulnerability of critical infrastructure to cyber-attacks. It has also led to increased international attention to cybersecurity and prompted many countries to invest in improving their cybersecurity defenses.

On June 1, 2012, according to David Sanger's report from the New York Times, the US and Israel jointly developed the Stuxnet virus and used it to attack Iran's uranium enrichment facilities [1]. Experts considered Stuxnet a "game-changing" cyber weapon [2]. It exploited an unknown vulnerability in Windows software and targeted the industrial control system at Iran's uranium enrichment facility. The attack reportedly destroyed more than 1,000 Iranian uranium-enriching centrifuges, undermining efforts to enrich its nuclear activities.

These cyber-attack incidents increasingly show that a country and its government's network management and control system, a country's infrastructure and social public systems are increasingly becoming targets of cyber-attacks. As the Chairman of the Joint Chiefs of Staff noted, cyber-attacks can be as damaging to critical infrastructure as weapons of mass destruction [3]. Cyber-attacks are increasingly being used by countries as new combat weapons in the information age, and the destructive power they cause is beyond the reach of traditional weapons.

Based on the investigation of existing laws and regulations and related cases, the current international law is difficult to effectively regulate cyber warfare, and cannot effectively maintain international network security and international cyberspace order. The current problems mainly include the following points. Firstly, the definition of cyber sovereignty is unclear, and the international community has not reached a broad consensus on this. Secondly, it is difficult to identify the state's responsibility for cyber-attacks, which makes it difficult to exercise the right of self-defense. Therefore, the international community needs to supplement and improve the existing rule system as soon as possible, and impose stronger legal constraints on transnational cyber-attacks.

In the research process, two methods, legal interpretation and literature research, are mainly used. Firstly, according to Article 2, Paragraph 4 and Article 51 of the UN Charter, it can be considered that cyber-attacks are "threats or use of force", and computer viruses and other programs commonly used to carry out such acts are "armed". Secondly, when discussing the shortcomings of the existing rules, it is mainly based on a large number of relevant Chinese and English literature, among which the "Tallinn Manual of International Law on Cyber Operations 2.0" has great reference value. The Tallinn Manual 2.0 is a large-scale manual that attempts to promote the formulation of international rules in cyberspace through the collective research of scholars. In numerous areas, including sovereignty, jurisdiction, state accountability, human rights law, law of the sea, and international telecommunications law, this manual systematically and exhaustively covers the laws of international law in peacetime cyberspace. At the same time, it also revised and covered the rules of international law on cyber warfare targeted by the 2013 Tallinn Manual, building a relatively complete system of international law on cyberspace that covers peacetime and wartime. Although it does not have legal effect, it still has a very high reference value in international judicial practice. However, the Tallinn Manual also has many disadvantages. Some scholars believe that the Tallinn Manual is dominated by Western developed countries, while the national conditions of the vast number of developing countries make it difficult for them to apply the rules [4]. Therefore, other more equal and effective ways should be adopted to contribute to the regulation of cyber-attacks.

The first part of this article will explain under what circumstances cyber-attacks constitute war crimes as a theoretical basis. The second part will discuss the focus of controversy and implementation difficulties in the regulation of cyber-attack in the existing international law. The third part will be based on the inadequacies of the existing international law in regulating cyber-attacks, and put forward relevant suggestions.

DOI: 10.54254/2753-7048/19/20231391

2. Theoretical Basis: Cyber-Attack May Constitute Acts of War

Cyber-attack is the starting point for cyber war, and determining what kind of cyber-attack can lead to cyber war requires examining its legality. In traditional warfare, the definitions of "threat or use of force" and "armed attack" in the UN Charter are used by the international community to determine whether an attack in traditional space is an act of war. Traditional attacks and cyber-attacks, as well as traditional and cyber conflicts, are basically different manifestations in various spatial domains. Even though there is no special international law to govern cyber warfare, the legality of cyber-attack can be examined from the standpoint of conventional war law.

2.1. Cyber-Attack and "Threat or Use of Force"

Driven by the spirit of fairness, justice and humanitarianism, the international community has made many efforts to regulate the use of force, including formulating and improving the UN Charter, convening several UN General Assembly resolutions, and so on. So far, the international community has reached a basic consensus on the standards and regulations for the legal use of force, and has established a set of international rules governing the use of force. The core provision of this system of rules is Article 2(4) of the UN Charter, which stipulates that countries shall not interfere or infringe other countries through threat or use of force, or any other method that is contrary to the purpose of the UN. That is to say, it prohibits a country from threatening or using force when dealing with international relations. Therefore, whether a cyber-attack constitutes the "threat or use of force" is the focus of determining whether it constitutes a cyber war. It needs to be judged from two situations, which are "threat of cyber-attack" and "actual implementation of cyber-attack".

