Advances in Economics, Business and Management Research, volume 215
Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)

Application of Existing Rules of International law in Cyberspace

Han Li[1, *, †], Junhao Zhang[2, †]

[1]*School of marine science, Sun Yat-sen University, Zhuhai, Guangdong, China*
[2]*School of journalism and communication, Shandong University, Jinan, Shandong, China*
[*] *Corresponding author. Email: lihan65@mail2.sysu.edu.cn*
[†]*These authors contributed equally.*

ABSTRACT
Since the birth of the Internet in the last century, it has promoted the rapid development of all walks of life. The network has penetrated into all aspects of human survival and development, including machinery manufacturing, banking, communication industry, even the government's public system and national security. With the outbreak of the first Gulf War, the Kosovo independence war and the Georgia independence war in 2008, the possible serious consequences of armed terrorist attacks on cyberspace in today's modern war have deeply attracted extensive and high attention from the international society. Furthermore, with the increasingly serious problem of network security, the exercise of the right of self-defense has become an important issue related to national security. At present, the application of the rules of international law in the field of cyberspace is still quite vague, and there is no consensus among the major powers. Therefore, through the case analysis and relevant research on the current system, this paper mainly discusses the following issues. Firstly, this essay will discuss the issues of the application of existing international law in cyberspace and make suggestions for the further development of international law. The second part will discuss under what circumstances a state can exercise its right to self-defense under international law. The definition of armed attack in cyberspace will be discussed in this part and also the circumstances under which wrongdoing constitutes the use of force. In the last part, this essay will discuss how to determine the object of the exercise of self-defense under existing international law, that is, the attribution of cyber-attacks.

Keywords: *cyber-attack, self-defense, Tallinn Manual, internationall law*

1. INTRODUCTION

With the development of modern society, the network has gradually become an integral part of human life and plays an important role in people's daily life. At the same time, with the rapid development of the Internet, the network has been gradually applied to modern wars from the end of the 20th century and has attracted extensive attention of the international community, such as the Gulf War, the Kosovo war and the Georgian war of independence.

In the Gulf War, computer network stations emerged. During the Gulf War in 1991, cyber warfare was applied to the battlefield for the first time. In this war, the network system of the Pentagon was extremely fiercely attacked. Hundreds of American confidential documents and hundreds of confidential information were stolen by hackers through the network and provided to America's opponent Iraq. The most prominent case is that a 10-year-old boy named Haka in the Netherlands invaded the electronic computer system of the U.S. Department of defense through the Internet, stole some confidential information, changed and copied some materials, and made some confidential contents of the U.S. military public. On the eve of the "Desert Storm" operation of the Gulf War, the multinational force that was ready for the war established the largest C4I system in history, but it was finally invaded by the United States using the virus.

In the Kosovo war, computer network showed its strength. During the Kosovo war, NATO led by the United States was attacked by anti-war hackers from all over the world. On March 29, 1999, Russian hackers invaded the White House website of the United States, paralyzed the website server for half an hour, and attacked the British website, which caused serious losses to the website of the British met office, which was most

needed in the NATO air raid, and then affected the change of the war situation. On March 31, 1999, NATO's Internet website and e-mail system were attacked by Yugoslavia hackers, blocking its e-mail server.

Before the full outbreak of the Russian Georgian war, a large number of data packets marked "Win+love+in+Russia" suddenly poured into the Georgian government website and completely paralyzed it. The photos of President Saakashvili were replaced with Hitler's, and the website of the Georgian presidential palace was paralyzed for 24 hours. When the Russian military action against Georgia began in full swing, the Russian cyber-attack against Georgia also began in full swing. Georgia's official websites, including media, communication and transportation systems, were paralyzed, which had a great impact on Georgia's military action and directly affected Georgia's war mobilization and support capacity.

Sufficient cases show that the role of network warfare in modern war is becoming more and more prominent. However, under the existing system, because the Internet goes beyond the limitations of the traditional national territorial boundaries, the law of war has caused many legal problems in the process of applying it to cyber war.

2. EXISTING PROBLEMS

In the face of cyber-attacks that seriously threaten the national security and public safety of other states, the existing international laws are extremely incomplete, and international community urgently needs a comprehensive law to regulate such international cyber-attacks [1]. Therefore, this part will discuss the issues of the application of existing international law in cyberspace and make suggestions for the further development of international law.