"Threat of cyber-attack" refers to the behavior of a country to take positive or negative, explicit or implicit methods to indicate to other countries that it intends to launch illegal cyber-attacks against it, but does not take actual attack actions, thereby forcing other countries to yield or make compromises in order to achieve relevant goals. The international community has unanimously determined that in traditional warfare, the threat of force as a means of coercion can have serious consequences, and it is equally regulated by international law as the actual implementation of armed attacks [5,6]. As far as threats to cyber-attacks are concerned, there are two ways, which are declaring threats to use traditional weapons through the Internet and threatening to carry out cyber-attacks. However, declaring threats to use traditional weapons through the Internet is only a means of conveying threats to threatened countries through the medium of the Internet. It is essentially a traditional combat method and has little to do with cyber-attacks. Threats to carry out cyber-attacks require a definition of whether the threat itself is illegal. The ICJ believes that the "threat" and "use" of force in Article 2(4) of the UN Charter are related to a certain extent. The threat of force is regulated by relevant laws because it is illegal as the actual use of force in specific circumstances. Therefore, "threat of cyber-attack" is based on the actual implementation of cyber-attack, and whether the cyber-attack violates Article 2(4) depends on whether the cyber-attack is legal and constitutes the use of force prohibited by this article.

"Force" refers to armed or military force, and "armed force" is the main or core content of force. The word "armed" should be construed as either arming a weapon or using a weapon. It can be seen that "armed force" is inseparable from the use of "weapons", and the technical level of weapons greatly affects the form of armed forces. The concept of "armed" should be updated synchronously with the development level of weapon technology. For example, the new biological and chemical weapons and laser weapons that emerged in World War II have been recognized as "armed" and regulated by international law, even though these weapons do not have the explosive or destructive force of traditional weapons [7,8]. As a new form of attack, cyber-attack does not have visual impact and visibility, and is obviously different from traditional attacks. It is almost impossible to use

DOI: 10.54254/2753-7048/19/20231391

traditional "armed" standards to identify its attributes. Therefore, its appearance has impacted people's customary concept of "arms", causing Article 2(4) of the UN Charter to be greatly challenged [9].

However, one person cannot judge whether a certain object or technology can be identified as "armed" based solely on the external characteristics or external manifestations of weapons, so that the use of it will further constitute "use of force". Just as the ICJ stated its views on nuclear weapons when it was asked about the legality of nuclear weapons, it believed that Articles 2(4) and 51 of the UN Charter should apply to all use of force. These situations are not closely related to the weapons used, and it can even be considered that whether a certain military action can constitute "use of force" has nothing to do with the form of weapons used in the action [10]. Therefore, according to the aforementioned understanding, whether the weapons used in cyber-attacks have the characteristics of traditional weapons is not the key to constitute "armed". Instead, the key is whether a cyber-attack constitutes a "use of force" or occurs within the context of a "use of force." Only then can such cyber-attacks be interpreted as "armed attacks".

2.2. Cyber-Attack and "Armed Attack"

Cyber warfare usually does not cause direct physical damage, but the attacking country can use various methods to cause destructive and joint substantial damage to the network system of the victim country, and its actual effectiveness far exceeds that of traditional combat methods. When the international community judges whether a specific cyber-attack is a "use of force" in the sense of Article 2(4) of the UN Charter, the cyber-attack should cause a certain degree of physical damage. In addition, the international community should conduct a comprehensive analysis of cyber-attacks, not just focus on the damage results or the characteristics of their use. That is to say, consideration should be given to multiple factors such as the method, means, scope, and purpose of cyber-attacks, otherwise it is easy to identify acts such as personal hacking attacks as cyber-attacks that constitute cyber wars.

Whether the victimized state can legally exercise the right of self-defense to safeguard its own interests should identify whether a cyber-attack constitutes an "armed attack" within the meaning of Article 51 of the UN Charter. Although being subject to "armed attack" is an important prerequisite for a state to legally exercise its right of self-defense, the UN Charter and other universal international conventions, resolutions, declarations, etc. do not clarify the meaning of "armed attack" or give necessary explanations. Even so, based on relevant legal theories and international practice results, three main points of "armed attack" can be summarized. Firstly, whether it is recognized as "armed attack" does not depend on what weapons the attacker equips or uses. Secondly, an armed attack falls within the scope of the use of force. Thirdly, the use of force must reach a serious level to constitute an armed attack ("use of force" is not the same as "armed attack"). Therefore, if a cyber-attack is to constitute an "armed attack", it must also have the above three characteristics. That is to say, it must cause very serious consequences, such as controlling the dissolution of the nuclear power plant reactor and causing the nuclear material to leak, causing heavy casualties. Although so far, no cyber-attack has constituted an "armed attack", it must be confirmed that before relevant authoritative interpretations and international agreements emerge, no party shall arbitrarily make an interpretation that violates or deviates from cyber-attacks. In line with the purpose of the UN Charter and the humanitarian spirit, neither party should undermine the international consensus reached by countries on issues such as "threat or use of force" and "armed attack".

DOI: 10.54254/2753-7048/19/20231391

3. The Dilemma of Applying Existing International Law to Cyber-Attack

3.1. Difficulties in Determining Cyber Sovereignty

The essence of cyberspace is a virtual and invisible space. There are many virtual existences in this space, which constantly impact the legal terms in the traditional space, thus triggering many new legal issues such as cyber-attacks, cybercrimes, cyber infringements and cyber wars. However, the virtuality of cyberspace cannot deny the existence of various civil and criminal legal relationships between individuals or organizations in cyberspace. These relationships are objective and real, and they need to be regulated legally. In addition to virtuality, the openness of cyberspace is also its essential attribute. In cyberspace, there is no real physical border, and the difference between borders cannot be felt physically, so there is no distinction between countries. The borderlessness and interoperability brought about by this openness lead people to have the illusion that cyberspace is shared by all human beings.

Existing international law does not make any recognition of cyber sovereignty, nor does the international community have a unified understanding of it. However, public opinion against Internet sovereignty continues to intrude on the attention of the international community. They believe that the network belongs to the global commons like the high seas and space, and the borderless nature of cyberspace itself makes the discussion of network sovereignty meaningless. Therefore, they believe that sovereignty should not and cannot exist in cyberspace. However, the opponent's theory only expounds cyber sovereignty at the level of physical space, ignoring the legal level of factual existence. In the same way that there are numerous interactions and exchanges between people and nations in physical space, there are also conflicts of interest between nations and disagreements between private citizens in cyberspace. At the national level, the existence of cyber sovereignty will facilitate the settlement of disputes between countries. Although cyberspace is special, it is not a place outside the law. It cannot be exempt from the jurisdiction of national sovereignty and resist international supervision because it transcends physical space.

3.2. Difficulties in Determining the Scope of State Responsibility and the Conditions for the Application of the Right of Self-Defense

As stated in Articles 8 and 8 bis of the Rome Statute of the ICC, war crimes are often committed by persons who have the capacity to effectively manage or influence the political or military actions of a country. Traditional international law requires that the victimized state can only take self-defense measures against the state that carried out the armed attack. In the context of cyber-attacks, self-defense measures can target the originating cyber-attacking state or its state proxies. The problem, however, is that locating the source of a cyber-attack can be difficult due to the anonymity of the technologies involved. Even if a victim nation may eventually succeed in tracking a cyber-attack to a specific server in another country, this can be a very time-consuming procedure, and it may not even be feasible to positively identify the entity or person who carried out the attack. This is because an attacker could take control of a specific network system and use it as a "zombie" to launch an assault.

For these reasons, an attempt to hold a state legally accountable must be able to conclusively attribute some kind of cyber-attack to that state or its proxies. However, judging from the current cyber-attack incidents, there is very little direct evidence that can prove that countries participate in transnational cyber-attacks. Typically, the attackers uncovered through investigations are mostly non-state actors. Therefore, in this case, it is difficult to hold the State accountable.

It is considerably more challenging to use your right of self-defense because it is impossible to pinpoint the nation that needs to take responsibility. The only legitimate reason for a nation to use

DOI: 10.54254/2753-7048/19/20231391

force unilaterally is in self-defense. It is an action done by a nation in conformity with the UN Charter as a legal form of self-defense against the illegal activities of another nation. However, in reality, the damaged country adjudicates unilaterally on whether the injured country properly used its right to self-defense. Due to the judgment's extreme subjectivity, it is very possible that it will be abused arbitrarily to cause further illegal harm. The assumption behind using one's right to self-defense is that there is enough proof of the infliction of unlawful harm to establish its receipt and to establish who is to blame for it. However, in cyber warfare, it is challenging to pursue national responsibility because the origin of cyber-attacks has not yet been precisely determined. Furthermore, it can be challenging to define the start of a cyber war and to compile sufficient evidence to demonstrate that the other party has committed unlawful infringements due to elements like the immediate nature of cyber-attacks. The right to self-defense is highly susceptible to abuse in such situations.