2.1. Lack of definitions of important concepts in international law

The first issue is the lack of definitions of some important concepts in the international law. According to the Article 51 of the UN Charter "nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United... [2]", the exercise of the right to self-defence is premised on an armed attack. The UN Charter does not specify the "armed attack", therefore interprets the definition of an armed attack is the key to this issue. Scholars often use phrases like cyber warfare, information warfare, cyber-attack, computer network attack, and electronic warfare interchangeably because states haven't agreed on a definition of "use of force" and "armed attack" until now [2]. For this reason, some deeper questions arise, such as what form of unlawful use of force can be considered an "armed attack"? Can cyber-attacks constitute "armed attacks" under international law? Due to the anonymity of the network and other attributes, how to define the use of force and the use of force in cyberspace is a more difficult challenge we are facing. If the operation is an armed attack, according to the UN Charter, the victim State may respond with kinetic or cyber operations at the UN Charter Article 2(4) "use of force" level, including destructive actions.

2.2. Severe problem of attribution

The second difficulty is the attribution problem, which involves determining who is responsible for a cyber-attack. It might be difficult, if not impossible, to track down the perpetrator of a professional cyber-attack. Tracking and similar forensic methods can sometimes offer very accurate attribution. Even if we can detect which computer in the globe is behind the attack using these and other methods, that fact does not always imply who is responsible for the aggression, because we cannot always determine the individual who operates the machine or her/his associations [3]. As a result, intelligence and information analysis are also required to identify the perpetrators of attacks, as well as to understand their intents and capabilities, as well as their links with other States or organizations [4]. With the anonymity of cyberspace and the existence of spoofing, access to information will become more difficult, and it may even violate law and politics, as it currently does in Nicaragua's situations. However, international law does not have strict criteria for the availability and probity of evidence. Altogether, to apply international law in cyber space, concrete standards for producing sufficient evidence for states to accuse each other of wrongdoing are required. Because only if international law's attribution conditions for self-defence are also fulfilled can the victim State legitimately initiate self-defence action against that State [5].

2.3. Lack of effectiveness of international law

The third issue is that governments are opting out of standards in favor of alternative possibilities, owing to the fact that present legislation cannot guarantee legal protection against cyber assaults by international institutions [4]. For example, the majority of countries in the world refuse to ratify the Convention on Cybercrime because it lacks clear enforcement and also it does little to limit the spread of malware or to regulate state behavior by punishing threats. The reports endorsed by the GGE and OEWG in 2021 for strengthening peace and security in cyberspace are currently non-binding, as is the Tallinn Manual as a soft law [6]. Another reason for this issue is that a government cannot detect whether its adversary is following the law, and hence cannot know whether it is benefiting from its constraint until it is too late [3]. In conclusion, the lack of binding norms governing conduct in cyberspace is a current issue in international law, leaving states with few options for

responding to and preventing cyber-enabled malicious behavior [7], which leads to more contradictions and conflicts.

3. SUGGESTIONS

3.1. Lack of definitions of important concepts in international law

3.1.1. Use of force according to Tallin Maunal

The Tallinn manual was written by 20 legal experts invited by the NATO center for excellence and cooperative Cyber Defense with the assistance of the International Red Cross and the U.S. Cyber Warfare Command. The manual is not an official NATO document or policy. It is only a recommended guide and does not represent any official position. However, Tallinn manual is the first attempt by the international community to create an international code applicable to cyber-attacks. It is the most important document on the legal aspects of cyber warfare. So, what's the definition of use of force?

Rule 68 holds that when the cyber action of a country's armed forces violates the territorial integrity or political independence of another country, it can be deemed to constitute the "use of force". It is worth noting that in the expert commentary of the rule, it is considered that once the network action has caused a considerable number of heavy casualties and serious property losses, and the physical consequences, it can certainly be regarded as constituting the use of force. However, it is considered that if the cyber-attack has not caused a considerable large-scale economic damage and consequences, then we should comprehensively consider the behavior of the cyber-attack [8].

In Rule 69, the group of experts referred to the Nicaragua case to discuss the "use of force". Through the analysis of the Nicaragua case, the expert group adopted "scale and effect" as the standard to judge that a specific act constitutes a "armed attack". The expert group believes that if the scale and effect of the relevant cyber action are equivalent to the non cyber action using force, it should be deemed to constitute the use of force. In view of the great controversy over whether a non-armed attack constitutes the use of force and there is no clear case, the expert group has put forward the method of "eight factors" to judgement. These eight factors include: seriousness, promptness, directness, invasiveness, measurable effect, military nature, the degree of state intervention and presumed legitimacy, which provides a scope for the state to evaluate whether the relevant acts constitute the use of force. These eight factors provide a range of considerations for states to assess whether the relevant acts constitute the use of force [9].