4. The Choice of International Legislative Model for Regulating Cyber War in the Future

4.1. Promote International Consensus on Cyber Sovereignty

In order to make the conditions for the use of the law clearer, it is first necessary for international countries to reach a basic consensus on the concept and definition of cyber sovereignty. The borderless nature of cyberspace makes national borders blurred, and the traditional physical boundary theory is vulnerable to cyberspace. However, as a country's main development object and approach in the future, once cyberspace is destroyed, it will affect the development process of a country and even cause social turmoil in the country. Therefore, the territorial scope of a country should extend to the cyberspace where the country is located, and national sovereignty in cyberspace must be resolutely safeguarded.

A scholar once said that the traditional norms of international law developed on the objective basis of national territorial boundaries should also apply to cyberspace [11]. Therefore, the definition and setting of national cyber sovereignty should be similar to other national sovereignty. That is to say, internally, the country develops, supervises, and manages Internet affairs independently and without interference. Externally, the country defends against other countries' intrusion into the country's cyberspace and attacks on the country's Internet domain. With the addition of new elements such as cyberspace, new measures must be taken in the form of traditional national sovereignty to face the ever-changing development of the Internet age, so as to improve the exercise and protection of cyber sovereignty and ensure that it is not interfered by the outside world.

4.2. Clarify Applicable Conditions under the Existing International Legal Framework

The existing body of international law is the result of ongoing development, consensus-building, and summation on the part of the international community. It can still serve as the cornerstone for resolving conflicts and have a big impact even in the face of new spatial formations and new kinds of warfare.

First of all, the international community should, on the basis of existing technologies, clarify and unify the technical standards for tracking the source of cyber-attacks and the identification standards for the rules of cyber-attack behavior [12]. This helps to identify whether an attack is a cyber-attack within the scope of cyber warfare, and it can also help to trace the source and identify the country that launched the cyber-attack in a timely and accurate manner.

Secondly, the international community should also make it clear that when there is no conclusive evidence to prove that the cyber-attack can be attributed to a certain country, in order to prevent innocent countries from being implicated, the country shall not bear the responsibility for individual or organizational cyber-attacks. Moreover, the transiting countries for cyber-attacks should not bear the responsibility, unless these countries fail to fulfill their obligations under international law or

DOI: 10.54254/2753-7048/19/20231391

knowingly and intentionally indulge such attacks. Under this premise, a state's behavior should be regarded as a refusal to fulfill its obligations under international law and may be deemed a "threat or use of force" or an "armed attack". Therefore, it should be regulated and sanctioned by international law on acts of war.

Thirdly, given the nature of cyberspace and cyber-attacks, the international community should likewise define "threat or use of force" and "armed attack" clearly. The circumstances of using one's right of self-defense in defence against cyber-attacks as well as the methods and techniques for doing so should also be made clear.

4.3. Create New Rules of International Law for Cyber War

4.3.1. Create New International Treaties

To encourage the participation of nations and allow them to voice their ideas, the United Nations should actively organise pertinent conferences on cyber security. An efficient agency should be set up under the auspices of the UN to handle the myriad regulatory conundrums associated with cyberwarfare. The international community generally agrees with this idea of controlling cyberwarfare inside the framework of the UN. To promote the effective expansion of important work procedures and steady advancement, countries should swiftly submit legislative suggestions to the International Law Commission when it conducts research on cyber war and develops relevant laws in the future. For instance, if applied to the area of cyber warfare, two normative documents created by the International Law Commission, Responsibility of States for Internationally Wrongful Acts and UN General Assembly resolution 3314 (XXIX) (Definition of Aggression) could address the use of the right of states to self-defense to some extent [13]. The international community should abide by the idea of attempting to bridge divides while keeping common ground in light of the current situation when countries have varied or even extremely different perspectives on cyber warfare.

4.3.2. Attach Importance to International Soft Law

The international community has to pay more attention to the role that international "soft law" plays because it has the potential to incorporate and enhance the new rules of international law in cyber warfare. Countries share common interests in maintaining critical network infrastructure, combating cyber terrorism, and combating transnational cybercrime [14]. The establishment of an international order in cyberspace is inseparable from the cooperation of the international community. The conflicts of interests of all parties in cyberspace require long-term coordination and balance in order to promote the final formation of international rules for the peaceful use of cyberspace. Whether the final rules can reflect the wishes and interests of the participants depends on whether the participants' positions and attitudes are clear during the rule-making process.

The Tallinn Manual occupies an important position in cyberspace legislation. Documents with important reference value, such as the Tallinn Manual, tend to generalize and identify cyber-attacks as armed attacks [15]. This standard has influenced the attitudes of many countries after the formulation of the Tallinn Manual, and even has a tendency to develop into an international custom [16]. However, this standard is premised on the advanced identification and defence capabilities of developed countries with relatively advanced information and communication technologies. At the same time, countries with relatively weak network technology are at a disadvantage when dealing with this standard. Relevant countries should pay attention to soft laws such as international customs and actively express their positions. This is conducive to the final formation of rules or habits that can reflect the interests of most countries and promote the establishment of a fair and reasonable cyberspace security governance system.

DOI: 10.54254/2753-7048/19/20231391

5. Conclusion

Despite the fact that the international community has established a set of legal guidelines for war, cyberwarfare cannot be fully governed by present international law because of the vast distinctions between traditional space and cyberspace. The international community should enhance the norms of international law in light of the peculiarities of network technology and the specific fighting methods employed in cyberspace. It is important to note that the challenges posed by cyber warfare cannot be addressed from the perspective of a single discipline. Although many problems are difficult to solve, a large part of which is technical, it is also necessary to think about solving these problems from the perspectives of politics, law, and public opinion. In addition, when perfecting the rules of international law for cyber warfare, not only legal professional advice is needed, but also technical and military input to determine feasible future rules of conduct. The international community should study new international legal rules from a multidisciplinary perspective, effectively promote the process of cyber warfare and the formulation of cyberspace rules, so as to ensure the cyber security of the international community and jointly build a harmonious future world.

References

[1] *David E. S. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran, New York Times. Retrieved from https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?smid=url-share.*

[2] *Charles J. (2010). Stuxnet: Cyber warfare's game-changer, Part One. SC Media. Retrieved from https://www.scmagazine.com/news/cybercrime/stuxnet-cyber-warfares-game-changer-part-one.*

[3] *James G. (2020). Vice Chairman Discusses Weapons of Mass Destruction at Symposium. Defense News, Retrieved from https://www.defense.gov/Explore/News/Article/Article/2351492/vice-chairman-discusses-weapons-ofmass-destruction-at-symposium/.*

[4] *Huang J.J. (2020). The Right to Self-Defense of Cyber War from the Perspective of International Law, Tianjin University of Finance and Economics.*

[5] *Vienna Convention on the Law of Treaties, 1969.*

[6] *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, 1970.*

[7] *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 1972.*

[8] *Protocol on Blinding Laser Weapons (Protocol IV to the 1980 Convention), 1995.*

[9] *Zhu Y.X. (2011). Analysis of "Use of Force" Constituted by Computer Network Attack, Journal of Xi'an Politics Institute, 24:100-105.*

[10] *Summaries of Judgments, Advisory Opinions and Orders of the International Court of Justice (1992-1996), 94-104. Retrieved from https://legal.un.org/icjsummaries/documents/english/st_leg_serf1_add1.pdf.*

[11] *Jens D.O. Kevin G., Claire F. (2015). Cyberwar Law and Ethics for Virtual Conflicts, Oxford University Press, New York.*

[12] *Huang S.Q. (2019). The Regulation of International Law on Cyber Warfare, South China University of Technology.*

[13] *Nie J.J. (2019). Research on the Regulation of Cyber War by International Law, Yantai University.*

[14] *Li Y., Yuan L.L. (2021). The Situation, Motivation and Future Trend of Sino-US Strategic Game in Cyberspace, Journal of Zhengzhou University: Philosophy and Social Sciences Edition, 6: 27-33.*

[15] *Song G.S., Zheng Z. (2023). International Legal Regulation of Militarized Cyber Attacks: Reflection and Response, Journal of Guangxi Administrative Cadre Institute of Politics and Law, 38: 46-54.*

[16] *Zhang H. (2022). The Legal Approach of Applying the Prohibition of the Use of Force Doctrine in Cyberspace, China Legal Science, 2: 283-304.*