3.1.2 The concept of "use of force" and its relationship with "armed attack" according to Tallinn Manual

Tallinn manual distinguishes the concept of "use of force" and its relationship with "armed attack". Not all forms of illegal use of force can be regarded as an armed attack. As for how network behavior constitutes "use of force", the manual adopts the current mainstream view, that is, the physical effect of network behavior meets the standard of "use of force". In the manual, the expert group adopted the "eight factors" mentioned in the above article, which is an expanded interpretation of the definition of "effect". However, some cyber-attacks may not cause substantial physical harm, but this does not prevent the cyber-attack from violating the national sovereignty of the attacked country. This requires an expanded interpretation of the definition of use attack. In the Tallinn manual, the expert group adopted the idea of eight factors, which is an expanded explanation of the effects caused by the use of attacks. However, due to the need for a lot of research and discussion at the beginning of rulemaking, these factors can only contribute to post analysis, but cannot provide real-time help to the country [10]. Among them, economic factors should also be taken into account. Economic factor refers to the change of national economic value after a country's cyber-attack. Economic factors are unavoidable factors when determining that network actions constitute the "use of force".

As for how a network action constitutes a "force attack", the definition given in rule 92 of the manual is to emphasize the predictability of network action, that is, it may cause casualties or object damage through reasonable prediction. It can be seen that the definition highlights the "effect factors" of network behavior and raises its time to "expectation", so that any cyber activities that will cause damage within a reasonable prediction can be regarded as a network attack. However, the definition does not define the scope of the "effect" caused by network action, so its operability will inevitably be questioned. It should be noted that cyber attack activities will inevitably lead to the destruction of network information system and may also be accompanied by the destruction of entities, but the attack behavior of only destroying entities without destroying the network does not exist.

In the judgment of Nicaragua v., the United States in 1986, the International Court of Justice first proposed the criterion of "scale and consequences". The manual holds that the International Court of justice held that "scale" and "consequence" are the two criteria for judging that the act constitutes a military attack, but the manual evades the objective quantity and degree to which a cyber-attack can be recognized as the use of force [11].

3.1.3 Criteria for judging armed attacks: scale elements and consequence elements

Scale factor, that is, the scope of influence of the damage caused by the network action constituting the armed attack. For example, the manual lists some cyber activities and believes that as long as they reach this scale, they constitute a network attack. For example, activities related to serious injury or killing of a large number of people and serious damage or destruction of property.

The consequence elements in the manual lack a unified measurement scale. According to the view of the expert group, the elements of consequences cover immediacy, directness, invasiveness, military nature, the degree of state intervention and presumed legitimacy. These six elements are subjective and flexible. This is also due to the current inability to objectively judge the consequences of network attacks. The international expert group was also aware of this when formulating the manual, so it further explained in the notes: the manual cannot exhaust all influencing factors. With the development of society, environmental factors are also taken into account. Among the consequence factors, some scholars believe that the severity of cyber aggression and offensive and defensive violence can be judged by referring to the standards for the identification of criminal acts in the criminal laws of various countries, so as to determine whether it has been within the scope of armed attack, rather than simply considering the consequences unilaterally [12].

3.2. The attribution of cyber attack

3.2.1 Standard for attribution of the international law

Suppose now we can determine the author of the network attack, then under international law and practice, if the author meet the following three criteria, then can attribute cyber-attacks to a State.

According to the first, attacks by State organs are attributed to that State. That means if a de jure organ of a State conducts a cyber-attack, this attack would be attributed to that State, which will become a legitimate goal of self-defense operations. However, the premise of this attribution standard is that the judicial status of the organ and its validity have been affirmed on many occasions. A de facto organ can also be attributed to the State but premised on this organ is assimilated or absorbed in the institution of this State, which means there is a dependency between the State and the organ and also the State controls all fields of the organ's activities [6]. Therefore, if there is certain evidence that the organ has a certain independence, then this organ cannot be attributed to the State. But the requisite degree of control over the organ is not specify under the jurisprudence, The required degree of control over the organ, however, is not specified in the law, with the Court in the Nicaragua Case mentioning effective control in addition to general control, whilst the ICJ in the Bosnia Genocide Case spoke of "strict control" or "a great degree of control".

According to the second, attacks committed by state agents are attributed to that State. Agents are the entities that instructed, directed or controlled by a State. However, there is also a divergence of the degree of control under jurisprudence. International Court of Justice proposes effective control theory in the case of Nicaragua, that premised on each specific actions of the entity are controlled by the State. The ICTY introduced a relatively low requirements standards for control, which is called "overall control". For individual or unorganized groups, the control of the State must be effective control, and for organized groups, overall control of a State suffices. Overall control includes not only through equipment and funding the entity, but also through coordination or helping its military activities, the State does not have to give orders to the Group's head or members. At this time, even if the country cannot be proven to participate in specific attacks, it can be attributed.

According to the third argument, attacks by entities tolerated by a state were committed by that state.

According to international law, a State should not allow "its territory to be used for acts contrary to the rights of other states" and more specifically its territory is not to be used for military acts against another State. This attribution standard of toleration and unwillingness was developed in the cases of terrorist attacks which show very often.

In all of the above cases, action can be taken in self-defence against the State involved. If none of the above applies, but a non-State actor attacks another State, that non-State actor becomes the direct target of an act of self-defence [5].

3.2.2 Political aspect of attribution

The attribution of cyber-attacks is not only about technologies, but also about politics. In order to identify the author their intentions and capabilities of attacks, and the relationship between the author and other States or other entities, intelligence and information analysis are required in addition to scientific and technological investigations. The core issue of attribution is the expert's assessment of intent to attack, so political factors need to be taken into account, but this raises questions about the availability and honesty of evidence. Evidence is often difficult to obtain due to security issues, or sometimes evidence may be truncated. With regard to probity, these are issues of self-defence where there is no specific standard of proof in existing international law.

International law has no strict standards for the availability and probity of evidence and unlike the evidence requirements of criminal cases, cyber events will be more political, but it does not mean that States can exercise the right of self-defense with arbitrary evidence and absurd political inference [5].

4. CONCLUSIONS

With the progress and development of network technology, especially the rapid development of 5G technology in recent years, there are more and more unpredictable factors in the field of cyberspace, the forms of cyberspace are complex and diverse, and the governance of cyberspace is becoming more and more difficult. Under the background of the network age, it has become a general trend for all countries to improve their network science and technology level to deal with any form of network attack, improve their own cyberspace system, and finally promote the formation of international cyberspace legal norms.

The Tallinn manual attempts to create an international code applicable to cyber-attacks for the first time, which involves the rules of international law of cyberspace in peacetime in 15 fields such as sovereignty, jurisdiction, state responsibility, human rights law, law of the sea and international telecommunications law. It systematically answers the question of the applicability of international law to cyber warfare and constructs an international code including peacetime and wartime relatively complete rule system of international law in Cyberspace.

Taking Tallinn manual version 2.0 as the starting point, this paper aims to provide theoretical support for the country to safeguard its own interests when it is attacked by the network and provide some references for improving international network governance. Because the law itself has the limited characteristics of lag, it makes the current legal norms unable to accurately predict the future development. However, it does not mean that the formulation of laws is not forward-looking. Preventing cyber-attacks and promoting cyberspace governance require equal dialogue and joint discussion among countries, and there is still a long way to go [9].

REFERENCES

[1] S. B. Jiang, Cyber-attack and the application of war law, Wuhan University International Law Review, vol. 16, no. 2, 2013, pp. 43-70.

[2] B. J. Li, On network warfare and the application of war law Legal review,2013,31(04):58-64.

[3] J. Goldsmith, How Cyber Changes the Laws of War, European Journal of International Law, vol. 24, no. 1, pp. 129-138, 2013.

[4] N. Katagiri, Why international law and norms do little in preventing non-state cyber-attacks. Journal of cybersecurity, vol. 7, no. 1, 2021.

[5] N. Tsagourias, Cyber Attacks, Self-Defence and the Problem of Attribution, Journal of Conflict and Security Law, vol. 17, no. 2, 2012, pp. 229-244.

[6] M. Schmitt, Cyber Responses “By The Numbers” in International Law, 2015. https://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/

[7] I. Bogdanova, M. V. Callo-Müller, Unilateral Economic Sanctions to Deter and Punish Cyber-Attacks: Are They Here to Stay? 2021, https://www.ejiltalk.org/unilateral-economic-sanctions-to-deter-and-punish-cyber-attacks-are-they-here-to-stay/

[8] M. N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare Cambridge:Cambridge University Press, 2013, pp.28.

[9] W. X. Zhou, The exercise of China's right to self-defense in cyber attacks from the perspective of Tallinn manual version 2.0, Shanghai Normal University, 2021.

[10] M. L. Wang, Y. Chen, On the principle of prohibiting the use of force in cyberspace, International law research, no. 4, 2019, pp. 18-32.

[11] Y. Zhang, Interpretation of the definition of “network attack” in Tallinn manual version 2.0, Wuhan University International Law Review, vol. 3, no. 3, 2019, pp. 124-138.

[12] G. H. Todd, Armed Attack in Cyberspace: Deterring Asymmetric Warfare with An Asymmetric Definition, The Air Force Review, 2009, pp. 75-81.